М. Айгнер, Г. Циглер

Доказательства из Книги

Лучшие доказательства со времен Евклида до наших дней

Издательство БИНОМ

ДОКАЗАТЕЛЬСТВА ИЗ КНИГИ

ЛУЧШИЕ ДОКАЗАТЕЛЬСТВА СО ВРЕМЕН ЕВКЛИДА ДО НАШИХ ДНЕЙ

Martin Aigner, Günter M. Ziegler

Proofs from THE BOOK

Fourth Edition

Including illustrations by Karl H. Hofmann

Corrected printing 2013

Springer

М. Айгнер, Г. Циглер

Доказательства из Книги

Лучшие доказательства со времен Евклида до наших дней

2-е издание, дополненное
(электронное)

С иллюстрациями Карла Г. Хофмана

Перевод 4-го английского издания
Б. И. Селиванова

под редакцией
А. М. Зубкова

Москва
БИНОМ. Лаборатория знаний
2014

УДК 51.1
ББК 22.1
А37

Айгнер М.

А37 Доказательства из Книги. Лучшие доказательства со времен Евклида до наших дней [Электронный ресурс] / М. Айгнер, Г. Циглер ; пер. 4-го англ. изд. — 2-е изд., доп. (эл.). — Электрон. текстовые дан. (1 файл pdf : 291 с.). — М. : БИНОМ. Лаборатория знаний, 2014. — Систем. требования: Adobe Reader XI ; экран 10".

ISBN 978-5-9963-2736-2

В книге собраны красивые и глубокие теоремы из различных областей теории чисел, геометрии, анализа, комбинаторики, теории графов. Доказательства этих теорем используют неожиданные сочетания разнородных идей. Изложение материала сопровождается большим числом иллюстраций.

Книга предназначена всем, кто увлечен математикой: в первую очередь студентам, аспирантам, а также преподавателям, научным работникам и просто любителям изящных математических рассуждений. Многое в книге доступно школьникам старших классов.

УДК 51.1
ББК 22.1

Деривативное электронное издание на основе печатного аналога: Доказательства из Книги. Лучшие доказательства со времен Евклида до наших дней / М. Айгнер, Г. Циглер ; пер. 4-го англ. изд. — 2-е изд., доп. — М. : БИНОМ. Лаборатория знаний, 2014. — 288 с. : ил. — ISBN 978-5-9963-0629-9.

16+

ISBN 978-5-9963-2736-2

Предисловие редактора перевода

Появление монографии «Доказательства из Книги», на мой взгляд, является выдающимся событием: редко бывает, чтобы математическая книга (не учебник!) за 5 лет переиздавалась 2 раза. Мартин Айгнер и Гюнтер Циглер, основываясь на предложениях и рекомендациях Пауля Эрдёша, собрали много замечательных и удивительных результатов из различных областей математики (теории чисел, геометрии, анализа, комбинаторики, теории графов) и сумели с блеском изложить их полные, но краткие доказательства, которые используют неожиданные сочетания разнородных идей. Текст удачно дополняют со вкусом подобранные и специально для этой книги сделанные рисунки.

В чем-то аналогами «Доказательств из Книги» были знаменитые «Числа и фигуры» Радемахера и Теплица, а также некоторые книги из издававшейся в СССР серии «Библиотека математического кружка». Однако в отличие от них цель «Доказательств из Книги» — не столько изложить какие-то части математических теорий, сколько предоставить читателю возможность насладиться изяществом математических рассуждений и почувствовать единство областей математики, кажущихся далекими друг от друга. Кроме того, «Доказательства из Книги» интересны для *всех* любителей математики, в том числе для увлеченных ею школьников (хотя доказательства в книге часто сложнее решений олимпиадных задач и требуют больше знаний), для студентов, аспирантов, преподавателей и для математиков-профессионалов. С этой точки зрения она не имеет аналогов.

Конечно, на отбор тем повлияли вкусы Пауля Эрдёша и ее авторов. Конечно, в других областях математики тоже есть красивые теоремы с замечательными доказательствами. Возможно, эта книга стимулирует их популяризацию.

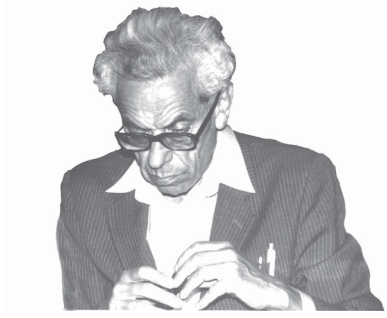
Надеюсь, что при переводе удалось сохранить непринужденный стиль изложения авторов. С их согласия был добавлен ряд замечаний (как правило — чтобы упростить понимание материала), а также расширены списки литературы к нескольким главам (ссылки, добавленные при переводе, отмечены звездочками).

Москва, ноябрь 2005 года *А.Зубков*

Первое издание «Доказательств из Книги» на русском языке (М.: Мир, 2006) сразу стало библиографической редкостью. Новое издание соответствует 4-му англоязычному изданию 2010 года, в которое авторы добавили 5 новых интересных глав и внесли изменения в другие главы.

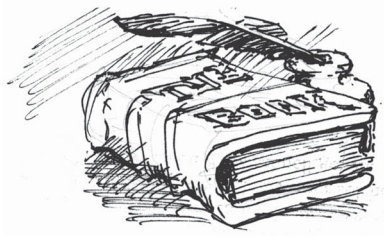
Москва, февраль 2014 года *А.Зубков*

Предисловие



Пауль Эрдёш

Пауль Эрдёш, вспоминая афоризм Г. Г. Харди о том, что для скверной математики не должно быть места, любил говорить о Книге, в которую Бог включает совершенные доказательства математических теорем. Эрдёш говорил также, что вы не обязаны верить в Бога, но как математик вы должны верить в Книгу. Несколько лет тому назад мы предложили ему написать первое (и достаточно скромное) приближение к Книге. Пауль с энтузиазмом воспринял эту идею и, что характерно для него, немедленно начал работу, заполняя страницу за страницей своими предложениями. Предполагалось, что наша книга появится в качестве подарка к 85-летию Эрдёша в марте 1998 года. К несчастью, летом 1996 года Пауль умер, что не позволило включить его в список соавторов. Вместо этого мы посвятили ему эту книгу.



«Книга»

У нас нет определения или четкого описания условий включения доказательства в Книгу. Все, что мы здесь предлагаем, — примеры, которые выбраны в надежде на то, что читатели разделят наш восторг от блестящих идей, тонкой интуиции и удивительных наблюдений. Мы надеемся также, что читатели получат удовольствие от книги, несмотря на несовершенство нашего изложения. Отбор доказательств был произведен в значительной степени под влиянием самого Пауля Эрдёша. Он предложил широкий список тем. Многие из доказательств найдены Эрдёшем или инициированы его удивительной способностью ставить правильные вопросы и выдвигать правильные гипотезы. Так что эта книга в большой степени отражает взгляды Пауля Эрдёша на то, каким должно быть доказательство из Книги.

Выбор тем ограничивался нашим желанием сделать материал книги доступным для читателей, подготовка которых лишь в малой степени включает технику студентов-математиков последних курсов. Немного сведений из линейной алгебры, основы анализа и теории чисел, довольно приличный объем элементарных понятий и соображений из дискретной математики достаточны для того, чтобы понимать написанное в этой книге и получать от этого удовольствие.

Мы чрезвычайно благодарны многим людям, которые помогали нам и поддерживали нас в работе над этим проектом. Среди них студенты семинара, на котором мы обсуждали предварительную версию книги: Бенно Артман, Стефан Брандт, Стефан Фельснер, Эли Гудман, Торстен Хелдман и Ханс Мильке. Мы благодарны Маргрит Баррет, Христиану Бресслеру, Евгению Гаврилову, Михаэлю Есвигу, Елке Позе и Йору Рамбау за техническую помощь в составлении книги. Мы многим обязаны Тому Троттеру, который прочитал рукопись от первой до последней страницы, Карлу Х. Хоффману за его удивительные рисунки, и более всего великому ушедшему от нас Паулю Эрдёшу.

Берлин, март 1998 года *Мартин Айгнер, Гюнтер М. Циглер*

Предисловие к четвертому изданию

Когда почти пятнадцать лет назад мы начинали этот проект, то не представляли себе, какие замечательные и непрекращающиеся отклики вызовет наша книга о Книге, сколько мы получим писем с благодарностями, интересными комментариями, сколько будет новых изданий и — к настоящему времени — тринадцать переводов. Не будет преувеличением сказать, что он стал частью наших жизней.

Кроме многочисленных улучшений, частично предложенных нашими читателями, настоящее четвертое издание содержит пять новых глав: две классические, о законе взаимности квадратичных вычетов и об основной теореме алгебры, две главы о разбиениях и их увлекательных решениях, и о прорыве в теории графов — хроматических числах графов Кнезера.

Мы благодарны всем, кто помогал нам и поддерживал нас все это время. По второму изданию этот список включает Стефана Брандта, Кристиана Элшольца, Юргена Элстродта, Дэниела Грайзера, Роджера Хит-Брауна, Ли Л.Кинера, Кристиана Лебофа, Ханфрида Ленца, Николаса Печа, Джона Скоулса, Бернульфа Вайсбаха и *многих* других. Заметно улучшили третье издание вклады Дэвида Бевэна, Андерса Бьернера, Дитриха Брэсса, Джона Косгрейва, Хьюберта Калфа, Гюнтера Пикерта, Алистера Синклэра и Херба Вилфа. За советы при подготовке настоящего четвертого издания мы особенно признательны Франсу Дакару, Оливеру Дайзеру, Антону Дохтерману, Михаэлю Харбеку, Стефану Хоугарди, Хендрику В.Ленстре, Гюнтеру Роту, Морису Шмитту и Карстену Шульцу. Мы благодарим Рут Аллевельт из издательства Шпрингер в Гейдельберге, а также Кристофа Эйриха, Торстена Хельдмана и Элке Поза из Берлина за помощь и поддержку в течение всех этих лет. Наконец, несомненно, вид этой книги был бы другим без оригинального оформления, предложенного Карлом-Фридрихом Кохом, и превосходных новых рисунков, которые к каждому изданию готовил Карл Х. Хоффман.

Берлин, июль 2009 года *Мартин Айгнер, Гюнтер М. Циглер*

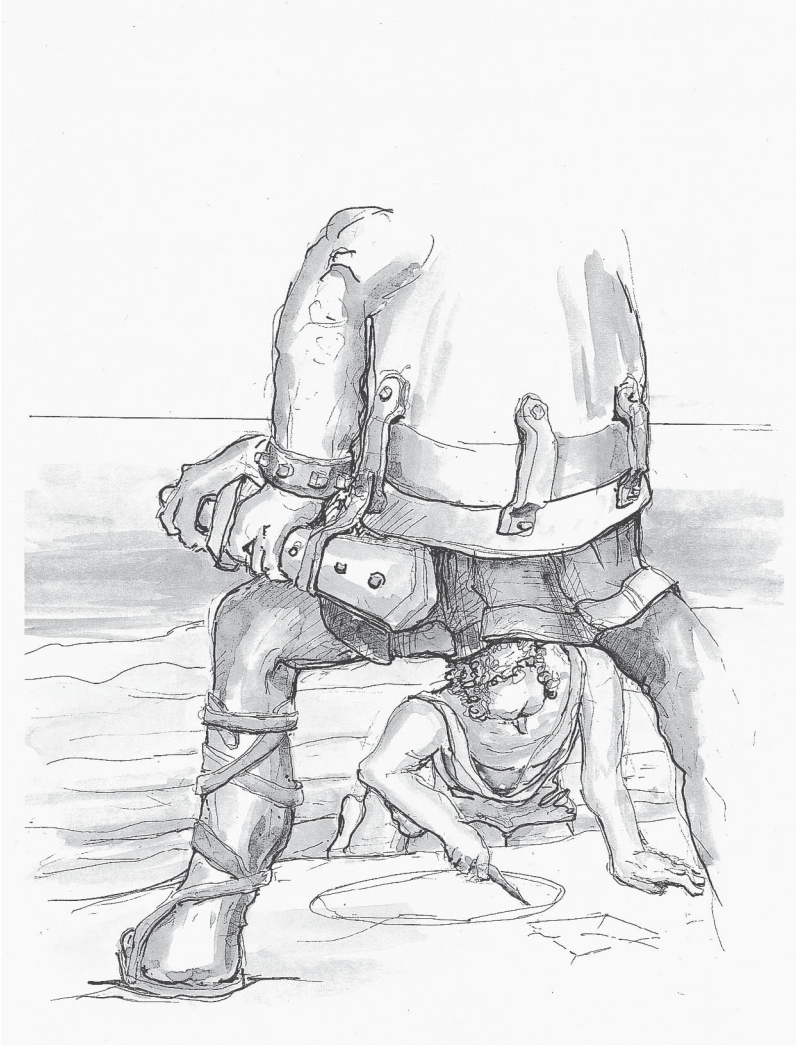
Предисловие ко второму русскому изданию

Когда мы представляли наш первый англоязычный вариант «Доказательств из Книги» на Международном математическом конгрессе в Берлине в 1998 году, мы не были уверены в том, как он будет встречен — и были поражены откликом. Мы тогда думали также, что закончили (всю необходимую) работу — но оказались не правы. Наоборот, этот проект развивался далее, окрыляемый откликами и предложениями наших читателей из разных стран, в частности, специалистов, переводивших книгу на разные языки.

Поэтому мы чрезвычайно рады тому, что первое русское издание получило такой замечательный прием (что подтверждается прекрасными письмами и e-mail'ами), а также желанию сделать расширенное четвертое английское издание нашей книги доступным для русских читателей. Мы признательны А. М. Зубкову и Б. И. Селиванову за их большой труд, внимание и знания, которые они вложили в этот перевод. Мы надеемся, что второе русское издание для многих читателей окажется полезным, поучительным и доставит им удовольствие.

Берлин, февраль 2014 года *Мартин Айгнер, Гюнтер М. Циглер*

Теория чисел



«Иррациональность и π»

Глава 1 Шесть доказательств бесконечности множества простых чисел

Очень естественно начать эти заметки, по-видимому, старейшим доказательством из Книги, которое обычно приписывают Евклиду (Начала, IX, см. [5*]). Оно обосновывает бесконечность последовательности простых чисел.

■ **Доказательство Евклида.** Для любого конечного множества простых $\{p_1, \ldots, p_r\}$ рассмотрим число $n = p_1 p_2 \cdots p_r + 1$. Это n имеет простой делитель p, который не совпадает ни с одним из чисел p_i, $i = 1, \ldots, r$: в противном случае p был бы делителем и n, и произведения $p_1 p_2 \cdots p_r$ и, следовательно, разности $n - p_1 p_2 \ldots p_r = 1$, что невозможно. Поэтому никакое конечное множество $\{p_1, \ldots, p_r\}$ не может быть совокупностью всех простых чисел. □

Зафиксируем следующие обозначения: $\mathbb{N} = \{1, 2, 3, \ldots\}$ — множество натуральных чисел, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ — множество целых чисел и $\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ — множество простых чисел.

Ниже приводится несколько других доказательств (выбранных из значительно большей коллекции); мы надеемся, что они понравятся читателю почти так же, как и нам. В них используются различные подходы, но для всех доказательств следующие базисные идеи являются общими: последовательность натуральных чисел неограниченно возрастает, каждое натуральное число $n \geq 2$ имеет простой делитель. Вместе эти два факта обусловливают бесконечность $\mathbb{P}$.

Второе доказательство предложил Кристиан Гольдбах (в письме Леонарду Эйлеру в 1730 году), третье, видимо, относится к фольклору, четвертое найдено Эйлером [3], пятое доказательство предложил Гарри Фюрстенберг [4], а последнее принадлежит Паулю Эрдёшу [2].

■ **Второе доказательство.** Вначале рассмотрим *числа Ферма* $F_n = 2^{2^n} + 1$, $n = 0, 1, 2, \ldots$ Покажем, что любые два числа Ферма взаимно просты; отсюда следует, что число простых чисел бесконечно. Для этого достаточно доказать рекуррентное соотношение

$$\prod_{k=0}^{n-1} F_k \quad = \quad F_n - 2 \qquad (n \geq 1),$$

из которого немедленно вытекает наше утверждение: если m делит, скажем, F_k и F_n $(k < n)$, то m делит 2 и поэтому m равно 1 или 2. Но равенство $m = 2$ невозможно, так как все числа Ферма нечетны.

Чтобы доказать рекуррентное соотношение, воспользуемся индукцией по n. Для $n = 1$ имеем $F_0 = 3$ и $F_1 - 2 = 3$. Теперь, учитывая

$F_0 = 3$
$F_1 = 5$
$F_2 = 17$
$F_3 = 257$
$F_4 = 65537$
$F_5 = 641 \cdot 6700417$

Несколько первых чисел Ферма

предположение индукции, получаем

$$\prod_{k=0}^{n} F_k \;=\; \Big(\prod_{k=0}^{n-1} F_k\Big)F_n \;=\; (F_n-2)F_n \;=$$
$$=\; (2^{2^n}-1)(2^{2^n}+1) \;=\; 2^{2^{n+1}}-1 \;=\; F_{n+1}-2.$$

□

■ **Третье доказательство.** Предположим, что $\mathbb{P}$ конечно и что p — наибольшее простое число. Рассмотрим так называемое *число Мерсенна*[1] 2^p-1 и покажем, что любой простой делитель q числа 2^p-1 больше p, что и даст желаемое противоречие. Пусть q — простой делитель 2^p-1, так что $2^p \equiv 1 \pmod q$. Поскольку p — простое число, это означает, что элемент 2 имеет порядок p в мультипликативной группе $\mathbb{Z}_q\backslash\{0\}$ конечного поля $\mathbb{Z}_q$. Эта группа содержит $q-1$ элементов. В силу теоремы Лагранжа (см. вставку на полях) порядок любого элемента делит порядок группы, т. е. $p \,|\, q-1$, и, значит, $p<q$. □

Теперь рассмотрим доказательство, в котором используются элементы математического анализа.

■ **Четвертое доказательство.** Пусть $\pi(x) := \#\{p \le x : p \in \mathbb{P}\}$ — число простых, не превосходящих действительного числа x. Перенумеруем простые числа в $\mathbb{P} = \{p_1, p_2, p_3, \ldots\}$ в возрастающем порядке. Рассматривая натуральный логарифм $\ln x$, будем использовать известное из анализа равенство $\ln x = \int_1^x \frac{1}{t}\,dt$.

Сравним теперь площадь под графиком функции $f(t) = \frac{1}{t}$ с площадью под графиком ступенчатой функции $g(t) = \frac{1}{[t]}$. (Об этом приеме см. также приложение к гл. 2 на с. 19.) Тогда при $n \le x < n+1$

$$\ln x \;\le\; 1+\frac12+\frac13+\ldots+\frac{1}{n-1}+\frac1n \le$$
$$\le\; \sum \frac1m\,, \text{ где сумма берется по всем } m\in\mathbb{N}, \text{ все простые делители которых не больше } x.$$

Так как каждое такое m можно *единственным* образом записать в виде произведения $\prod\limits_{p\le x} p^{k_p}$, где $k_p \ge 0$, то сумма в правой части равна

$$\prod_{\substack{p\in\mathbb{P}\\ p\le x}} \Big(\sum_{k\ge 0}\frac{1}{p^k}\Big).$$

Под знаком произведения стоят суммы членов геометрических прогрессий со знаменателями $\frac1p$. Следовательно,

$$\ln x \;\le\; \prod_{\substack{p\in\mathbb{P}\\ p\le x}} \frac{1}{1-\frac1p} \;=\; \prod_{\substack{p\in\mathbb{P}\\ p\le x}} \frac{p}{p-1} \;=\; \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k-1}\,.$$

Теорема Лагранжа

Если G — конечная (мультипликативная) группа и U — ее подгруппа, то $|U|$ (число элементов U) делит $|G|$.

■ **Доказательство.** Рассмотрим бинарное отношение

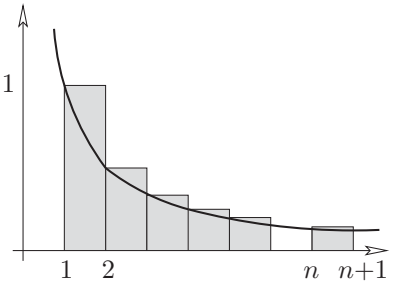
$$a \sim b :\iff ba^{-1} \in U.$$

Из определения группы следует, что $\sim$ есть отношение эквивалентности. Содержащий элемент a класс эквивалентности совпадает с классом смежности

$$Ua = \{xa : x \in U\}.$$

Ясно, что $|Ua| = |U|$, поэтому G разбивается на классы эквивалентности, каждый из которых имеет $|U|$ элементов. Отсюда вытекает, что $|U|$ делит $|G|$. □

Частный случай: пусть $U = \{a, a^2, \ldots, a^m\}$ — циклическая подгруппа и m — наименьшее положительное целое число, для которого $a^m = 1$ (такое число называется *порядком* элемента a). Согласно теореме Лагранжа порядок элемента a делит порядок $|G|$ группы G.



Функция $f(t) = \frac1t$ и ступенчатая функция $g(t) = \frac{1}{[t]}$

[1] Марен Мерсенн (1588–1648) — французский математик, физик и философ. — *Прим. ред.*

Ясно, что $p_k \geq k+1$, и поэтому

$$\frac{p_k}{p_k-1} \;=\; 1+\frac{1}{p_k-1} \;\leq\; 1+\frac{1}{k} \;=\; \frac{k+1}{k}\,,$$

вследствие чего

$$\ln x \;\leq\; \prod_{k=1}^{\pi(x)} \frac{k+1}{k} \;=\; \pi(x)+1.$$

Функция $\ln x$ не ограничена. Поэтому $\pi(x)$ тоже не ограничена, а это значит, что существует бесконечно много простых чисел. □

■ **Пятое доказательство.** Теперь после аналитического дадим топологическое доказательство. Рассмотрим следующую занятную топологию на множестве $\mathbb{Z}$ целых чисел. Положим для $a,\ b \in \mathbb{Z},\ b>0$,

$$N_{a,b} = \{a+nb : n \in \mathbb{Z}\}.$$

«Запускаем плоские камушки в бесконечность»

Каждое множество $N_{a,b}$ есть бесконечная в обе стороны арифметическая прогрессия. Назовем множество $O \subseteq \mathbb{Z}$ *открытым*, если O пусто или если для каждого $a \in O$ существует такое $b>0$, что $N_{a,b} \subseteq O$. (*Замкнутыми* называются множества $S \subseteq \mathbb{Z}$, дополнения $\mathbb{Z}\backslash S$ к которым открыты, и только такие множества. — *Прим. ред.*) Ясно, что объединение открытых множеств является открытым. Если O_1, O_2 — открытые множества и $a \in O_1 \cap O_2$, причем $N_{a,b_1} \subseteq O_1$ и $N_{a,b_2} \subseteq O_2$ для некоторых $b_1,\ b_2 \in \mathbb{Z}$, то $a \in N_{a,b_1b_2} \subseteq O_1 \cap O_2$. Поэтому любое конечное пересечение открытых множеств тоже открыто[2]. Это семейство открытых множеств индуцирует топологию на $\mathbb{Z}$.

Теперь отметим два факта:

(A) Любое непустое открытое множество бесконечно.

(B) Любое множество $N_{a,b}$ является замкнутым.

В самом деле, (A) следует из определения. Далее, заметим, что

$$N_{a,b} \;=\; \mathbb{Z}\backslash \bigcup_{i=1}^{b-1} N_{a+i,b},$$

значит, $N_{a,b}$ замкнуто как дополнение к открытому множеству.

До сих пор о простых числах мы не упоминали; теперь, наконец, они появляются.

Так как любое число $n \neq 1, -1$ имеет некоторый простой делитель p и, следовательно, содержится в $N_{0,p}$, мы приходим к выводу, что

$$\mathbb{Z}\backslash\{1,-1\} \;=\; \bigcup_{p\in\mathbb{P}} N_{0,p}.$$

Если бы $\mathbb{P}$ было конечно, то $\bigcup_{p\in\mathbb{P}} N_{0,p}$ было бы замкнуто как конечное объединение замкнутых согласно (B) множеств. Поэтому $\{1,-1\}$ как дополнение к замкнутому множеству было бы открытым, что противоречит (A). □

[2] Из этого свойства и правил теоретико-множественных операций следует, что объединение конечного числа замкнутых множеств замкнуто (как дополнение к пересечению их дополнений). — *Прим. ред.*

■ **Шестое доказательство.** Наше последнее доказательство значительно более содержательно и обосновывает не только бесконечность множества простых чисел, но и расходимость ряда $\sum_{p\in\mathbb{P}} \frac{1}{p}$. Первое доказательство этого важного результата было получено Эйлером (и оно по-своему интересно), но приведенное ниже доказательство, изобретенное Эрдёшем, очень красиво.

Пусть $p_1, p_2, p_3, \ldots$ — последовательность простых чисел в возрастающем порядке. Предположим, что ряд $\sum_{p\in\mathbb{P}} \frac{1}{p}$ сходится. Тогда существует такое натуральное число k, что

$$\sum_{i\geq k+1} \frac{1}{p_i} < \frac{1}{2}.$$

Следовательно, для произвольного натурального числа N

$$\sum_{i\geq k+1} \frac{N}{p_i} \;<\; \frac{N}{2}. \tag{1}$$

Назовем $p_1, \ldots, p_k$ *малыми* простыми числами, а $p_{k+1}, p_{k+2}, \ldots$ — *большими* простыми числами.

Пусть N_b — количество положительных целых $n \leq N$, которые делятся хотя бы на одно большое простое число, и N_s — количество положительных целых $n \leq N$, имеющих лишь малые простые делители. Покажем, что для некоторого $N < \infty$ имеет место неравенство

$$N_b + N_s \;<\; N,$$

которое даст нам желаемое противоречие, так как по определению сумма $N_b + N_s$ должна равняться N.

Заметим, что $\lfloor \frac{N}{p_i} \rfloor$ равно количеству положительных целых чисел $n \leq N$, кратных p_i (символом $\lfloor x \rfloor$ здесь и далее обозначается наибольшее целое, не превосходящее x, а символом $\lceil x \rceil$ — наименьшее целое, которое не меньше x. — *Прим. перев.*). Поэтому в силу (1) получаем

$$N_b \;\leq\; \sum_{i\geq k+1} \left\lfloor \frac{N}{p_i} \right\rfloor \;<\; \frac{N}{2}. \tag{2}$$

Теперь рассмотрим N_s. Запишем каждое $n \leq N$, имеющее лишь малые простые делители, в виде $n = a_n b_n^2$, где множитель a_n свободен от квадратов, т. е. каждое a_n есть произведение *различных* малых простых чисел. Отсюда вытекает, что имеется ровно 2^k различных свободных от квадратов множителей. Далее, так как $b_n \leq \sqrt{n} \leq \sqrt{N}$, то существует не более $\sqrt{N}$ различных квадратов, меньших N, и поэтому

$$N_s \;\leq\; 2^k\sqrt{N}.$$

Поскольку (2) справедливо для *произвольного* N, остается лишь найти такое число N, что $2^k\sqrt{N} \leq \frac{N}{2}$, или $2^{k+1} \leq \sqrt{N}$, для чего достаточно положить $N = 2^{2k+2}$. □

Литература

[1] Artmann B. *Euclid — The Creation of Mathematics.* Springer-Verlag, New York, 1999.

[2] Erdös P. *Über die Reihe* $\sum \frac{1}{p}$, Mathematica, Zutphen B, **7** (1938), 1–2.

[3] Euler L. *Introductio in Analysin Infinitorum,* Tomus Primus, Lausanne 1748; Opera Omnia, Ser. 1, Vol. 8. [Имеется перевод: Эйлер Л. *Введение в анализ бесконечных*, т. 1. М.: Физматгиз, 1961.]

[4] Fürstenberg H. *On the infinitude of primes,* Amer. Math. Monthly, **62** (1955), 353.

[5*] Евклид. *Начала, кн. VII–X.* М.–Л.: ГИТТЛ, 1949.

Постулат Бертрана

Глава 2

Мы видели, что последовательность простых чисел $2, 3, 5, 7, \ldots$ бесконечна. Чтобы показать, что размеры лакун (промежутков между соседними числами) в ней не ограничены, обозначим через

$$N = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p$$

произведение всех простых чисел, которые меньше $k + 2$. Заметим, что ни одно из k чисел

$$N + 2, N + 3, N + 4, \ldots, N + k, N + (k + 1)$$

не является простым, так как простые делители любого числа $i = 2, 3, \ldots, k + 1$ меньше $k + 2$ и делят N; следовательно, они делят также $N + i$. С помощью этого приема мы находим, например, для $k = 10$, что ни одно из чисел

$$2312, 2313, 2314, \ldots, 2321$$

не является простым.

Существуют также верхние оценки для лакун в последовательности простых чисел. Согласно самой известной оценке, «лакуна до следующего простого не может быть больше числа, с которой она начинается». Это утверждение называют постулатом Бертрана, так как оно было высказано в форме предположения и проверено эмпирически для $n < 3\,000\,000$ Джозефом Бертраном. Впервые оно было доказано Пафнутием Чебышёвым около 1850 года [5*]. Значительно более простое доказательство нашел индийский гений Рамануджан. Доказательство в нашей книге принадлежит Паулю Эрдёшу. Оно взято из его первой статьи [1], опубликованной в 1932 году, когда Эрдёшу было 19 лет.

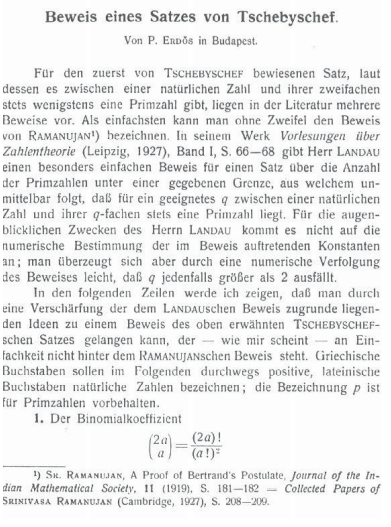
Джозеф Бертран

Постулат Бертрана.
Для каждого $n \geq 1$ существует такое простое число p, что $n < p \leq 2n$.

■ **Доказательство.** Мы получим достаточно хорошую оценку биномиального коэффициента $\binom{2n}{n}$ и с ее помощью покажем, что если бы он не имел простых делителей p, лежащих между n и $2n$, то он был бы «слишком мал». Наше рассуждение состоит из пяти шагов.

(1) Вначале докажем постулат Бертрана для $n < 4000$. Для этого нет необходимости проверять 4000 вариантов: достаточно (используя «прием Ландау») проверить, что

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001$$



Beweis eines Satzes von Tschebyschef.

Von P. Erdös in Budapest.

Für den zuerst von Tschebyschef bewiesenen Satz, laut dessen es zwischen einer natürlichen Zahl und ihrer zweifachen stets wenigstens eine Primzahl gibt, liegen in der Literatur mehrere Beweise vor. Als einfachsten kann man ohne Zweifel den Beweis von Ramanujan[1]) bezeichnen. In seinem Werk *Vorlesungen über Zahlentheorie* (Leipzig, 1927), Band I, S. 66—68 gibt Herr Landau einen besonders einfachen Beweis für einen Satz über die Anzahl der Primzahlen unter einer gegebenen Grenze, aus welchem unmittelbar folgt, daß für ein geeignetes q zwischen einer natürlichen Zahl und ihrer q-fachen stets eine Primzahl liegt. Für die augenblicklichen Zwecken des Herrn Landau kommt es nicht auf die numerische Bestimmung der im Beweis auftretenden Konstanten an; man überzeugt sich aber durch eine numerische Verfolgung des Beweises leicht, daß q jedenfalls größer als 2 ausfällt.

In den folgenden Zeilen werde ich zeigen, daß man durch eine Verschärfung der dem Landauschen Beweis zugrunde liegenden Ideen zu einem Beweis des oben erwähnten Tschebyschefschen Satzes gelangen kann, der — wie mir scheint — an Einfachkeit nicht hinter dem Ramanujanschen Beweis steht. Griechische Buchstaben sollen im Folgenden durchwegs positive, lateinische Buchstaben natürliche Zahlen bezeichnen; die Bezeichnung p ist für Primzahlen vorbehalten.

1. Der Binomialkoeffizient

$$\binom{2a}{a} = \frac{(2a)!}{(a!)^2}$$

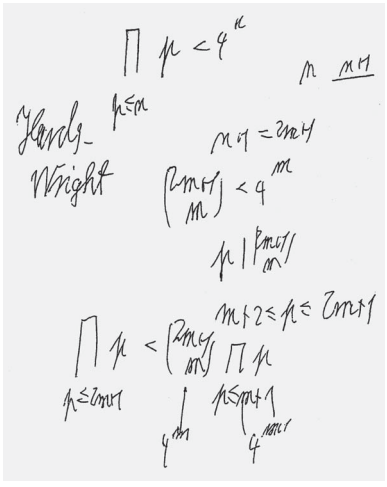
[1]) Sr. Ramanujan, A Proof of Bertrand's Postulate. *Journal of the Indian Mathematical Society*, 11 (1919), S. 181—182 — *Collected Papers of* Srinivasa Ramanujan (Cambridge, 1927), S. 208—209.

есть последовательность простых чисел, в которой каждое последующее меньше удвоенного предыдущего. Поэтому каждый интервал $\{y : n < y \le 2n\}$, где $n \le 4000$, содержит одно из этих 14 простых чисел.

(2) Далее докажем, что

$$\prod_{p \le x} p \;\le\; 4^{x-1} \quad \text{для всех вещественных } x \ge 2, \tag{1}$$

запись $\prod_{p \le x} p$ здесь и в дальнейшем означает, что произведение берется по всем *простым* числам $p \le x$.



Приведенное ниже доказательство этого факта использует индукцию по числу простых. Оно не содержится в оригинальной статье Эрдёша, но также принадлежит ему (см. рисунок на полях) и является истинным Доказательством из Книги.

Вначале заметим, что если q — наибольшее простое, не превосходящее x, то

$$\prod_{p \le x} p \;=\; \prod_{p \le q} p \qquad \text{и} \qquad 4^{q-1} \;\le\; 4^{x-1}.$$

Таким образом, (1) достаточно проверить в случае $x = q$, где q — простое число.

Если $q = 2$, мы имеем «$2 \le 4$», так что база индукции обоснована, и мы далее будем рассматривать нечетные числа $q = 2m + 1$. Разобьем произведение на две части и убедимся в том, что

$$\prod_{p \le 2m+1} p \;=\; \prod_{p \le m+1} p \cdot \prod_{m+1 < p \le 2m+1} p \;\le\; 4^m \binom{2m+1}{m} \;\le\; 4^m 2^{2m} \;=\; 4^{2m}.$$

Действительно, неравенство

$$\prod_{p \le m+1} p \;\le\; 4^m$$

справедливо в силу предположения индукции. Неравенство

$$\prod_{m+1 < p \le 2m+1} p \;\le\; \binom{2m+1}{m}$$

вытекает из того, что

$$\binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!}$$

есть целое число и что все входящие в произведение простые числа являются делителями числителя $(2m+1)!$, но ни одно из них не является делителем знаменателя $m!(m+1)!$ Наконец, неравенство

$$\binom{2m+1}{m} \;\le\; 2^{2m}$$

вытекает из того, что

$$\binom{2m+1}{m} \quad \text{и} \quad \binom{2m+1}{m+1}$$

суть два (равных!) слагаемых в сумме

$$\sum_{k=0}^{2m+1} \binom{2m+1}{k} = 2^{2m+1}.$$

Итак, соотношение (1) доказано по индукции.

(3) Согласно приведенной на полях теореме Лежандра, разложение биномиального коэффициента $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ на простые множители содержит p ровно

$$\sum_{k\ge 1} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right)$$

раз. Каждое слагаемое в этой сумме не превосходит 1, так как оно является целым числом и

$$\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \;<\; \frac{2n}{p^k} - 2\left(\frac{n}{p^k} - 1\right) \;=\; 2.$$

Более того, слагаемые, для которых $p^k > 2n$, равны нулю. Поэтому разложение $\binom{2n}{n}$ содержит простой множитель p

$$\sum_{k\ge 1} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right) \;\le\; \max\{r : p^r \le 2n\}$$

раз. Следовательно, наибольшая степень числа p, которая делит $\binom{2n}{n}$, не превосходит $2n$. В частности, каждое простое $p > \sqrt{2n}$ появляется в разложении $\binom{2n}{n}$ не более одного раза.

Кроме того (и это, согласно Эрдёшу, является ключом к его доказательству), простые p, удовлетворяющие условию $\frac{2}{3}\,n < p \le n$, вообще не являются делителями числа $\binom{2n}{n}$. Действительно, из условия $3p > 2n$ следует (для $n \ge 3$, и, следовательно, для $p \ge 3$), что из кратных простого p в качестве множителей в числитель дроби $\frac{(2n)!}{n!n!}$ могут входить только p и $2p$, в то время как в знаменателе мы уже имеем два множителя, равных p.

(4) Теперь перейдем к оценке $\binom{2n}{n}$. Для $n \ge 3$, используя неравенство со с. 20 в качестве нижней оценки, получаем

$$\frac{4^n}{2n} \;\le\; \binom{2n}{n} \;\le\; \prod_{p\le\sqrt{2n}} 2n \;\cdot \prod_{\sqrt{2n}<p\le\frac{2}{3}n} p \;\cdot \prod_{n<p\le 2n} p\,,$$

и, так как существует не более $\sqrt{2n}$ простых чисел $p \le \sqrt{2n}$, отсюда для $n \ge 3$ находим:

$$4^n \;\le\; (2n)^{1+\sqrt{2n}} \cdot \prod_{\sqrt{2n}<p\le\frac{2}{3}n} p \;\cdot \prod_{n<p\le 2n} p\,. \qquad (2)$$

(5) Предположим теперь, что простых чисел в промежутке $n < p \le 2n$ не содержится, так что второе произведение в (2) равно 1. Подставляя (1) в (2), находим

$$4^n \;\le\; (2n)^{1+\sqrt{2n}}\, 4^{\frac{2}{3}n},$$

Теорема Лежандра

Простое число p входит в разложение числа $n!$ на простые множители ровно

$$\sum_{k\ge 1} \left\lfloor \frac{n}{p^k} \right\rfloor$$

раз.

■ **Доказательство.** В произведении $n! = 1\cdot 2\cdot 3\cdot \ldots \cdot n$ ровно $\lfloor \frac{n}{p} \rfloor$ сомножителей делятся на p, что дает $\lfloor \frac{n}{p} \rfloor$ простых множителей p в разложении $n!$. Далее, $\lfloor \frac{n}{p^2} \rfloor$ чисел среди $1, \ldots, n$ делятся на p^2, что дает еще $\lfloor \frac{n}{p^2} \rfloor$ простых множителей p в разложении $n!$, и т. д. □

Примеры
$\binom{26}{13} = 2^3 \cdot 5^2 \cdot 7 \cdot 17 \cdot 19 \cdot 23$
$\binom{28}{14} = 2^3 \cdot 3^3 \cdot 5^2 \cdot 17 \cdot 19 \cdot 23$
$\binom{30}{15} = 2^4 \cdot 3^2 \cdot 5 \cdot 17 \cdot 19 \cdot 23 \cdot 29$
показывают, что «очень малые» простые множители $p < \sqrt{2n}$ могут входить в разложение $\binom{2n}{n}$ с большими степенями, «малые» простые из промежутка $\sqrt{2n} < p \le \frac{2}{3}n$ могут быть только в первой степени, а простые множители из лакуны $\frac{2}{3}\,n < p \le n$ вообще отстутствуют.

или

$$4^{\frac{1}{3}n} \;\le\; (2n)^{1+\sqrt{2n}}, \tag{3}$$

что для достаточно больших n неверно! В самом деле, так как $a+1 < 2^a$ для всех $a \ge 2$, то

$$2n = \left(\sqrt[6]{2n}\right)^6 < \left(\lfloor \sqrt[6]{2n} \rfloor + 1\right)^6 < 2^{6\left\lfloor \sqrt[6]{2n} \right\rfloor} \le 2^{6\sqrt[6]{2n}}. \tag{4}$$

При $n \ge 50$ (когда $18 < 2\sqrt{2n}$) из (3) и (4) вытекает, что

$$2^{2n} \le (2n)^{3\left(1+\sqrt{2n}\right)} <$$
$$< 2^{\sqrt[6]{2n}\left(18+18\sqrt{2n}\right)} < 2^{20\sqrt[6]{2n}\sqrt{2n}} = 2^{20(2n)^{2/3}}.$$

Поэтому $(2n)^{1/3} < 20$, вследствие чего $n < 4000$. Значит, для любого $n \ge 4000$ существует такое простое число p, что $n < p < 2n$. □

Из приведенной выше оценки (2) тем же самым способом можно извлечь большее: для $n \ge 4000$

$$\prod_{n<p\le 2n} p \ge 2^{\frac{1}{30}n},$$

и поэтому в промежутке между n и $2n$ имеется не менее

$$\log_{2n}\left(2^{\frac{1}{30}n}\right) \;=\; \frac{1}{30}\,\frac{n}{\log_2 n + 1}$$

простых чисел. Это не слишком грубая оценка: «истинное» число простых чисел в указанном промежутке равно приблизительно $n/\ln n$, что следует из «закона распределения простых чисел», согласно которому

$$\lim_{n\to\infty} \frac{\#\{p \le n : p \text{ простое}\}}{n/\ln n}$$

существует и равен 1 (запись $\#A$ обозначает число элементов множества A). Этот замечательный результат был впервые доказан Адамаром и де ла Валле-Пуссеном в 1896 году[1]. Селберг и Эрдёш в 1948 году нашли элементарное доказательство без использования комплексного анализа, но длинное и сложное.

В законе распределения простых чисел последнее слово, однако, еще не сказано. Например, доказательство гипотезы Римана (см. с. 59), одной из главных нерешенных проблем математики, может привести к существенному уточнению оценок в теореме о простых числах. Можно надеяться также на значительное усиление постулата Бертрана. Например, следующее предложение еще не доказано:

[1] Важным шагом на пути к теореме Адамара и Валле-Пуссена были работы П.Л.Чебышёва ([5*], [6*], см. также [7*]), из которых следовало, что

$$0.921 < \frac{\#\{p \le n : p \text{ простое }\}}{n/\ln n} < 1.106$$

при достаточно больших n. Отметим также один из последних результатов (см. [8*]):

$$\#\{p \le n : p \text{ простое}\} < \frac{n}{\ln n - 1 - (\ln n)^{-1/2}} \text{ при } n \ge 6,$$

$$\#\{p \le n : p \text{ простое}\} > \frac{n}{\ln n - 1 + (\ln n)^{-1/2}} \text{ при } n \ge 59.$$

— *Прим. ред.*

В промежутке между n^2 и $(n+1)^2$ всегда найдется простое число.

Дополнительную информацию можно найти в [3, с. 19] и [4, с. 248, 257].

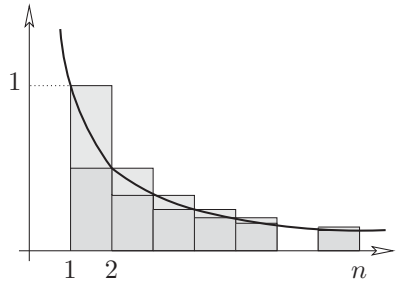
Приложение: Некоторые оценки

Оценки с помощью интегралов

Существует очень простой, но эффективный метод оценивания сумм с помощью интегралов, использованный на с. 11. Для оценивания *гармонических чисел*

$$H_n \;=\; \sum_{k=1}^{n} \frac{1}{k}$$

рассмотрим приведенные на полях графики функций $\frac{1}{t}$, $\frac{1}{\lfloor t \rfloor}$ и $\frac{1}{1+\lfloor t \rfloor}$.



Неравенство

$$H_n - 1 \;=\; \sum_{k=2}^{n} \frac{1}{k} \;<\; \int_1^n \frac{1}{t}\,dt \;=\; \ln n$$

доказывается сравнением области под графиком функции $f(t) = \frac{1}{t}$ $(1 \le t \le n)$ с областью, состоящей из темных заштрихованных прямоугольников, а неравенство

$$H_n - \frac{1}{n} \;=\; \sum_{k=1}^{n-1} \frac{1}{k} \;>\; \int_1^n \frac{1}{t}\,dt \;=\; \ln n$$

— сравнением с областью, состоящей из больших прямоугольников и включающей светлые заштрихованные части. Объединяя эти оценки, получаем

$$\ln n + \frac{1}{n} \;<\; H_n \;<\; \ln n \;+\; 1.$$

В частности, $\lim\limits_{n\to\infty} H_n = \infty$, и порядок роста чисел H_n описывается соотношением $\lim\limits_{n\to\infty} \frac{H_n}{\ln n} = 1$. Известны также (см. [2]) значительно лучшие оценки, например

$$H_n \;=\; \ln n + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + \frac{1}{120n^4} + O\left(\frac{1}{n^6}\right),$$

где $\gamma \approx 0.5772$ — «константа Эйлера».

Здесь запись $O\left(\frac{1}{n^6}\right)$ обозначает функцию $g(n)$ такую, что $|g(n)| \le c\frac{1}{n^6}$, где c — некоторая константа.

Оценки факториалов — формула Стирлинга

Тот же самый метод, примененный к сумме

$$\ln(n!) \;=\; \ln 2 + \ln 3 + \ldots + \ln n \;=\; \sum_{k=2}^{n} \ln k,$$

приводит к оценкам

$$\ln((n-1)!) \;<\; \int_1^n \ln t\,dt \;<\; \ln(n!),$$

и интеграл легко вычисляется:

$$\int_1^n \ln t\,dt \;=\; \Big[t\ln t - t\Big]_1^n \;=\; n\ln n - n + 1.$$

Отсюда мы получаем как оценку снизу для $n!$

$$n! \;>\; e^{n\ln n - n + 1} \;=\; e\Big(\frac{n}{e}\Big)^n,$$

так и оценку сверху

$$n! \;=\; n\,(n-1)! \;<\; ne^{n\ln n - n + 1} \;=\; en\Big(\frac{n}{e}\Big)^n.$$

Здесь выражение $f(n) \sim g(n)$ означает, что $\lim\limits_{n\to\infty} \dfrac{f(n)}{g(n)} = 1$.

Чтобы найти асимптотику $n!$, требуется более тонкий анализ, который приводит к *формуле Стирлинга*

$$n! \;\sim\; \sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

И снова существуют ее уточненные варианты, например:

$$n! \;=\; \sqrt{2\pi n}\left(\frac{n}{e}\right)^n\left(1 + \frac{1}{12n} + \frac{1}{288n^2} - \frac{139}{5140n^3} + O\left(\frac{1}{n^4}\right)\right).$$

Оценки биномиальных коэффициентов

Как известно, непосредственно из определения биномиальных коэффициентов $\binom{n}{k}$ как числа k-подмножеств n-множества следует, что последовательность $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$:

- суммируется и $\sum\limits_{k=0}^{n}\binom{n}{k} = 2^n$,
- симметрична: $\binom{n}{k} = \binom{n}{n-k}$.

```
                1
              1   1
            1   2   1
          1   3   3   1
        1   4   6   4   1
      1   5   10  10  5   1
    1   6   15  20  15  6   1
1   7   21  35  35  21  7   1
```

Треугольник Паскаля

Из функционального уравнения $\binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1}$ легко найти, что для каждого n биномиальные коэффициенты $\binom{n}{k}$ образуют последовательность, которая симметрична и *унимодальна*: ее элементы возрастают при приближении к середине, так что средние биномиальные коэффициенты являются наибольшими:

$$1 = \tbinom{n}{0} < \tbinom{n}{1} < \ldots < \tbinom{n}{\lfloor n/2\rfloor} = \tbinom{n}{\lceil n/2\rceil} > \ldots > \tbinom{n}{n-1} > \tbinom{n}{n} = 1.$$

Из асимптотических формул для факториалов, упомянутых выше, можно получить очень точные оценки для биномиальных коэффициентов. Однако в этой книге нам понадобятся лишь довольно грубые и простые оценки, например, $\binom{n}{k} \le 2^n$ для всех k. С другой стороны, для $n \ge 2$ имеем

$$\binom{n}{\lfloor n/2\rfloor} \;\ge\; \frac{2^n}{n},$$

причем равенство выполняется только при $n = 2$. В частности, для $n \ge 1$

$$\binom{2n}{n} \;\ge\; \frac{4^n}{2n}.$$

Действительно, так как центральный биномиальный коэффициент $\binom{n}{\lfloor n/2 \rfloor}$ является максимальным в последовательности

$$\binom{n}{0} + \binom{n}{n}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1},$$

сумма всех n элементов которой равна 2^n, то он больше среднего значения элементов этой последовательности, равного $\frac{2^n}{n}$.

Наконец, отметим еще одну верхнюю оценку для биномиальных коэффициентов:

$$\binom{n}{k} = \frac{n(n-1)\ldots(n-k+1)}{k!} \leq \frac{n^k}{k!} \leq \frac{n^k}{2^{k-1}};$$

она довольно хороша для «малых» биномиальных коэффициентов из хвостов образуемой ими последовательности, если n велико по сравнению с k.

Литература

[1] Erdős P. *Beweis eines Satzes von Tschebyschef.* Acta Sci. Math. (Szeged), **5** (1930–32), 194–198.

[2] Graham R. L., Knuth D. E., Patashnik O. *Concrete Mathematics. A Foundation for Computer Science.* Addison-Wesley, Reading MA, 1989. [Есть русский перевод: Грэхем Р., Кнут Д., Паташник О. *Конкретная математика. Основание информатики.* М., Мир, 1998.]

[3] Hardy G. H., Wright E. M. *An Introduction to the Theory of Numbers,* 5th edition. Oxford University Press, 1979.

[4] Ribenboim P. *The New Book of Prime Number Records.* Springer-Verlag, New York, 1989.

[5*] Chebyshev P. L. *Mémoire sur les nombres premies.* Mémoires des savants étrangers de l'Acad. Imp. Sci. de St.-Pétersbourg, 1850, t.VII; J. de math. pures et appl., I série, 1852, t.XVII; русский перевод: *О простых числах.* В сб. Чебышёв П. Л. *Избранные математические труды*, М.-Л., ГИТТЛ, 1946, с.53–72; *Избранные труды*, изд-во АН СССР, М., 1955, с.33–54.

[6*] Chebyshev P. *Sur la fonction qui détermine la totalité des nombers premiers inférieurs à une limite donnée.* — Приложение III к Теории сравнений, С.-Петербург, 1849; Mémoires des savants étrangers de l'Acad. Imp. Sci. de St.-Pétersbourg, 1848, t.VI; J. de math. pures et appl., I série, 1852, t.XVII; русский перевод: *Об определении числа простых чисел, не превосходящих данной величины.* В сб. Чебышёв П. Л. *Избранные математические труды*, М.-Л., ГИТТЛ, 1946, с.29–52, *Избранные труды*, изд-во АН СССР, 1955, с.9–32.

[7*] Делоне Б. Н. *Петербургская школа теории чисел.* М.-Л, изд-во АН СССР, 1947.

[8*] Panaitopol L. *Inequalities concerning the function $\pi(x)$: Applications.* Acta Arithmetica, 2000, v.XCIV, № 4, 373–381.

Глава 3

Биномиальные коэффициенты (почти) никогда не являются степенями

У постулата Бертрана есть уточнение, которое приводит к замечательному результату для биномиальных коэффициентов. В 1892 году Сильвестр следующим образом усилил постулат Бертрана:

Если $n \geq 2k$, то хотя бы одно из чисел $n, n-1, \ldots, n-k+1$ имеет простой делитель p, больший k.

Заметим, что в случае $n = 2k$ мы получаем в точности постулат Бертрана. В 1934 году Эрдёш нашел для предложения Сильвестра короткое и элементарное доказательство из Книги, аналогичное его доказательству постулата Бертрана. Эквивалентная формулировка теоремы Сильвестра выглядит следующим образом:

Биномиальный коэффициент

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} \qquad (n \geq 2k)$$

всегда имеет простой делитель $p > k$.

Имея в виду это замечание, обратимся к другому бриллианту Эрдёша. Когда $\binom{n}{k}$ равно степени m^ℓ? Легко видеть, что при $k = \ell = 2$ существует бесконечно много решений уравнения $\binom{n}{2} = m^2$. Действительно, если $\binom{n}{2}$ — квадрат, то $\binom{(2n-1)^2}{2}$ — тоже квадрат: при $n(n-1) = 2m^2$ справедливо равенство

$$(2n-1)^2((2n-1)^2-1) = (2n-1)^2 \cdot 4n(n-1) = 2(2m(2n-1))^2,$$

так что

$$\binom{(2n-1)^2}{2} = (2m(2n-1))^2.$$

Начиная с $\binom{9}{2} = 6^2$, мы получим бесконечно много решений; следующее решение есть $\binom{289}{2} = 204^2$. Однако это не дает нам всех решений. Например, $\binom{50}{2} = 35^2$ начинает другую серию решений, как и $\binom{1682}{2} = 1189^2$. Известно, что в случае $k = 3$ уравнение $\binom{n}{3} = m^2$ имеет единственное решение $n = 50$, $m = 140$. Но на этом решения исчерпываются: для $k \geq 4$ и любого $\ell \geq 2$ решений не существует, и это доказано Эрдёшем с помощью остроумного рассуждения.

$\binom{50}{3} = 140^2$ — единственное решение для $k = 3$, $\ell = 2$

Теорема. *Если $\ell \geq 2$ и $4 \leq k \leq n-4$, то уравнение*

$$\binom{n}{k} = m^\ell$$

не имеет решений в целых числах.

■ **Доказательство.** Вначале заметим, что достаточно рассмотреть случай $n \geq 2k$, так как $\binom{n}{k} = \binom{n}{n-k}$. Предположим, что теорема не верна, т. е. выполняется равенство $\binom{n}{k} = m^\ell$. Доказательство того, что это приводит к противоречию, разобьем на четыре пункта.

(1) По теореме Сильвестра биномиальный коэффициент $\binom{n}{k}$ имеет простой делитель p, больший k, так что p^ℓ делит $n(n-1)\cdots(n-k+1)$. Ясно, что лишь один из множителей $n-i$ может быть кратен p, поскольку $p > k$, и, следовательно, $p^\ell \mid n-i$, в силу чего

$$n \;\geq\; p^\ell \;>\; k^\ell \;\geq\; k^2.$$

(2) Рассмотрим произвольный множитель $n-j$ в числителе дроби $\frac{n(n-1)\cdots(n-k+1)}{k!}$ и запишем его в виде

$$n - j = a_j m_j^\ell, \quad j = 0, 1, \ldots, k-1, \tag{1}$$

где a_j не делится ни на какую нетривиальную ℓ-ю степень. Заметим, что согласно п.**(1)** все простые делители a_j не превосходят k. Теперь покажем, что $a_i \neq a_j$, если $i \neq j$. Для этого предположим противное, т. е. что $a_i = a_j$ для некоторых $i < j$. Тогда $m_i \geq m_j + 1$ и

$$\begin{aligned} k \;&>\; (n-i) - (n-j) = \; a_j(m_i^\ell - m_j^\ell) \;\geq\; a_j((m_j+1)^\ell - m_j^\ell) \\ &>\; a_j \ell m_j^{\ell-1} \;\geq\; \ell(a_j m_j^\ell)^{1/2} \;\geq\; \ell(n-k+1)^{1/2} \geq \\ &\geq\; \ell(\tfrac{n}{2}+1)^{1/2} \;>\; n^{1/2}, \end{aligned}$$

что противоречит неравенству $n > k^2$, полученному в п. **(1)**.

(3) Далее докажем, что числа $a_0, a_1, \ldots, a_{k-1}$ образуют перестановку множества $1, 2, \ldots, k$. (Согласно Эрдёшу, это центральный момент доказательства.) Так как из п. **(2)** мы уже знаем, что все эти числа различны, то достаточно показать, что

$$a_0 a_1 \cdots a_{k-1} \quad \text{делит} \quad k!$$

Подставляя $n - j = a_j m_j^\ell$, $j = 0, 1, \ldots, k-1$, в уравнение $\binom{n}{k} = m^\ell$, получаем

$$a_0 a_1 \cdots a_{k-1}(m_0 m_1 \cdots m_{k-1})^\ell \;=\; k! m^\ell.$$

Сокращая общие множители чисел $m_0 \ldots m_{k-1}$ и m, находим

$$a_0 a_1 \cdots a_{k-1} u^\ell \;=\; k! v^\ell,$$

причем НОД$(u, v) = 1$. Осталось доказать, что $v = 1$. Если это не так, то v имеет некоторый простой делитель p. Так как НОД$(u, v) = 1$, то p должен быть простым делителем произведения $a_0 a_1 \ldots a_{k-1}$ и, следовательно, $p \leq k$. Согласно теореме Лежандра (см. с. 17),

$$k! \quad \text{содержит } p \text{ в степени} \quad \sum_{i \geq 1} \left\lfloor \frac{k}{p^i} \right\rfloor. \tag{2}$$

Теперь оценим степень p в произведении $n(n-1)\cdots(n-k+1)$. Пусть i — натуральное число, а числа $b_1 < b_2 < \ldots < b_s$ — кратные p^i элементы последовательности $n, n-1, \ldots, n-k+1$. Тогда $b_s = b_1 + (s-1)p^i$ и поэтому

$$(s-1)p^i \;=\; b_s - b_1 \;\leq\; n - (n-k+1) \;=\; k-1,$$

откуда следует, что

$$s \;\le\; \Big\lfloor \frac{k-1}{p^i} \Big\rfloor + 1 \;\le\; \Big\lfloor \frac{k}{p^i} \Big\rfloor + 1.$$

Итак, для каждого i число элементов, кратных p^i, среди $n, \dots, n-k+1$ (и, тем самым, среди $a_0, a_1, \dots, a_{k-1}$) ограничено сверху величиной $\lfloor \frac{k}{p^i} \rfloor + 1$. Это означает, что степень p в произведении $a_0 a_1 \cdots a_{k-1}$ (аналогично теореме Лежандра из гл. 2) не превосходит

$$\sum_{i=1}^{\ell-1} \Big(\Big\lfloor \frac{k}{p^i} \Big\rfloor + 1 \Big). \tag{3}$$

Суммирование в (3) останавливается на $i = \ell - 1$, так как множители $a_0, a_1, \dots, a_{k-1}$ не делятся на ℓ-е степени.

Мы видим, что наш анализ согласуется с равенством $\binom{50}{3} = 140^2$, так как
$50 = 2 \cdot 5^2$
$49 = 1 \cdot 7^2$
$48 = 3 \cdot 4^2$
и $5 \cdot 7 \cdot 4 = 140$.

Учитывая оценки (2) и (3), мы находим, что степень p в v^ℓ не превосходит

$$\sum_{i=1}^{\ell-1} \Big(\Big\lfloor \frac{k}{p^i} \Big\rfloor + 1 \Big) - \sum_{i \ge 1} \Big\lfloor \frac{k}{p^i} \Big\rfloor \;\le\; \ell - 1,$$

и получаем противоречие, так как v^ℓ есть ℓ-я степень v.

Этого достаточно, чтобы установить справедливость теоремы в случае $\ell = 2$. Действительно, так как $k \ge 4$, то один из множителей a_i должен равняться четырем, но согласно п. **(2)** числа a_i не делятся на квадраты.

Поэтому теперь предположим, что $\ell \ge 3$.

(4) Так как $k \ge 4$, то для некоторых i_1, i_2, i_3 мы должны иметь равенства $a_{i_1} = 1$, $a_{i_2} = 2$, $a_{i_3} = 4$, т. е.

$$n - i_1 = m_1^\ell, \quad n - i_2 = 2m_2^\ell, \quad n - i_3 = 4m_3^\ell.$$

Докажем, что $(n-i_2)^2 \ne (n-i_1)(n-i_3)$. Предположив противное, положим $b = n - i_2$ и $n - i_1 = b - x$, $n - i_3 = b + y$, где $0 < |x|, |y| < k$. Тогда

$$b^2 = (b-x)(b+y), \qquad \text{или} \qquad (y-x)b = xy,$$

где равенство $x = y$, очевидно, невозможно. Теперь согласно п.**(1)**

$$|xy| \;=\; b|y-x| \;\ge\; b \;>\; n-k \;>\; (k-1)^2 \;\ge\; |xy|,$$

и мы пришли к противоречию.

Итак, $m_2^2 \ne m_1 m_3$; предположим, что $m_2^2 > m_1 m_3$ (в противном случае будем действовать аналогично), и выпишем нашу последнюю цепочку неравенств

$$\begin{aligned} 2(k-1)n \;&>\; n^2 - (n-k+1)^2 \;>\; (n-i_2)^2 - (n-i_1)(n-i_3) = \\ &=\; 4[m_2^{2\ell} - (m_1 m_3)^\ell] \;\ge\; 4[(m_1 m_3 + 1)^\ell - (m_1 m_3)^\ell] \ge \\ &\ge\; 4\ell m_1^{\ell-1} m_3^{\ell-1}. \end{aligned}$$

Так как $\ell \ge 3$ and $n > k^\ell \ge k^3 > 6k$, то отсюда получаем

$$\begin{aligned} 2(k-1)n m_1 m_3 \;&>\; 4\ell m_1^\ell m_3^\ell \;=\; \ell(n-i_1)(n-i_3) > \\ &>\; \ell(n-k+1)^2 \;>\; 3\Big(n - \frac{n}{6}\Big)^2 \;>\; 2n^2. \end{aligned}$$

Далее, поскольку $m_i \le n^{1/\ell} \le n^{1/3}$, окончательно находим

$$kn^{2/3} \;\ge\; km_1m_3 \;>\; (k-1)m_1m_3 \;>\; n,$$

или $k^3 > n$. Полученное противоречие завершает доказательство. $\square$

Литература

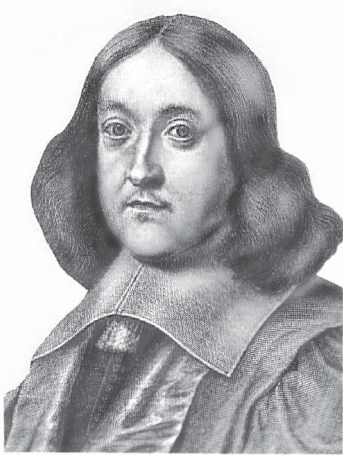
[1] Erdős P. *A theorem of Sylvester and Schur.* J. London Math. Soc., **9** (1934), 282–288.

[2] Erdős P. *On a diophantine equation.* J. London Math. Soc., **26** (1951), 176–178.

[3] Sylvester J. J. *On arithmetical series.* Messenger of Math. **21** (1892), 1–19, 87–120; Collected Mathematical Papers, Vol. 4, 1912, 687–731.

Глава 4 Представления чисел в виде сумм двух квадратов

$$
\begin{aligned}
1 &= 1^2 + 0^2 \\
2 &= 1^2 + 1^2 \\
3 &= \\
4 &= 2^2 + 0^2 \\
5 &= 2^2 + 1^2 \\
6 &= \\
7 &= \\
8 &= 2^2 + 2^2 \\
9 &= 3^2 + 0^2 \\
10 &= 3^2 + 1^2 \\
11 &= \\
&\vdots
\end{aligned}
$$



Пьер де Ферма

Какие числа могут быть записаны в виде сумм двух квадратов?

Эта проблема такая же древняя, как и теория чисел, а ее решение является классическим. «Трудная» часть решения состоит в доказательстве того, что каждое простое число вида $4m+1$ есть сумма двух квадратов. Г. Г. Харди пишет, что эта *теорема Ферма о двух квадратах* «вполне справедливо считается одной из наиболее совершенных в арифметике».

Тем не менее, ее доказательство, приведенное в нашей Книге Доказательств, получено совсем недавно.

Начнем с небольшой подготовки. Во-первых, нам нужно различать простое число $p = 2$, простые вида $p = 4m+1$, и простые вида $p = 4m+3$. Каждое простое число принадлежит ровно одному из этих трех классов. Покажем (используя метод Евклида), что существует бесконечно много простых чисел вида $4m+3$. В самом деле, допустим, что их число конечно, и обозначим наибольшее простое число вида $4m+3$ через p_k. Положив

$$N_k \;:=\; 2^2 \cdot 3 \cdot 5 \cdots p_k - 1,$$

где $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots$ — последовательность всех простых чисел, мы найдем, что

$$N_k \equiv 3 \,(\mathrm{mod}\, 4);$$

поэтому N_k должно иметь простой делитель вида $4m+3$, и этот простой делитель больше p_k. Таким образом, мы получили противоречие.

Первая наша лемма характеризует простые числа, для которых -1 есть квадрат в поле $\mathbb{Z}_p$, которое описано на вставке на следующей странице. Она позволяет, кроме того, получить простое доказательство того, что множество простых чисел вида $4m+1$ бесконечно.

Лемма. *Для простых $p = 4m+1$ уравнение $s^2 \equiv -1 \,(\mathrm{mod}\, p)$ имеет два решения $s \in \{1, 2, \ldots, p-1\}$, для $p = 2$ существует одно такое решение, а для простых чисел вида $p = 4m+3$ решений не существует.*

■ **Доказательство.** В случае $p = 2$ решением является $s = 1$. Для нечетных p введем на $\{1, 2, \ldots, p-1\}$ отношение эквивалентности, полагая каждый элемент эквивалентным его аддитивному и мультипликативному обратным в $\mathbb{Z}_p$. Следовательно, «общие» классы эквивалентности будут содержать четыре элемента:

$$\{x, -x, \overline{x}, -\overline{x}\},$$

так как такое четырехэлементное множество содержит оба обратных для каждого своего элемента. Однако если некоторые из четырех

элементов совпадают, то мощность (число элементов) класса эквивалентности уменьшается:

- $x \equiv -x$ — невозможно для нечетных p.
- $x \equiv \overline{x}$ — эквивалентно сравнению $x^2 \equiv 1$, которое имеет два решения, а именно, $x = 1$ и $x = p - 1$, и приводит к классу эквивалентности $\{1, p-1\}$, содержащему два элемента.
- $x \equiv -\overline{x}$ — эквивалентно сравнению $x^2 \equiv -1$. Оно может не иметь решений или иметь два различных решения $\{x_0, p - x_0\}$.

Множество $\{1, 2, \ldots, p-1\}$ имеет $p-1$ элементов, и мы разбили его на четверки (классы эквивалентности мощности 4) и одну или две пары (классы эквивалентности мощности 2). Если $p - 1 = 4m + 2$, то может существовать лишь одна пара $\{1, p-1\}$, остальные — четверки, так что сравнение $s^2 \equiv -1 \pmod p$ решений не имеет. Если $p - 1 = 4m$, то в разбиении имеется вторая пара, которая содержит два искомых решения уравнения $s^2 \equiv -1$. □

Для $p = 11$ разбиение есть $\{1, 10\}, \{2, 9, 6, 5\}, \{3, 8, 4, 7\}$; для $p = 13$ оно имеет вид $\{1, 12\}, \{2, 11, 7, 6\}, \{3, 10, 9, 4\}$ и $\{5, 8\}$, причем $\{5, 8\}$ дает два решения $s^2 \equiv -1 (\mathrm{mod} 13)$.

Согласно лемме 1 любой нечетный простой делитель числа $M^2 + 1$ имеет вид $4m+1$. Отсюда следует, что множество простых чисел такого вида бесконечно: в противном случае можно рассмотреть число $(2 \cdot 3 \cdot 5 \cdot \ldots \cdot q_k)^2 + 1$, где q_k — наибольшее простое число такого вида, и получить противоречие аналогично предыдущему.

Простые поля

Если p — простое число, то множество $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, в котором определены сложение и умножение «по модулю p», образует конечное поле. Нам потребуются следующие простые свойства множества $\mathbb{Z}_p$:

- Для $x \in \mathbb{Z}_p$, $x \neq 0$, аддитивный обратный (который мы обычно обозначаем $-x$) вычисляется по формуле $p - x \in \{1, 2, \ldots, p-1\}$. Если $p > 2$, то x и $-x$ — различные элементы множества $\mathbb{Z}_p$.
- Каждый элемент $x \in \mathbb{Z}_p \backslash \{0\}$ имеет единственный мультипликативный обратный $\overline{x} \in \mathbb{Z}_p \backslash \{0\}$, причем $x\overline{x} \equiv 1 \pmod p$.
  Из определения простых чисел следует, что отображение $\mathbb{Z}_p \to \mathbb{Z}_p$: $z \mapsto xz$, инъективно для любого $x \neq 0$. Поэтому на конечном множестве $\mathbb{Z}_p \backslash \{0\}$ оно должно быть также и сюръективным, вследствие чего для каждого $x \neq 0$ найдется единственный элемент $\overline{x}$, для которого $x\overline{x} \equiv 1 \pmod p$.
- Если $h = \lfloor \frac{p}{2} \rfloor$, то $0^2, 1^2, 2^2, \ldots, h^2$ — различные элементы множества $\mathbb{Z}_p$. Действительно, из сравнения $x^2 \equiv y^2$, т. е. $(x + y)(x - y) \equiv 0$, следует, что либо $x \equiv y$, либо $x \equiv -y$.
  Эти $1 + \lfloor \frac{p}{2} \rfloor$ элементов $0^2, 1^2, \ldots, h^2$ будем называть *квадратами в* $\mathbb{Z}_p$.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Сложение и умножение в $\mathbb{Z}_5$

Попутно заметим, что для *всех* простых чисел существуют решения сравнения $x^2+y^2\equiv -1\,(\mathrm{mod}\,p)$. Действительно, в $\mathbb{Z}_p$ существует $\lfloor \frac{p}{2}\rfloor+1$ различных квадратов x^2 и $\lfloor \frac{p}{2}\rfloor+1$ различных чисел вида $-(1+y^2)$. Эти два множества имеют непустое пересечение, так как $\mathbb{Z}_p$ состоит лишь из p элементов, поэтому должны существовать такие x и y, что $x^2\equiv -(1+y^2)\,(\mathrm{mod}\,p)$.

Лемма. *Никакое число вида $n=4m+3$ нельзя представить в виде суммы двух квадратов.*

■ **Доказательство.** Заметим, что квадрат любого четного числа есть $(2k)^2=4k^2\equiv 0\,(\mathrm{mod}\,4)$, а для квадратов нечетных чисел имеем $(2k+1)^2=4(k^2+k)+1\equiv 1\,(\mathrm{mod}\,4)$. Поэтому любая сумма квадратов сравнима по модулю 4 с 0, 1 или 2. □

Значит, простые $p=4m+3$ являются «плохими», так что далее мы будем заниматься свойствами «хороших» простых чисел вида $p=4m+1$. По пути к главной теореме следующее утверждение является ключевым.

Предложение. *Каждое простое число вида $p=4m+1$ есть сумма двух квадратов, т. е. его можно представить в виде $p=x^2+y^2$, где $x,y\in\mathbb{N}$ — некоторые натуральные числа.*

Мы приведем здесь два доказательства этого предложения; каждое из них элегантно и неожиданно. Первое доказательство основано на поразительном применении «принципа Дирихле», который мы уже неявно использовали перед леммой 4 (дополнительно см. гл. 25), и тонких переходах к рассуждениям «по модулю p» и обратно. Его идея принадлежит норвежскому теоретико-числовику Акселю Туэ [6].

■ **Доказательство.** Рассмотрим такие пары (x',y') целых чисел, что $0\le x',y'\le\sqrt{p}$, т. е. $x',y'\in\{0,1,\ldots,\lfloor\sqrt{p}\rfloor\}$. Их число равно $(\lfloor\sqrt{p}\rfloor+1)^2$; так как $\lfloor x\rfloor+1>x$ при $x=\sqrt{p}$, то это число больше p. Следовательно, для любого $s\in\mathbb{Z}_p$ значения $x'-sy'$, полученные с помощью всех пар (x',y'), не могут быть попарно различными по модулю p. Иначе говоря, для каждого s существуют две различные пары

$$(x',y'),\ (x'',y'')\quad\in\quad\{0,1,\ldots,\lfloor\sqrt{p}\rfloor\}^2,$$

для которых

$$x'-sy'\quad\equiv\quad x''-sy''\ \ (\mathrm{mod}\,p).$$

Теперь рассмотрим разности этих пар. Из последнего сравнения следует, что $x'-x''\equiv s(y'-y'')\ (\mathrm{mod}\,p)$. Поэтому, полагая

$$x:=|x'-x''|,\quad y:=|y'-y''|,$$

мы получим пару

$$(x,y)\in\{0,1,\ldots,\lfloor\sqrt{p}\rfloor\}^2,\quad\text{где}\quad x\equiv\pm sy\ (\mathrm{mod}\,p).$$

Одновременно x и y не могут быть нулями, так как пары (x',y') и (x'',y'') различны.

Пусть теперь s — решение сравнения $s^2\equiv -1\ (\mathrm{mod}\,p)$, которое существует в силу леммы 4. Тогда $x^2\equiv s^2y^2\equiv -y^2\ (\mathrm{mod}\,p)$, и, следовательно, мы построили пару

$$(x,y)\in\mathbb{Z}^2,\quad\text{для которой}\quad 0<x^2+y^2<2p\quad\text{и}\quad x^2+y^2\equiv 0\ (\mathrm{mod}\,p).$$

Для $p=13$, $\lfloor\sqrt{p}\rfloor=3$ рассмотрим пару $(x',y')\in\{0,1,2,3\}$. Для $s=5$ сумма $x'-sy'\,(\mathrm{mod}\,13)$ принимает следующие значения:

x' \ y'	0	1	2	3
0	0	8	3	11
1	1	9	4	12
2	2	10	5	0
3	3	11	6	1

Но p — единственное число, заключенное между 0 и $2p$, которое делится на p. Поэтому $x^2 + y^2 = p$. Доказано! □

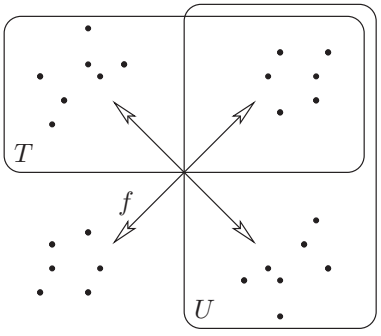
Второе доказательство предложения — также несомненное Доказательство из Книги — было открыто Роджером Хит-Броуном в 1971 году и опубликовано в 1984 году [2]. (Сжатая версия доказательства в виде «одного предложения» была предложена Доном Загиром, см. [8].) Оно настолько элементарно, что нам даже не придется использовать лемму 4.

Важную роль в доказательстве Хит-Броуна играют три линейные инволюции: одна совершенно очевидная, одна скрытая инволюция и одна тривиальная, которая ставит финальную точку. Вторая, неожиданная, инволюция соответствует скрытой структуре на множестве S целочисленных решений уравнения $4xy + z^2 = p$.

■ **Доказательство.** Рассмотрим множество решений

$$S \;:=\; \{(x, y, z) \in \mathbb{Z}^3 : 4xy + z^2 = p, \quad x > 0, \quad y > 0\}.$$

Оно конечно. Действительно, из условий $x \geq 1$ и $y \geq 1$ следует, что $y \leq \frac{p}{4}$ и $x \leq \frac{p}{4}$. Поэтому существует лишь конечное число возможных значений x и y, а при заданных x и y — не более двух значений z.



1. Первая — линейная — инволюция есть

$$f : S \longrightarrow S, \quad (x, y, z) \longmapsto (y, x, -z);$$

она переставляет x и y и меняет знак z. Ясно, что f отображает S в себя и является *инволюцией*: примененная дважды, она дает тождественное отображение. Далее, f не имеет неподвижных точек, так как равенство $z = 0$ имело бы следствием $p = 4xy$, что невозможно. Более того, f отображает решения, принадлежащие множеству

$$T \;:=\; \{(x, y, z) \in S : z > 0\},$$

в решения из $S\backslash T$, для которых $z < 0$. Далее, f обращает знаки $x - y$ и z и, следовательно, отображает решения, принадлежащие множеству

$$U \;:=\; \{(x, y, z) \in S : (x - y) + z > 0\},$$

в решения из $S\backslash U$. Чтобы убедиться в этом, достаточно проверить, что отсутствуют решения с $(x - y) + z = 0$. Но последнее равенство невозможно, так как из него следовало бы, что $p = 4xy + z^2 = 4xy + (x-y)^2 = (x + y)^2$.

Что мы получили, изучая инволюцию f? Заметим, что f отображает множества T и U в их дополнения; поэтому она переводит элементы из $T\backslash U$ в $U\backslash T$. Значит, число решений в U, не принадлежащих T, равно числу решений в T, не принадлежащих U. *Следовательно, T и U имеют одинаковую мощность.*

2. Вторая инволюция, которую мы рассмотрим, есть инволюция на множестве U:

$$g : U \longrightarrow U, \quad (x, y, z) \longmapsto (x - y + z, y, 2y - z).$$

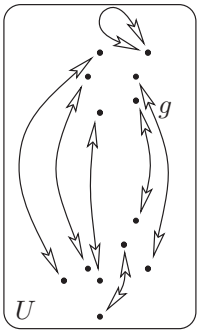
Вначале проверим, что g отображает U в U. Если $(x, y, z) \in U$, то $x - y + z > 0, y > 0$ и $4(x-y+z)y + (2y-z)^2 = 4xy + z^2$, так что $g(x, y, z) \in S$. Так как $(x-y+z) - y + (2y-z) = x > 0$, то действительно $g(x, y, z) \in U$.

Далее, g — инволюция: точка $g(x,y,z) = (x-y+z, y, 2y-z)$ под действием g переходит в $((x-y+z)-y+(2y-z), y, 2y-(2y-z)) = (x,y,z)$.

И, наконец, g имеет ровно одну неподвижную точку: если

$$(x,y,z) \quad = \quad g(x,y,z) \quad = \quad (x-y+z, y, 2y-z),$$

то $y = z$, и тогда $p = 4xy + y^2 = (4x+y)y$, что может выполняться только при $y = 1 = z$ и $x = \frac{p-1}{4}$.



Но если g — инволюция на U, которая имеет ровно одну неподвижную точку, то *мощность U нечетна*.

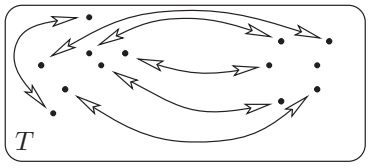
3. Третья инволюция действует на T тривиально, переставляя x и y:

$$h : T \longrightarrow T, \quad (x,y,z) \longmapsto (y,x,z).$$

Ясно, что это определение корректно и что h является инволюцией.

Объединим полученные результаты. Мощность множества T равна мощности множества U, которая нечетна. Но любая инволюция h на конечном множестве нечетной мощности имеет *неподвижную точку*: существует точка $(x,y,z) \in T$ с $x = y$, а ей соответствует целочисленное решение уравнения

$$p = 4x^2 + z^2 = (2x)^2 + z^2. \qquad \square$$



Инволюция на конечном множестве нечетной мощности имеет не менее одной неподвижной точки.

Заметим, что из приведенного доказательства следует большее: число представлений p в виде $p = x^2 + (2y)^2$ *нечетно* для всех простых чисел вида $p = 4m+1$. (На самом деле такое представление единственно, см. [3].) Заметим также, что оба доказательства не эффективны: попробуйте найти x и y для десятиразрядного простого числа! Эффективные способы поиска таких представлений (в частности, в виде суммы двух квадратов) обсуждаются в [1] и [7].

Следующая теорема полностью отвечает на вопрос, с которого началась эта глава.

Теорема. *Натуральное число n можно представить в виде суммы двух квадратов тогда и только тогда, когда в каноническом разложении n на простые сомножители каждый простой множитель вида $p = 4m+3$ имеет четную степень.*

■ **Доказательство.** Назовем число n *представимым*, если оно есть сумма двух квадратов, т. е. если $n = x^2 + y^2$ для некоторых $x, y \in \mathbb{N}_0 = \{0, 1, 2, \ldots\}$. Теорема вытекает из следующих пяти предложений.

(1) Числа $1 = 1^2 + 0^2$ и $2 = 1^2 + 1^2$ представимы. Каждое простое число вида $p = 4m+1$ представимо.

(2) Произведение двух любых представимых чисел $n_1 = x_1^2 + y_1^2$ и $n_2 = x_2^2 + y_2^2$ представимо: $n_1 n_2 = (x_1x_2 + y_1y_2)^2 + (x_1y_2 - x_2y_1)^2$.

(3) Если n представимо: $n = x^2 + y^2$, то представимо также и число $nz^2 = (xz)^2 + (yz)^2$.

Из (1), (2) и (3) следует достаточность условий теоремы.

(4) Если $p = 4m + 3$ — простое, которое делит представимое число $n = x^2 + y^2$, то p делит и x, и y, и поэтому n делится на p^2. Действительно, если $x \not\equiv 0 \pmod p$, то существует такое $\overline{x}$, что $x\overline{x} \equiv 1 \pmod p$. Умножив сравнение $x^2 + y^2 \equiv 0$ на $\overline{x}^2$, мы получили бы $1 + y^2\overline{x}^2 = 1 + (\overline{x}y)^2 \equiv 0 \pmod p$, что для простых вида $p = 4m+3$ в силу леммы 4 невозможно.

(5) Если n представимо и $p = 4m + 3$ делит n, то p^2 делит n и $\frac{n}{p^2}$ представимо. Это следует из (4) и завершает доказательство. □

Завершим наше обсуждение двумя замечаниями.

- Если a и b — два натуральных взаимно простых числа, то существует бесконечно много простых вида $am + b$ ($m \in \mathbb{N}$) — это известная (и трудная) теорема Дирихле. Точнее, можно показать, что количество простых $p \le x$ вида $p = am + b$ при больших x довольно точно описывается функцией $\frac{1}{\varphi(a)} \frac{x}{\log x}$, где $\varphi(a)$ — количество чисел b, $1 \le b < a$, взаимно простых с a. (Это существенно уточняет теорему о распределении простых чисел, которую мы обсуждали на с. 18.)
- Таким образом, для фиксированного a и разных b простые числа встречаются одинаково часто. Однако, например, при $a = 4$ доля простых чисел вида $4m + 3$ незначительно, но заметно и устойчиво превышает долю простых чисел вида $4m + 1$: для случайно выбранного большого x количество простых $p \le x$ вида $p = 4m + 3$, скорее всего, будет больше количества простых вида $p = 4m+1$. Этот эффект известен как «смещение Чебышёва» — см. Райзел [4], Рубинштейн и Сарнак [5].

Литература

[1] Clarke F. W., Everitt F. W., Littlejohn L. L., Vorster S. J. R. *H. J. S. Smith and the Fermat Two Squares Theorem.* Amer. Math. Monthly, **106** (1999), 652–665.

[2] Heath-Brown D. R. *Fermat's two squares theorem.* Invariant, (1984), 2–5.

[3] Niven I., Zuckerman H. S. *An Introduction to the Theory of Numbers.* Fifth edition, Wiley, New York, 1972.

[4] Riesel H. *Prime Numbers and Computer Methods for Factorization.* Second edition, Progress in Mathematics, **126**, Birkhäuser, Boston MA, 1994.

[5] Rubinstein M., Sarnak P. *Chebyshev's bias.* Experimental Mathematics, **3** (1994), 173–197.

[6] Thue A. *Et par antydninger til en taltheoretisk metode.* Kra. Vidensk. Selsk. Forh., **7** (1902), 57–75.

[7] Wagon S. *Editor's corner: The Euclidean algorithm strikes again.* Amer. Math. Monthly, **97** (1990), 125–129.

[8] Zagier D. *A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares.* Amer. Math. Monthly, **97** (1990), 144.

Глава 5 Закон взаимности квадратичных вычетов

Карл Фридрих Гаусс

Какая известная математическая теорема доказывалась чаще всего? Конечно, хорошими претендентами являются теорема Пифагора и основная теорема алгебры. Но чемпионом является закон взаимности квадратичных вычетов в теории чисел. В замечательной монографии Франца Леммермейера [5] перечислено не менее 196 доказательств, предложенных до 2000 г. Конечно, многие из них различаются лишь деталями, но перечень разных идей производит глубокое впечатление, как и список их авторов. Карл Фридрих Гаусс предложил в 1801 году первое полное доказательство, к которому потом добавил еще семь. Немного позднее Фердинанд Готтхолд Эйзенштейн предложил еще пять доказательств, а непрерывно обновляющийся список авторов выглядит как «Кто есть Кто в математике».

Ввиду большого числа доказательств вопрос о том, какое из них записано в Книге, не имеет простого ответа. Находится там самое короткое, самое неожиданное, или это доказательство, наиболее пригодное для обобщений на другие и более глубокие законы взаимности? Мы выбрали два доказательства, основанные на третьем и шестом доказательствах Гаусса. Первое из них, возможно, самое простое и приятное, а другое является отправной точкой для фундаментальных результатов в более общих структурах.

Как и в предыдущей главе, мы будем работать по «модулю p», где p — простое нечетное число. Пусть $\mathbb{Z}_p$ — поле вычетов по модулю p; обычно (но не всегда) будем отождествлять его с множеством $\{0, 1, \ldots, p-1\}$. Рассмотрим некоторое $a \not\equiv 0 \pmod p$, т. е. $p \nmid a$. Назовем такое a *квадратичным вычетом* по модулю p, если $a \equiv b^2 \pmod p$ для некоторого b из $\mathbb{Z}_p$, и *квадратичным невычетом* в противном случае. Следовательно, квадратичными вычетами являются числа $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ и поэтому имеется $\frac{p-1}{2}$ квадратичных вычетов и $\frac{p-1}{2}$ квадратичных невычетов. Действительно, если $i^2 \equiv j^2 \pmod p$, где $1 \le i, j \le \frac{p-1}{2}$, то $p \mid i^2 - j^2 = (i-j)(i+j)$. Так как $2 \le i + j \le p - 1$, то $p \mid i - j$, т. е. $i \equiv j \pmod p$.

Для $p = 13$ квадратичными вычетами являются $1 \equiv 1^2$, $4 \equiv 2^2$, $9 \equiv 3^2$, $3 \equiv 4^2$, $12 \equiv 5^2$ и $10 \equiv 6^2$, а невычетами являются 2, 5, 6, 7, 8, 11.

Удобно ввести так называемый *символ Лежандра*. Пусть $a \not\equiv 0 \pmod p$. Тогда

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{если } a - \text{квадратичный вычет,} \\ -1, & \text{если } a - \text{квадратичный невычет.} \end{cases}$$

История начинается с «*малой теоремы Ферма*»:
Если $a \not\equiv 0 \pmod p$), то

$$a^{p-1} \equiv 1 \pmod p. \tag{1}$$

В самом деле, так как $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ — группа по умножению, множество

$$\{1a, 2a, \ldots, (p-1)a\}$$

состоит из всех ненулевых вычетов:

$$(1a)(2a)(3a)\cdots((p-1)a) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p};$$

разделив левую и правую части этого сравнения на $(p-1)!$, мы получим $a^{p-1} \equiv 1 \pmod{p}$.

Другими словами, все ненулевые вычеты по модулю p являются корнями многочлена $x^{p-1} - 1 \in \mathbb{Z}_p[x]$.[1] Далее заметим, что

$$x^{p-1} - 1 = (x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1).$$

Пусть $a \equiv b^2 \pmod{p}$ — квадратичный вычет. Тогда по малой теореме Ферма $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}$. Поэтому квадратичные вычеты являются в точности корнями первого множителя $x^{\frac{p-1}{2}} - 1$, так что $\frac{p-1}{2}$ невычетов должны быть корнями второго множителя $x^{\frac{p-1}{2}} + 1$. Сравнивая этот вывод с определением символа Лежандра, мы получаем следующий важный инструмент для его нахождения.

Критерий Эйлера. *Для* $a \not\equiv 0 \pmod{p}$

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Это немедленно дает нам важное *правило умножения*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right), \tag{2}$$

которое очевидным образом вытекает из критерия Эйлера. Правило умножения чрезвычайно полезно при вычислении символов Лежандра. Так как любое целое есть произведение ± 1 и простых чисел, мы должны найти только $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ и $\left(\frac{q}{p}\right)$ для простых нечетных q.

Согласно критерию Эйлера $\left(\frac{-1}{p}\right) = 1$, если $p \equiv 1 \pmod{4}$, и $\left(\frac{-1}{p}\right) = -1$, если $p \equiv 3 \pmod{4}$. Кое-что мы уже узнали в предыдущей главе. Случай $\left(\frac{2}{p}\right)$ вытекает из леммы Гаусса (см. ниже): $\left(\frac{2}{p}\right) = 1$, если $p \equiv \pm 1 \pmod{8}$, в то время как $\left(\frac{2}{p}\right) = -1$, если $p \equiv \pm 3 \pmod{8}$.

Например, для $p = 17$ и $a = 3$ имеем: $3^8 = (3^4)^2 = 81^2 \equiv (-4)^2 \equiv -1 \pmod{17}$, в то время как для $a = 2$ получаем $2^8 = (2^4)^2 \equiv (-1)^2 \equiv 1 \pmod{17}$. Следовательно, 2 — квадратичный вычет, а 3 — невычет.

Гаусс проделал большое количество вычислений с квадратичными вычетами. В частности, он исследовал вопрос о существовании зависимости между условиями «q — квадратичный вычет по модулю p» и «p — квадратичный вычет по модулю q», когда p и q — нечетные

[1] Символ $\mathbb{Z}_p[x]$ обозначает множество всех многочленов от x с коэффициентами из $\mathbb{Z}_p$. — *Прим. ред.*

простые числа. После множества экспериментов он сформулировал, а затем доказал следующее утверждение.

Закон взаимности квадратичных вычетов. *Пусть p и q — нечетные простые числа. Тогда*

$$\left(\frac{q}{p}\right)\left(\frac{p}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Например, $\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{-1}{p}\right) = -1$, так что 3 — невычет по модулю 17.

Если $p \equiv 1 \pmod 4$ или $q \equiv 1 \pmod 4$, то $\frac{p-1}{2}$ (соответственно, $\frac{q-1}{2}$) четно и потому $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1$, так что $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$. Если же $p = q \equiv 3 \pmod 4$, то мы имеем $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ и, следовательно, для нечетных простых чисел мы получаем равенство $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ за исключением случая, когда *оба* числа p и q сравнимы с 3 по модулю 4.

■ **Первое доказательство.** Ключ к нашему первому доказательству (оно у Гаусса третье) — вычислительная формула, которую вскоре стали называть *леммой Гаусса*.

Лемма Гаусса. *Пусть $a \not\equiv 0 \pmod p$. Рассмотрим числа $1a, 2a, \ldots, \frac{p-1}{2}a$ и приведем их по модулю p к системе вычетов с наименьшими абсолютными значениями: $ia \equiv r_i \pmod p$, где $-\frac{p-1}{2} \le r_i \le \frac{p-1}{2}$ для всех i. Тогда*

$$\left(\frac{a}{p}\right) = (-1)^s, \text{ где } s = \#\{i : r_i < 0\}.$$

■ **Доказательство.** Допустим, что $u_1, \ldots, u_s$ — вычеты, меньшие нуля, а $v_1, \ldots, v_{\frac{p-1}{2}-s}$ — вычеты, большие нуля. Тогда числа $-u_1, \ldots, -u_s$ лежат между 1 и $\frac{p-1}{2}$ и все отличны от $v_1, \ldots, v_{\frac{p-1}{2}-s}$ (см. замечание на полях).

Если $-u_i = v_j$, то $u_i + v_j \equiv 0 \pmod p$. Из условий $u_i \equiv ka$, $v_j \equiv la \pmod p$ следует, что $p \mid (k+l)a$. Поскольку p и a взаимно просты, p должно делить $k + l$, что невозможно, так как $k + l \le p - 1$.

Поэтому $\{-u_1, \ldots, -u_s, v_1, \ldots, v_{\frac{p-1}{2}-s}\} = \{1, 2, \ldots, \frac{p-1}{2}\}$. Следовательно,

$$\prod_i (-u_i) \prod_j v_j = \tfrac{p-1}{2}!,$$

откуда вытекает, что

$$(-1)^s \prod_i u_i \prod_j v_j \equiv \tfrac{p-1}{2}! \pmod p.$$

Теперь вспомним, как были получены числа u_i и v_j: они являются вычетами чисел $1a, 2a, \ldots, \frac{p-1}{2}a$. Таким образом,

$$\frac{p-1}{2}! \equiv (-1)^s \prod_i u_i \prod_j v_j \equiv (-1)^s \, \tfrac{p-1}{2}! \, a^{\frac{p-1}{2}} \pmod{p}.$$

Сокращая на $\frac{p-1}{2}!$ и используя критерий Эйлера, получаем равенство

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^s \pmod{p},$$

и поэтому ввиду нечетности p находим $\left(\frac{a}{p}\right) = (-1)^s$. □

Используя лемму, мы можем легко вычислить $\left(\frac{2}{p}\right)$. Ввиду того, что все числа $1 \cdot 2, 2 \cdot 2, \ldots, \frac{p-1}{2} \cdot 2$ заключены между 1 и $p-1$, имеем

$$s = \#\left\{i : \tfrac{p-1}{2} < 2i \le p-1\right\} = \tfrac{p-1}{2} - \#\left\{i : 2i \le \tfrac{p-1}{2}\right\} = \left\lceil \tfrac{p-1}{4} \right\rceil.$$

Легко проверить, что s четно только для $p = 8k \pm 1$.

Лемма Гаусса служит основой многих опубликованных доказательств закона квадратичной взаимности. Возможно, наиболее элегантным является доказательство, которое предложил Фердинанд Готтхолд Эйзенштейн [2]. Он изучал теорию чисел по знаменитому труду Гаусса Disquisitiones Arithmeticae [6*] и успел внести важный вклад в «высшие теоремы взаимности» до своей безвременной кончины в возрасте 29 лет. Его доказательство заключается в точном подсчете числа точек решетки!

Пусть p и q — простые нечетные числа; рассмотрим символ Лежандра $\left(\frac{q}{p}\right)$. Пусть кратное iq простого q имеет, как в лемме Гаусса, отрицательный вычет $r_i < 0$ по модулю p. Это означает, что существует единственное целое j, для которого $-\frac{p}{2} < iq - jp < 0$. Заметим, что $0 < j < \frac{q}{2}$, так как $0 < i < \frac{p}{2}$. Другими словами, $\left(\frac{q}{p}\right) = (-1)^s$, где s — число точек (x, y) решетки, т. е. число пар целых чисел x, y, удовлетворяющих неравенствам

$$0 < py - qx < \frac{p}{2}, \quad 0 < x < \frac{p}{2}, \quad 0 < y < \frac{q}{2}. \tag{3}$$

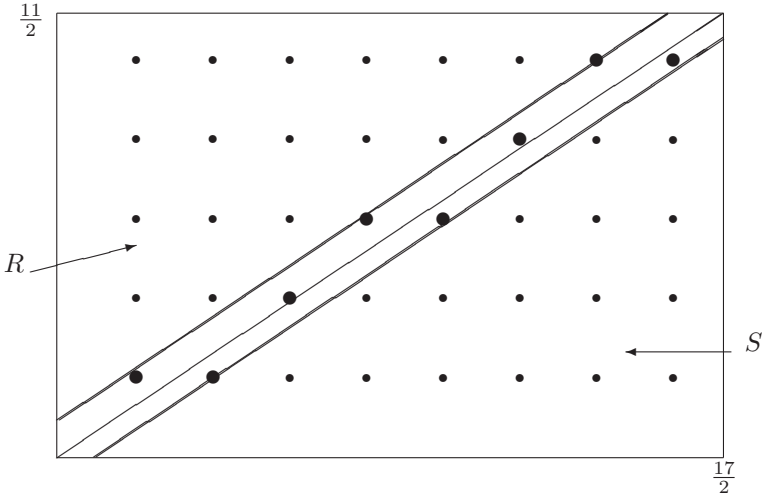
Аналогично $\left(\frac{p}{q}\right) = (-1)^t$, где t — число точек (x, y) решетки, для которых выполняются условия

$$0 < qx - py < \frac{q}{2}, \quad 0 < x < \frac{p}{2}, \quad 0 < y < \frac{q}{2}. \tag{4}$$

Теперь рассмотрим прямоугольник со сторонами длин $\frac{p}{2}$ и $\frac{q}{2}$. Проведем две прямые, параллельные диагонали $py = qx$: прямую $y = \frac{q}{p}x + \frac{1}{2}$, или $py - qx = \frac{p}{2}$, и, соответственно, $y = \frac{q}{p}(x - \frac{1}{2})$, или $qx - py = \frac{q}{2}$.

Ниже на чертеже изображен случай $p = 17, q = 11$.

$p = 17 \quad q = 11$
$s = 5 \quad t = 3$
$\left(\frac{q}{p}\right) = (-1)^5 = -1$
$\left(\frac{p}{q}\right) = (-1)^3 = -1$



Доказательство теперь несложно завершить с помощью следующих трех наблюдений.

1. На диагонали и на обеих параллельных прямых точек решетки нет, так как из равенства $py = qx$ вытекает, что $p \mid x$, а это невозможно. Относительно параллельных заметим, что $py - qx$ — целое число, в то время как $\frac{p}{2}$ и $\frac{q}{2}$ целыми не являются.

2. Точки решетки, для которых выполняются условия (3), являются в точности точками, расположенными в верхней полосе $0 < py - qx < \frac{p}{2}$. Точки, которые удовлетворяют неравенствам (4), находятся в нижней полосе $0 < qx - py < \frac{q}{2}$. Поэтому число точек решетки в обеих полосах равно $s + t$.

3. Две другие области, а именно, $R : py - qx > \frac{p}{2}$ и $S : qx - py > \frac{q}{2}$, содержат *одно и то же* число точек. Чтобы убедиться в этом, рассмотрим отображение $\varphi : R \longrightarrow S$, которое переводит точку (x, y) в $(\frac{p+1}{2} - x, \frac{q+1}{2} - y)$; легко проверить, что φ взаимно однозначно.

Поскольку общее число точек решетки в прямоугольнике равно $\frac{p-1}{2} \cdot \frac{q-1}{2}$, мы приходим к выводу, что $s + t$ и $\frac{p-1}{2} \cdot \frac{q-1}{2}$ имеют одинаковую четность и что поэтому

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{s+t} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

□

■ **Второе доказательство.** Во втором выбранном нами доказательстве вместо леммы Гаусса используются так называемые «суммы Гаусса» в конечных полях. Гаусс изобрел их при исследованиях уравнения $x^p - 1 = 0$ и арифметических свойств поля $\mathbb{Q}(\zeta)$ (которое называют *цикломатическим*), где ζ — корень p-й степени из единицы. Они послужили отправной точкой в поиске высших законов взаимности в общих числовых полях.

Приведем сначала несколько свойств конечных полей.

A. Пусть p и q — различные простые нечетные числа. Рассмотрим конечное поле F, содержащее q^{p-1} элементов. Его простое поле есть $\mathbb{Z}_q$, поэтому $qa = 0$ для любого $a \in F$. Отсюда следует, что $(a+b)^q = a^q + b^q$, так как все биномиальные коэффициенты $\binom{q}{i}$ с $0 < i < q$ кратны q и поэтому соответствующие слагаемые $\binom{q}{i}a^i b^{q-i}$ равны нулю в F. Отметим, что критерий Эйлера можно записать в виде равенства $\left(\frac{p}{q}\right) = p^{\frac{q-1}{2}}$ в конечном поле $\mathbb{Z}_q$.

B. Мультипликативная группа $F^* = F \setminus \{0\}$ является циклической порядка $q^{p-1} - 1$ (см. вставку на следующей странице). Согласно малой теореме Ферма p есть делитель числа $q^{p-1} - 1$, поэтому существует элемент $\zeta \in F$ порядка p, т. е. $\zeta^p = 1$, и ζ порождает подгруппу $\{\zeta, \zeta^2, \dots, \zeta^p = 1\}$ группы F^*. Заметим, что ζ^i при любом $i \not\equiv p$ тоже порождает эту подгруппу. Следовательно, мы получаем разложение многочлена: $x^p - 1 = (x - \zeta)(x - \zeta^2)\dots(x - \zeta^p)$.

Теперь мы можем начать доказательство. Рассмотрим *сумму Гаусса*

$$G := \sum_{i=1}^{p-1} \left(\frac{i}{p}\right)\zeta^i \in F,$$

где $\left(\frac{i}{p}\right)$ — символ Лежандра. Чтобы доказать закон взаимности, мы получим и затем приравняем два различных выражения для G^q.

Первое выражение. Мы имеем

$$G^q = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right)^q \zeta^{iq} = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right)\zeta^{iq} = \left(\frac{q}{p}\right)\sum_{i=1}^{p-1} \left(\frac{iq}{p}\right)\zeta^{iq} = \left(\frac{q}{p}\right)G, \qquad (5)$$

Пример: положим $p = 3, q = 5$. Тогда $G = \zeta - \zeta^2$ и $G^5 = \zeta^5 - \zeta^1 0 = \zeta^2 - \zeta = -(\zeta - \zeta^2) = -G$, что согласуется с тем, что $\left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$.

где первое равенство следует из тождества $(a+b)^q = a^q + b^q$, второе — из равенства $\left(\frac{i}{p}\right)^q = \left(\frac{i}{p}\right)$ (поскольку q нечетно), третье — из формулы (2), согласно которой $\left(\frac{i}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{iq}{p}\right)$, а последнее имеет место в силу того, что iq пробегает вместе с i все ненулевые вычеты по модулю p.

Второе выражение. Если использовать формулу

$$G^2 = (-1)^{\frac{p-1}{2}} p, \qquad (6)$$

то доказательство легко завершается. Действительно,

$$G^q = G\big(G^2\big)^{\frac{q-1}{2}} = G(-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}} = G\left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \qquad (7)$$

Приравнивая выражения (5) и (7) и сокращая на величину G, которая согласно (6) не равна нулю, мы находим, что $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, следовательно,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Мультипликативная группа конечного поля — циклическая

Пусть F^* — мультипликативная группа конечного поля F и $|F^*| = n$. Обозначим через $\mathrm{ord}(a)$ порядок элемента a, т. е. наименьшее натуральное число k, при котором $a^k = 1$. Мы хотим найти такой элемент $a \in F^*$, что $\mathrm{ord}(a) = n$. Если $\mathrm{ord}(b) = d$, то по теореме Лагранжа d делит n (см. вставку на полях в гл. 1). Группируя элементы в соответствии с их порядками, получаем равенство

$$n = \sum_{d|n} \psi(d), \quad \text{где} \quad \psi(d) = \#\{b \in F^* : \mathrm{ord}(b) = d\}. \tag{8}$$

Если $\mathrm{ord}(b) = d$, то каждый элемент b^i $(i = 1, \ldots, d)$ удовлетворяет равенству $(b^i)^d = 1$ и, следовательно, является корнем многочлена $x^d - 1$. Но, поскольку F — поле, $x^d - 1$ имеет не более d корней, значит, $b, b^2, \ldots, b^d = 1$ и являются этими корнями. В частности, каждый элемент порядка d имеет вид b^i.
С другой стороны, легко проверить, что $\mathrm{ord}(b^i) = \frac{d}{(i,d)}$, где (i, d) — наибольший общий делитель i и d. Поэтому $\mathrm{ord}(b^i) = d$ тогда и только тогда, когда $(i, d) = 1$, т. е. когда i и d взаимно просты. Используя *функцию Эйлера*

$$\varphi(d) = \#\{i : 1 \le i \le d,\ (i, d) = 1\},$$

находим, что $\psi(d) = \varphi(d)$ всякий раз, когда $\psi(d) > 0$. Учитывая (8), находим

$$n = \sum_{d|n} \psi(d) \le \sum_{d|n} \varphi(d).$$

Но поскольку, как мы докажем далее,

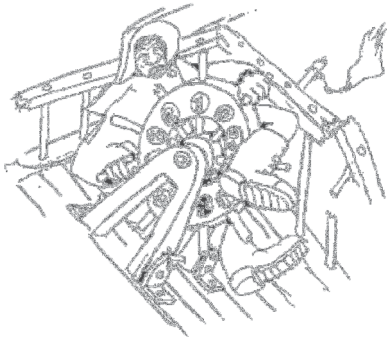
$$\sum_{d|n} \varphi(d) = n, \tag{9}$$

равенство $\psi(d) = \varphi(d)$ должно выполняться для всех d. В частности, $\psi(n) = \varphi(n) \ge 1$, и поэтому элемент порядка n существует.

Следующее (фольклорное) доказательство формулы (9) тоже входит в Книгу. Рассмотрим n дробей

$$\tfrac{1}{n}, \tfrac{2}{n}, \ldots, \tfrac{k}{n}, \ldots, \tfrac{n}{n},$$

приведем их к несократимому виду $\frac{k}{n} = \frac{i}{d}$, где $1 \le i \le d$, $(i, d) = 1$, $d \mid n$, и заметим, что знаменатель d среди этих n сокращенных дробей встречается точно $\varphi(d)$ раз.



«Даже в абсолютном хаосе мы можем зацепиться за циклическую группу»

Остается проверить справедливость формулы (6). С этой целью сделаем вначале два простых замечания.

- $\sum_{i=1}^{p}\zeta^i = 0$ и, значит, $\sum_{i=1}^{p-1}\zeta^i = -1$. Действительно, сумма $-\sum_{i=1}^{p}\zeta^i$ совпадает с коэффициентом при x^{p-1} в разложении $x^p - 1 = \prod_{i=1}^{p}(x-\zeta^i)$ и поэтому равна нулю.
- $\sum_{k=1}^{p-1}\left(\frac{k}{p}\right) = 0$ и, следовательно, $\sum_{k=1}^{p-2}\left(\frac{k}{p}\right) = -\left(\frac{-1}{p}\right)$, так как числа квадратичных вычетов и невычетов одинаковы.

Справедливо равенство

$$G^2 = \Big(\sum_{i=1}^{p-1}\Big(\frac{i}{p}\Big)\zeta^i\Big)\Big(\sum_{j=1}^{p-1}\Big(\frac{j}{p}\Big)\zeta^j\Big) = \sum_{i,j}\Big(\frac{ij}{p}\Big)\zeta^{i+j}.$$

Положив $j \equiv ik \pmod p$, мы получим

$$G^2 = \sum_{i,k}\Big(\frac{k}{p}\Big)\zeta^{(1+k)i} = \sum_{k=1}^{p-1}\Big(\frac{k}{p}\Big)\sum_{i=1}^{p-1}\zeta^{(1+k)i}.$$

Сумма слагаемых в правой части, соответствующих $k = p-1 \equiv -1 \pmod p$, равна $\left(\frac{-1}{p}\right)(p-1)$, так как в этом случае $\zeta^{1+k} = 1$.

Поэтому

Критерий Эйлера: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

$$G^2 = \Big(\frac{-1}{p}\Big)(p-1) + \sum_{k=1}^{p-2}\Big(\frac{k}{p}\Big)\sum_{i=1}^{p-1}\zeta^{(1+k)i}. \qquad (10)$$

Так как ζ^{1+k} при $k \neq p-1$ является порождающим элементом подгруппы, то согласно нашему первому замечанию внутренние суммы по i в (10)для всех $k \neq p-1$ равны $\sum_{i=1}^{p-1}\zeta^i = -1$. Поэтому в силу нашего второго замечания двойная сумма в правой части (10) есть $-\sum_{k=1}^{p-2}\left(\frac{k}{p}\right) = \left(\frac{-1}{p}\right)$. Отсюда следует,что $G^2 = \left(\frac{-1}{p}\right)p$ и, так как по критерию Эйлера $G^2 = (-1)^{\frac{p-1}{2}}$, то доказательство завершено. □

Для $p=3$, $q=5$, $G^2 = (\zeta-\zeta^2)^2 = \zeta^2 - 2\zeta^3 + \zeta^4 = \zeta^2 - 2 + \zeta = -3 = (-1)^{\frac{p-1}{2}}$, так как $1+\zeta+\zeta^2 = 0$.

Литература

[1] Baker A. *A Concise Introduction to the Theory of Numbers.* Cambridge University Press, Cambridge, 1984.

[2] Eisenstein F.G. *Geometrischer Beweis des Fundamentaltheorems für die quadratischen Reste,* J. Reine Angewandte Mathematik, **28** (1844), 186–191.

[3] Gauss C.F. *Theorema arithmetici demonstratio nova,* Comment. Soc. regiae sci. Göttingen, **XVI** (1808), 69; Werke II, 1-8 (Содержит третье доказательство).

[4] Gauss C.F. *Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et amplicationes novae (1818),* Werke II, 47-64 (Содержит шестое доказательство.)

[5] Lemmermeyer F. *Reciprocity Laws: From Euler to Eisenstein,* Springer-Verlag, Berlin, 2000.

[6*] Gauss C.F. *Disquisitiones Arithmeticae,* Leipzig, 1801; (есть русский перевод: Гаусс К. Ф. *Труды по теории чисел*, Изд-во АН СССР, Москва, 1959).

Что происходит?

Я везу 196 доказательств
взаимности квадратичных вычетов

Каждое конечное кольцо с делением — поле

Глава 6

Кольца являются важными структурами в современной алгебре. Если кольцо R имеет мультипликативный единичный элемент 1 и каждый ненулевой элемент имеет мультипликативный обратный, то R называется *кольцом с делением*[1]. Единственное, чем такое кольцо R может отличаться от поля, — это коммутативность умножения. Известный пример некоммутативного кольца с делением — кольцо кватернионов, открытое Гамильтоном. Но, как видно из названия главы, каждое некоммутативное кольцо с делением бесконечно. Если R конечно, то из аксиом следует, что умножение в R коммутативно.

Этот результат, который теперь является классическим, поразил воображение многих математиков; например, Херштейн назвал его «совершенно неожиданной взаимосвязью двух кажущихся далекими друг от друга вещей: числа элементов в некоторой алгебраической системе и свойств умножения в этой системе».

Эрнст Витт

Теорема. *Каждое конечное кольцо с делением коммутативно.*

Эту прекрасную теорему, которую обычно приписывают МакЛагану Веддербурну, доказывали многие математики с помощью различных идей. Сам Веддербурн в 1905 году [2] дал ей три доказательства. В том же году еще одно доказательство предложил Леонард Диксон [1]. Позднее Эмилем Артином, Хансом Цассенхаузом, Николаем Бурбаки и многими другими были получены разные доказательства. Одно из них выделяется своей простотой и элегантностью. Оно было найдено Эрнстом Виттом в 1931 году [3] и сочетает две элементарные идеи, приводящие к великолепному окончанию.

■ **Доказательство.** Первая часть доказательства связана с линейной алгеброй и теорией групп. Пусть R — конечное кольцо с делением. Для каждого элемента $s \in R$ определим множество $C_s := \{x \in R : xs = sx\}$ элементов из R, коммутирующих с s; множество C_s называется *централизатором* элемента s. Ясно, что C_s содержит 0 и 1 и является подкольцом с делением кольца R. *Центром* Z называется множество элементов из R, коммутирующих со всеми элементами из R, т. е. $Z = \bigcap_{s \in R} C_s$. В частности, все элементы из Z коммутируют друг с другом, 0 и 1 принадлежат Z и, следовательно, Z есть *конечное поле*. Положим $|Z| = q$.

Мы можем рассматривать R и C_s как векторные пространства над полем Z и отсюда вывести, что $|R| = q^n$, где n – размерность векторного пространства R над Z, и аналогично $|C_s| = q^{n_s}$ для некоторых целых чисел $n_s \geq 1$.

[1] В отечественной литературе обычно используется термин *тело*. Заметим, что авторы неявно предполагают также ассоциативность умножения. – *Прим. перев.*

Пусть теперь R — не поле. Это означает, что для *некоторого* $s \in R$ централизатор C_s не совпадает с R или, что то же, $n_s < n$.

Рассмотрим на множестве $R^* := R\backslash\{0\}$ отношение

$$r' \sim r \quad \Longleftrightarrow \quad r' = x^{-1}rx \quad \text{для некоторого } x \in R^*.$$

Легко проверить, что $\sim$ есть отношение эквивалентности. Пусть

$$A_s \;:=\; \{x^{-1}sx : x \in R^*\}$$

— класс эквивалентности, содержащий s. Заметим, что $|A_s| = 1$ только тогда, когда s принадлежит центру Z. Поэтому в силу нашего предположения существуют классы A_s с $|A_s| \geq 2$. Рассмотрим теперь для $s \in R^*$ отображение $f_s : x \longmapsto x^{-1}sx$ из R^* в A_s. Тогда для $x, y \in R^*$

$$\begin{aligned} x^{-1}sx = y^{-1}sy \quad &\Longleftrightarrow \quad (yx^{-1})s = s(yx^{-1}) \Longleftrightarrow \\ &\Longleftrightarrow \quad yx^{-1} \in C_s^* \quad \Longleftrightarrow \quad y \in C_s^* x, \end{aligned}$$

где $C_s^* = C_s\backslash\{0\}$, причем мощность множества $C_s^* x = \{zx : z \in C_s^*\}$ равна $|C_s^*|$. Следовательно, при отображении f_s каждый элемент $x^{-1}sx$ является образом ровно $|C_s^*| = q^{n_s} - 1$ элементов из R^*, и мы заключаем, что $|R^*| = |A_s|\,|C_s^*|$. Таким образом,

$$\frac{|R^*|}{|C_s^*|} \;=\; \frac{q^n - 1}{q^{n_s} - 1} \;=\; |A_s| \quad \text{есть } \textit{целое} \text{ число для всех } s.$$

Классы эквивалентности образуют разбиение R^*. Обозначим теперь через $Z^* = Z \setminus \{0\}$ объединение одноэлементных классов эквивалентности и через $A_1, \ldots, A_t$ — классы эквивалентности, содержащие более одного элемента. По нашему предположению $t \geq 1$. Равенство $|R^*| = |Z^*| + \sum_{k=1}^{t} |A_k|$ доказывает так называемую *формулу классов*

$$q^n - 1 \;=\; q - 1 + \sum_{k=1}^{t} \frac{q^n - 1}{q^{n_k} - 1}\,, \tag{1}$$

где $1 < \frac{q^n-1}{q^{n_k}-1} \in \mathbb{N}$ для всех k.

Теперь мы оставим абстрактную алгебру и вернемся к натуральным числам. Прежде всего покажем, что если $q^{n_k} - 1 \,|\, q^n - 1$, то $n_k \,|\, n$. В самом деле, пусть $n = an_k + r$, где $0 \leq r < n_k$. Из условия $q^{n_k} - 1 \,|\, q^{an_k+r} - 1$ вытекает, что

$$q^{n_k} - 1 \,|\, (q^{an_k+r} - 1) - (q^{n_k} - 1) = q^{n_k}(q^{(a-1)n_k+r} - 1),$$

и, следовательно, $q^{n_k} - 1 \,|\, q^{(a-1)n_k+r} - 1$, так как q^{n_k} и $q^{n_k} - 1$ взаимно просты. Продолжая таким образом, мы находим, что $q^{n_k} - 1 \,|\, q^r - 1$, где $0 \leq r < n_k$, что возможно только при $r = 0$, т. е. при $n_k \,|\, n$. Итак

$$n_k \,|\, n \quad \text{для всех } k. \tag{2}$$

Во второй части доказательства используются комплексные числа. Рассмотрим многочлен $x^n - 1$. Его (комплексные) корни называются *корнями n-й степени из единицы*. Так как $\lambda^n = 1$ для каждого корня λ,

то $|\lambda| = 1$, т. е. все они лежат на единичной окружности комплексной плоскости. Фактически (см. вставку) они имеют вид

$$\lambda_k = e^{\frac{2k\pi i}{n}} = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right),\ 0 \le k \le n-1.$$

Некоторые корни n-й степени λ удовлетворяют также соотношениям $\lambda^d = 1$ при $d < n$; например, при четном n для корня $\lambda = -1$ имеем $\lambda^2 = 1$. Для корня λ обозначим через d наименьшее натуральное число, при котором $\lambda^d = 1$, т. е. d — порядок λ в группе корней из единицы. Тогда $d \mid n$ согласно теореме Лагранжа («порядок любого элемента группы делит порядок группы» — см. вставку в гл. 1). Заметим, что существуют корни из единицы любого порядка n, например, $\lambda_1 = e^{\frac{2\pi i}{n}}$.

Корни из единицы

Любое комплексное число $z = x + iy$ можно записать в полярных координатах:

$$z \;=\; re^{i\varphi} \;=\; r(\cos\varphi + i\sin\varphi),$$

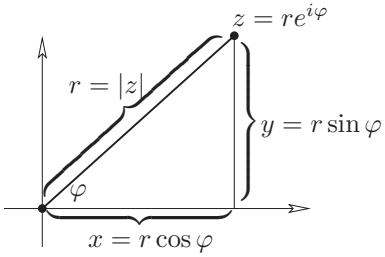
где $r = |z| = \sqrt{x^2 + y^2}$ — расстояние от точки z до начала координат и φ — угол, измеренный от положительного луча оси x. Корни n-й степени из единицы, следовательно, имеют вид

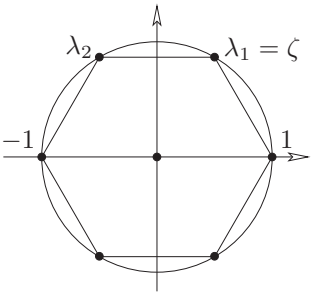
$$\lambda_k = e^{\frac{2k\pi i}{n}} = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right), \qquad 0 \le k \le n-1,$$

так как при любом k

$$\lambda_k^n = e^{2k\pi i} = \cos(2k\pi) + i\sin(2k\pi) = 1.$$

Можно получить эти корни геометрически, вписывая правильный n-угольник в единичный круг. Заметим, что для всех k выполняются соотношения $\lambda_k = \zeta^k$, где $\zeta = e^{\frac{2\pi i}{n}} = \lambda_1$. Таким образом, корни n-й степени из единицы образуют циклическую группу $\{\zeta, \zeta^2, \ldots, \zeta^{n-1}, \zeta^n = 1\}$ порядка n.





Корни 6-й степени из единицы.

Сгруппируем теперь все корни порядка d вместе и положим

$$\phi_d(x) \;:=\; \prod_{\lambda \text{ имеет порядок } d} (x - \lambda).$$

По определению $\phi_d(x)$ не зависит от n. Так как каждый корень n-й степени из единицы имеет некоторый порядок d, мы заключаем, что

$$x^n - 1 \;=\; \prod_{d \mid n} \phi_d(x). \tag{3}$$

Теперь сделаем решающее замечание. *Коэффициенты* многочленов $\phi_n(x)$ являются *целыми числами* (т. е. $\phi_n(x) \in \mathbb{Z}[x]$ для всех n); кроме того, свободный член многочлена $\phi_n(x)$ есть либо 1, либо -1.

Убедимся в справедливости этого утверждения. При $n = 1$ единственным корнем является 1, и поэтому $\phi_1(x) = x - 1$. Далее, действуя

по индукции, предположим, что $\phi_d(x) \in \mathbb{Z}[x]$ для всех $d < n$ и что свободный член $\phi_d(x)$ есть 1 или -1. В силу (3)

$$x^n - 1 \;=\; p(x)\,\phi_n(x), \tag{4}$$

где $p(x) = \sum\limits_{j=0}^{\ell} p_j x^j, \phi_n(x) = \sum\limits_{k=0}^{n-\ell} a_k x^k$, причем либо $p_0 = 1$, либо $p_0 = -1$.

Так как $p_0 a_0 = -1$, то $a_0 \in \{1, -1\}$. Далее рассуждаем по индукции. Допустим, что уже известны $a_0, a_1, \ldots, a_{k-1} \in \mathbb{Z}$. Вычисляя коэффициент при x^k в обеих частях (4), находим:

$$\sum_{j=0}^{k} p_j a_{k-j} \;=\; \sum_{j=1}^{k} p_j a_{k-j} + p_0 a_k \;\in\; \mathbb{Z}.$$

Согласно предположению, все коэффициенты $a_0, \ldots, a_{k-1}$ (и все p_j) принадлежат $\mathbb{Z}$. Так как p_0 есть 1 или -1, то $p_0 a_k$ и, следовательно, a_k также должны быть целыми числами.

Мы готовы к завершающему шагу. Пусть $n_k \,|\, n$ — одно из чисел, фигурирующих в (1). Тогда

$$x^n - 1 \;=\; \prod_{d \,|\, n} \phi_d(x) \;=\; (x^{n_k} - 1)\phi_n(x) \prod_{d \,|\, n,\, d \nmid n_k,\, d \neq n} \phi_d(x).$$

Значит, в $\mathbb{Z}$ выполняются соотношения делимости

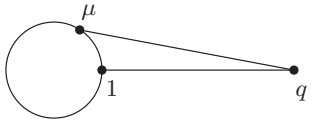
$$\phi_n(q) \mid q^n - 1 \qquad \text{и} \qquad \phi_n(q) \;\Big|\; \frac{q^n - 1}{q^{n_k} - 1}\,. \tag{5}$$

Так как соотношения (5) справедливы для всех k, то из формулы (1) мы получаем

$$\phi_n(q) \,|\, q - 1,$$

но этого быть не может. Почему? Мы знаем, что $\phi_n(x) = \prod(x - \lambda)$, где λ пробегает все множество корней двучлена $x^n - 1$, имеющих порядок n. Пусть $\widetilde{\lambda} = a + ib$ — один из этих корней. Так как $n > 1$ (поскольку $R \neq Z$), то корень $\widetilde{\lambda} \neq 1$, значит, a (вещественная часть $\widetilde{\lambda}$) меньше единицы. Далее, так как $|\widetilde{\lambda}|^2 = a^2 + b^2 = 1$ и $a < 1$, то

$$\begin{aligned} |q - \widetilde{\lambda}|^2 \;&=\; |q - a - ib|^2 \;=\; (q-a)^2 + b^2 = \\ &=\; q^2 - 2aq + a^2 + b^2 \;=\; q^2 - 2aq + 1 > \\ &>\; q^2 - 2q + 1 = (q-1)^2, \end{aligned}$$



$|q - \mu| > |q - 1|$

так что $|q - \widetilde{\lambda}| > q - 1$ для *всех* корней из единицы порядка n. Следовательно,

$$|\phi_n(q)| = \prod_{\lambda} |q - \lambda| > q - 1.$$

Это означает, что $\phi_n(q)$ не может быть делителем $q - 1$. Полученное противоречие завершает доказательство. □

Литература

[1] Dickson L. E. *On finite algebras.* Nachrichten der Akad. Wissenschaften Göttingen Math.-Phys. Klasse (1905), 1-36. (Collected Mathematical Papers, Vol. III, Chelsea Publ. Comp, The Bronx, NY, 1975, 539–574.)

[2] Wedderburn J. H. M. *A theorem on finite algebras.* Trans. Amer. Math. Soc., **6** (1905), 349–352.

[3] Witt E. *Über die Kommutativität endlicher Schiefkörper.* Abh. Math. Sem. Univ. Hamburg, **8** (1931), 413.

Глава 7 Некоторые иррациональные числа

Шарль Эрмит

«π иррационально»

Еще Аристотель предполагал, что диаметр и окружность круга несоизмеримы. Первое доказательство этого фундаментального факта получил Йохан Хейнрих Ламберт в 1766 году. Приведенное ниже доказательство из Книги нашел Иван Нивен в 1947 году [5]. Это в высшей степени элегантное короткое доказательство использует лишь элементарные вычисления. Его идея является очень мощной: с ее помощью, например, Ивамото [2] и Коксма [3] показали, что:

- π^2 иррационально (это более сильное утверждение!),
- e^r иррационально для рациональных $r \neq 0$.

Метод Нивена, конечно, появился не на пустом месте: его истоки можно проследить вплоть до классической статьи Шарля Эрмита 1873 года [1], в которой впервые было установлено, что e — трансцендентное число, т. е. что e не может быть корнем многочлена с рациональными коэффициентами.

$$\begin{aligned} e &:= 1+\tfrac{1}{1}+\tfrac{1}{2}+\tfrac{1}{6}+\tfrac{1}{24}+\dots \\ &= 2.718281828... \\ e^x &:= 1+\tfrac{x}{1}+\tfrac{x^2}{2}+\tfrac{x^3}{6}+\tfrac{x^4}{24}+\dots \\ &= \sum_{k\geqslant 0}\tfrac{x^k}{k!} \end{aligned}$$

Перед тем, как изучать π, мы рассмотрим e и его степени и убедимся в том, что они иррациональны. Это значительно проще, и мы поэтому будем следовать исторической последовательности получения результатов.

Прежде всего, легко показать (как установил Фурье в 1815 году), что $e = \sum_{k\geq 0}\frac{1}{k!}$ иррационально. В самом деле, если бы для целых $a, b > 0$ выполнялось равенство $e = \frac{a}{b}$, то мы получили бы, что *при любом* $n \geq 0$

$$n!\,b\,e \;=\; n!\,a.$$

Но это не может быть правильным, поскольку в правой части стоит целое число, тогда как левая ввиду равенства

$$e \;=\; \Big(1+\frac{1}{1!}+\frac{1}{2!}+\ldots+\frac{1}{n!}\Big) \;+\; \Big(\frac{1}{(n+1)!}+\frac{1}{(n+2)!}+\frac{1}{(n+3)!}+\;\ldots\;\Big)$$

разбивается на целое число

$$b\,n!\Big(1+\frac{1}{1!}+\frac{1}{2!}+\ldots+\frac{1}{n!}\Big)$$

и остаток

$$b\Big(\frac{1}{n+1}+\frac{1}{(n+1)(n+2)}+\frac{1}{(n+1)(n+2)(n+3)}+\;\ldots\;\Big),$$

который *приближенно* равен $\frac{b}{n}$ и поэтому при больших n не может быть целым числом. Действительно, остаток больше $\frac{b}{n+1}$ и меньше $\frac{b}{n}$, в чем легко убедиться, проводя сравнение с геометрическим рядом:

$$\begin{aligned}\frac{1}{n+1} &< \frac{1}{n+1}+\frac{1}{(n+1)(n+2)}+\frac{1}{(n+1)(n+2)(n+3)}+\ \dots\\ &< \frac{1}{n+1}+\frac{1}{(n+1)^2}+\frac{1}{(n+1)^3}+\ \dots\ =\ \frac{1}{n}\,.\end{aligned}$$

Может показаться, что этот простой прием умножения на $n!$ не достаточен для доказательства иррациональности e^2. Это утверждение более сильное: $\sqrt{2}$ — пример иррационального числа, квадрат которого таковым не является.

От Джона Косгрейва мы узнали, что с помощью двух тонких приемов можно тем не менее сделать еще два шага. Каждый из них достаточен для доказательства иррациональности e^2, а их комбинация позволяет доказать иррациональность e^4. Первый прием можно найти в одностраничной статье Ж. Лиувилля 1840 года, а второй — в двухстраничном «дополнении», которое Лиувилль опубликовал на следующих двух страницах журнала [4].

Почему e^2 иррационально? Что мы можем вывести из равенства $e^2=\frac{a}{b}$? Согласно Лиувиллю мы должны переписать его в виде

$$b\,e\ =\ a\,e^{-1},$$

подставить в это равенство ряды

$$e=1+\frac{1}{1}+\frac{1}{2}+\frac{1}{6}+\frac{1}{24}+\frac{1}{120}+\dots$$

и

$$e^{-1}=1-\frac{1}{1}+\frac{1}{2}-\frac{1}{6}+\frac{1}{24}-\frac{1}{120}+\dots,$$

и затем умножить на $n!$ с достаточно большим четным n. Тогда мы увидим, что число $n!\,be$ приблизительно целое. В самом деле,

$$n!\,b\Big(1+\frac{1}{1}+\frac{1}{2}+\frac{1}{6}+\dots+\frac{1}{n!}\Big)$$

— целое число, а остаток

$$n!\,b\Big(\frac{1}{(n+1)!}+\frac{1}{(n+2)!}+\dots\Big)$$

близок к $\frac{b}{n}$: как показано выше, он больше $\frac{b}{n+1}$ и меньше $\frac{b}{n}$.

Число $n!\,ae^{-1}$ тоже приблизительно целое: оно аналогично разлагается на большое целое и остаток

$$(-1)^{n+1}n!a\Big(\frac{1}{(n+1)!}-\frac{1}{(n+2)!}+\frac{1}{(n+3)!}-\dots\Big),$$

который приближенно равен $(-1)^{n+1}\frac{a}{n}$. Точнее, для четных n остаток больше $-\frac{a}{n}$ и меньше

$$-a\Big(\frac{1}{n+1}-\frac{1}{(n+1)^2}-\frac{1}{(n+1)^3}-\dots\Big)\ =\ -\frac{a}{n+1}\Big(1-\frac{1}{n}\Big)\ <\ 0.$$

Геометрический ряд

Для бесконечного геометрического ряда

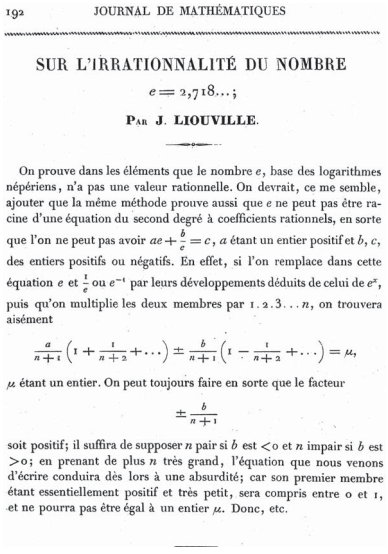
$Q=\frac{1}{q}+\frac{1}{q^2}+\frac{1}{q^3}+\dots$

при $q>1$, очевидно, имеем

$qQ=1+\frac{1}{q}+\frac{1}{q^2}+\dots=1+Q$,

значит,

$$Q=\frac{1}{q-1}\,.$$



192 JOURNAL DE MATHÉMATIQUES

SUR L'IRRATIONNALITÉ DU NOMBRE

$e=2{,}718\dots$;

PAR J. LIOUVILLE.

On prouve dans les éléments que le nombre e, base des logarithmes népériens, n'a pas une valeur rationnelle. On devrait, ce me semble, ajouter que la même méthode prouve aussi que e ne peut pas être racine d'une équation du second degré à coefficients rationnels, en sorte que l'on ne peut pas avoir $ae+\frac{b}{e}=c$, a étant un entier positif et b, c, des entiers positifs ou négatifs. En effet, si l'on remplace dans cette équation e et $\frac{1}{e}$ ou e^{-1} par leurs développements déduits de celui de e^x, puis qu'on multiplie les deux membres par $1.2.3\dots n$, on trouvera aisément

$$\frac{a}{n+1}\Big(1+\frac{1}{n+2}+\dots\Big)\pm\frac{b}{n+1}\Big(1-\frac{1}{n+2}+\dots\Big)=\mu,$$

μ étant un entier. On peut toujours faire en sorte que le facteur

$$\pm\frac{b}{n+1}$$

soit positif; il suffira de supposer n pair si b est <0 et n impair si b est >0; en prenant de plus n très grand, l'équation que nous venons d'écrire conduira dès lors à une absurdité; car son premier membre étant essentiellement positif et très petit, sera compris entre 0 et 1, et ne pourra pas être égal à un entier μ. Donc, etc.

Статья Лиувилля

Но отсюда следует, что при большом четном n число $n!\,ae^{-1}$ чуть-чуть меньше целого, а $n!\,be$ чуть-чуть больше целого, и поэтому равенство $n!\,ae^{-1} = n!\,be$ не может выполняться. □

Ободренные успехом, мы теперь для доказательства иррациональности e^4 допустим, что $e^4 = \frac{a}{b}$ рационально, и запишем это в виде

$$b\,e^2 \;=\; a\,e^{-2}.$$

Можно попытаться умножить обе части на $n!$ для какого-нибудь большого n, и собрать нецелые слагаемые, но это не даст ничего полезного: сумма оставшихся членов в левой части окажется приближенно равной $b\,\frac{2^{n+1}}{n}$, в правой части — приближенно равной $(-1)^{n+1}a\,\frac{2^{n+1}}{n}$, и обе будут очень большими при больших n.

Поэтому придется изучить ситуацию внимательнее и внести в стратегию два небольших уточнения. Во-первых, будем выбирать не *произвольные* большие n, а большие степени двойки, т. е. $n = 2^m$; во-вторых, будем умножать не на $n!$, а на $\frac{n!}{2^{n-1}}$. Нам потребуется также маленькая лемма — частный случай теоремы Лежандра (см. с. 17): Для любого $n \geq 1$ число $n!$ содержит простой множитель 2 не более $n-1$ раз, и равенство имеет место тогда и только тогда, когда n есть степень двух: $n = 2^m$.

Доказать эту лемму несложно: $\lfloor \frac{n}{2} \rfloor$ сомножителей в $n!$ четные, $\lfloor \frac{n}{4} \rfloor$ из них делятся на 4, и т. д. Поэтому если 2^k — наибольшая степень двойки, для которой $2^k \leq n$, то $n!$ содержит простой множитель 2 ровно

$$\left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor + \ldots + \left\lfloor \frac{n}{2^k} \right\rfloor \;\leq\; \frac{n}{2} + \frac{n}{4} + \ldots + \frac{n}{2^k} \;=\; n\Big(1 - \frac{1}{2^k}\Big) \;\leq\; n-1$$

раз, причем оба неравенства обращаются в равенство только в случаях, когда $n = 2^k$.

Вернемся к равенству $b\,e^2 = a\,e^{-2}$. Приведем его к виду

$$b\,\frac{n!}{2^{n-1}}\,e^2 \;=\; a\,\frac{n!}{2^{n-1}}\,e^{-2} \tag{1}$$

и подставим в него ряды

$$e^2 \;=\; 1 + \frac{2}{1} + \frac{4}{2} + \frac{8}{6} + \;\ldots\; + \frac{2^r}{r!} + \ldots$$

и

$$e^{-2} \;=\; 1 - \frac{2}{1} + \frac{4}{2} - \frac{8}{6} + \;\ldots\; + (-1)^r\frac{2^r}{r!} + \ldots$$

При $r \leq n$ мы получаем целочисленные слагаемые в обеих частях:

$$b\,\frac{n!}{2^{n-1}}\,\frac{2^r}{r!} \quad \text{и} \quad (-1)^r a\,\frac{n!}{2^{n-1}}\,\frac{2^r}{r!}\,,$$

и при $r > 0$ знаменатель $r!$ содержит простой множитель 2 *не более* $r-1$ раз, а $n!$ содержит его *ровно* $n-1$ раз. (Значит, при $r > 0$ слагаемые четные.)

Поскольку n четное (мы считаем, что $n = 2^m$), ряды, соответствующие значениям $r \geq n+1$, имеют вид

$$2b\Big(\frac{2}{n+1} + \frac{4}{(n+1)(n+2)} + \frac{8}{(n+1)(n+2)(n+3)} + \;\ldots\Big)$$

и

$$2a\Big(-\frac{2}{n+1}+\frac{4}{(n+1)(n+2)}-\frac{8}{(n+1)(n+2)(n+3)}+\ \dots\Big).$$

Сравнение с геометрическими рядами показывает, что при больших n эти суммы приближенно равны соответственно $\frac{4b}{n}$ и $-\frac{4a}{n}$. Это значит, что при больших $n=2^m$ левая часть (1) *чуть-чуть* больше целого числа, а правая часть *чуть-чуть* меньше, и мы приходим к противоречию! □

Таким образом, мы доказали, что e^4 иррационально. Для доказательства иррациональности e^3, e^5 и т. д. нам потребуются более сложная техника (кое-что из анализа) и новая идея, по существу принадлежащая Шарлю Эрмиту; ключом к ней является следующая простая лемма.

Лемма. *Пусть*

$$f(x) \;=\; \frac{x^n(1-x)^n}{n!},$$

где $n\ge 1$ — некоторое фиксированное целое число. Тогда

(i) *Функция $f(x)$ — многочлен вида $f(x)=\dfrac{1}{n!}\displaystyle\sum_{i=n}^{2n}c_i x^i$ с целыми коэффициентами c_i.*

(ii) *При $0<x<1$ выполняются неравенства $0<f(x)<\frac{1}{n!}$.*

(iii) *Для всех $k\ge 0$ производные $f^{(k)}(0)$ и $f^{(k)}(1)$ — целые числа.*

■ **Доказательство.** Утверждения (i) и (ii) леммы очевидны. Для доказательства (iii) заметим, что согласно (i) k-я производная $f^{(k)}$ в точке $x=0$ равна нулю за исключением значений k из интервала $n\le k\le 2n$, для которых $f^{(k)}(0)=\frac{k!}{n!}\,c_k$ есть целое число. Из равенства $f(x)=f(1-x)$ мы получаем, что $f^{(k)}(x)=(-1)^k f^{(k)}(1-x)$ для всех x, и, следовательно, $f^{(k)}(1)=(-1)^k f^{(k)}(0)$ — тоже целое число. □

Теорема 1. *Число e^r иррационально для каждого $r\in\mathbb{Q}\backslash\{0\}$.*

■ **Доказательство.** Достаточно показать, что число e^s не может быть рациональным для целых положительных s (если $e^{\frac{s}{t}}$ рационально, то рационально также и $\big(e^{\frac{s}{t}}\big)^t=e^s$). Предположим, что $e^s=\frac{a}{b}$ для целых $a,b>0$, и выберем n таким большим, чтобы выполнялось неравенство $n!>as^{2n+1}$. Положим

Неравенство $n!>e(\frac{n}{e})^n$ позволяет получить явные оценки для этих «достаточно больших» n.

$$F(x):=s^{2n}f(x)-s^{2n-1}f'(x)+s^{2n-2}f''(x)-\ \dots\ +f^{(2n)}(x),$$

где $f(x)$ — функция из леммы. Функцию $F(x)$ можно представить также бесконечной суммой

$$F(x)=s^{2n}f(x)-s^{2n-1}f'(x)+s^{2n-2}f''(x)-\dots,$$

поскольку производные $f^{(k)}(x)$ при $k>2n$ равны 0. Отсюда следует, что $F(x)$ удовлетворяет тождеству

$$F'(x)\;=\;-s\,F(x)+s^{2n+1}f(x).$$

Поэтому дифференцирование дает

$$\frac{d}{dx}\left[e^{sx}F(x)\right] \;=\; se^{sx}F(x)+e^{sx}F'(x) \;=\; s^{2n+1}e^{sx}f(x)$$

и, следовательно,

$$N \;:=\; b\int_0^1 s^{2n+1}e^{sx}f(x)dx \;=\; b\left[e^{sx}F(x)\right]_0^1 \;=\; aF(1)-bF(0).$$

Значение N является целым, так как согласно утверждению (iii) леммы числа $F(0)$ и $F(1)$ — целые. Далее, утверждение (ii) леммы позволяет оценить N снизу и сверху:

$$0 \;<\; N \;=\; b\int_0^1 s^{2n+1}e^{sx}f(x)dx \;<\; bs^{2n+1}e^s\frac{1}{n!} \;=\; \frac{as^{2n+1}}{n!} \;<\; 1.$$

Значит, N не может быть целым числом. Полученное противоречие доказывает, что e^s иррационально. □

Убедившись в полезности этого приема, воспользуемся им еще раз.

Теорема 2. *π^2 иррационально.*

■ **Доказательство.** Предположим, что $\pi^2=\frac{a}{b}$, где $a,b>0$ — целые числа. На этот раз воспользуемся многочленом

$$F(x) \;:=\; b^n\Big(\pi^{2n}f(x)-\pi^{2n-2}f^{(2)}(x)+\pi^{2n-4}f^{(4)}(x)-\ldots\Big),$$

где $f(x)$ — функция из леммы. Он удовлетворяет соотношению

$$F''(x)=-\pi^2F(x)+b^n\pi^{2n+2}f(x).$$

Число π не рациональное, но хорошо приближается рациональными числами; некоторые из этих приближений известны с античных времен:

$\frac{22}{7}$ = 3.142857142857...
$\frac{355}{113}$ = 3.141592920353...
$\frac{104348}{33215}$ = 3.141592653921...
π = 3.141592653589...

Из утверждения (iii) леммы и предположения $\pi^2=\frac{a}{b}$ следует, что $F(0)$ и $F(1)$ — целые числа. Элементарные правила дифференцирования приводят к равенству

$$\begin{aligned}\frac{d}{dx}\big[F'(x)\sin\pi x-\pi F(x)\cos\pi x\big] &= \big(F''(x)+\pi^2F(x)\big)\sin\pi x\\ &= b^n\pi^{2n+2}f(x)\sin\pi x\\ &= \pi^2a^nf(x)\sin\pi x,\end{aligned}$$

а из него мы получаем, что

$$\begin{aligned}N:=\pi\int_0^1 a^nf(x)\sin\pi x\,dx &= \Big[\frac{1}{\pi}F'(x)\sin\pi x-F(x)\cos\pi x\Big]_0^1\\ &= F(0)+F(1)\end{aligned}$$

есть целое число. Более того, N положительно, так как эта величина есть интеграл от функции, положительной всюду, кроме концевых точек. Однако если n столь велико, что выполняется неравенство $\frac{\pi a^n}{n!}<1$, то из утверждения (ii) леммы следуют неравенства

$$0 \;<\; N \;=\; \pi\int_0^1 a^nf(x)\sin\pi x\,dx \;<\; \frac{\pi a^n}{n!} \;<\; 1,$$

которые противоречат тому, что N — целое число. □

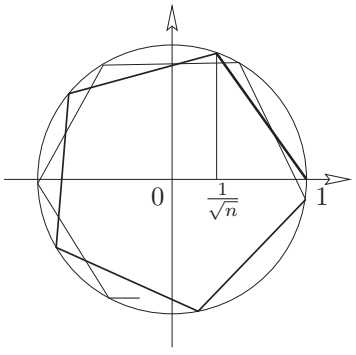
В заключение приведем еще один результат, связанный с иррациональностью.

Теорема 3. *Для каждого нечетного целого $n \geq 3$ число*

$$A(n) := \frac{1}{\pi} \arccos\left(\frac{1}{\sqrt{n}}\right)$$

иррационально.

Это предложение нам понадобится при рассмотрении третьей проблемы Гильберта (см. гл. 9) в случаях $n = 3$ и $n = 9$. Для $n = 2$ и $n = 4$ мы имеем $A(2) = \frac{1}{4}$ и $A(4) = \frac{1}{3}$, так что ограничение, связанное с нечетностью n, существенно. Указанные значения легко находятся с помощью рисунка на полях, поскольку утверждение «$\frac{1}{\pi} \arccos\left(\frac{1}{\sqrt{n}}\right)$ иррационально» эквивалентно тому, что вписанная в единичную окружность построенная по $\frac{1}{\sqrt{n}}$ ломаная, все звенья которой — хорды одной и той же длины, не может быть замкнутой.



Мы предлагаем читателю в качестве упражнения показать, что $A(n)$ рационально *только* при $n \in \{1, 2, 4\}$ (нужно отдельно рассмотреть случаи, когда $n = 2^r$ и когда n не есть степень числа 2).

■ **Доказательство.** Воспользуемся теоремой сложения

$$\cos\alpha + \cos\beta = 2\cos\tfrac{\alpha+\beta}{2}\cos\tfrac{\alpha-\beta}{2}$$

из элементарной тригонометрии, согласно которой при $\alpha = (k+1)\varphi$ и $\beta = (k-1)\varphi$

$$\cos(k+1)\varphi \;=\; 2\cos\varphi\;\cos\,k\varphi \;-\; \cos(k-1)\varphi. \tag{2}$$

Для угла $\varphi_n = \arccos\left(\frac{1}{\sqrt{n}}\right)$, который определяется условиями $\cos\varphi_n = \frac{1}{\sqrt{n}}$ и $0 \leq \varphi_n \leq \pi$, это приводит к представлениям вида

$$\cos\,k\varphi_n \;=\; \frac{A_k}{\sqrt{n}^k},$$

где A_k — целое число, не делящееся на n при любом $k \geq 0$. Для $k = 0, 1$ такие представления имеют место с $A_0 = A_1 = 1$; с помощью индукции по k, используя (2), для $k \geq 1$ получаем

$$\cos(k+1)\varphi_n \;=\; 2\frac{1}{\sqrt{n}}\frac{A_k}{\sqrt{n}^k} - \frac{A_{k-1}}{\sqrt{n}^{k-1}} \;=\; \frac{2A_k - nA_{k-1}}{\sqrt{n}^{k+1}}.$$

Следовательно, $A_{k+1} = 2A_k - nA_{k-1}$. Если $n \geq 3$ нечетно и A_k не делится на n, то и A_{k+1} не может делиться на n.

Теперь предположим, что

$$A(n) \;=\; \frac{1}{\pi}\,\varphi_n \;=\; \frac{k}{\ell}$$

— рациональное число ($k, \ell > 0$ — целые). Из равенства $\ell\varphi_n = k\pi$ следует, что

$$\pm 1 \;=\; \cos\,k\pi \;=\; \frac{A_\ell}{\sqrt{n}^\ell}\,.$$

Поэтому $(\sqrt{n})^\ell = \pm A_\ell$ — целое число, и $\ell \geq 2$. Значит, $n \mid \sqrt{n}^\ell$. Так как $\sqrt{n}^\ell \mid A_\ell$, то n делит A_ℓ, что противоречит доказанному ранее. □

Литература

[1] Hermite C. *Sur la fonction exponentielle.* Comptes rendus de l'Académie des Sciences (Paris), **77** (1873), 18-24; Œuvres de Charles Hermite, Vol. III, Gauthier-Villars, Paris, 1912, pp. 150–181.

[2] Iwamoto Y. *A proof that π^2 is irrational.* J. Osaka Institute of Science and Technology, **1** (1949), 147–148.

[3] Koksma J. F. *On Niven's proof that π is irrational.* Nieuw Archief voor Wiskunde (2), **23** (1949), 39.

[4] Liouville J. *Sur l'irrationalité du nombre e = 2,718...* Journal de Mathématiques Pures et Appl. (1), **5** (1840), 192; *Addition*, 193–194.

[5] Niven I. *A simple proof that π is irrational.* Bulletin Amer. Math. Soc., **53** (1947), 509.

Три раза о $\pi^2/6$

Глава 8

Мы знаем, что бесконечный ряд $\sum_{n\geq 1}\frac{1}{n}$ расходится. Более того, в главе 1 мы убедились в том, что даже ряд $\sum_{p\in\mathbb{P}}\frac{1}{p}$ расходится.

Однако ряд из чисел, обратных квадратам, сходится (хотя, как мы увидим, очень медленно) к весьма примечательному значению.

Ряд Эйлера.

$$\sum_{n\geq 1}\frac{1}{n^2} \;=\; \frac{\pi^2}{6}\,.$$

Этот классический, знаменитый и важный результат был получен Леонардом Эйлером в 1734 году. Одна из его важнейших интерпретаций состоит в том, что он дает первое нетривиальное значение $\zeta(2)$ дзета-функции Римана (см. приложение на с. 59). Как мы видели в главе 7, это значение иррационально.

Но не только само это утверждение занимает важное место в истории математики; для него найдено много чрезвычайно изящных и глубоких доказательств, имеющих свои собственные истории и доставившие радость открытия и переоткрытия многим математикам. В этой главе мы приводим три таких доказательства.

1	$=$	1.000000
$1+\frac{1}{4}$	$=$	1.250000
$1+\frac{1}{4}+\frac{1}{9}$	$=$	1.361111
$1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}$	$=$	1.423611
$1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\frac{1}{25}$	$=$	1.463611
$1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\frac{1}{25}+\frac{1}{36}$	$=$	1.491388
$\pi^2/6$	$=$	$1.644934.$

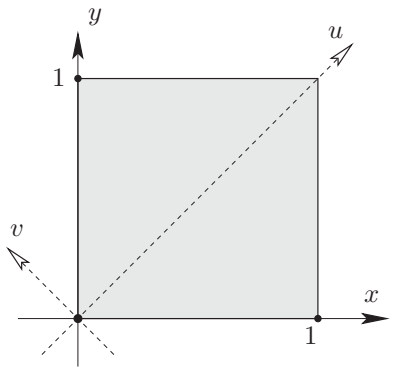
■ **Доказательство.** Наше первое доказательство содержится в виде упражнения в учебнике Вильяма ЛеВекью по теории чисел, изданном в 1956 году. Однако он пишет: «У меня нет ни малейшего представления о том, где возникла эта задача, но я совершенно уверен в том, что не имею к ней отношения».

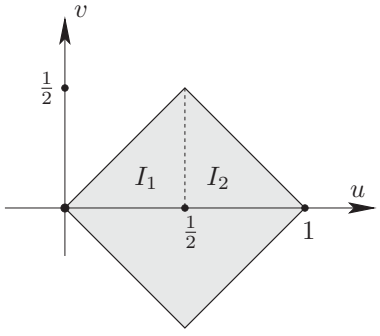
Доказательство состоит в сопоставлении двух различных способов вычисления двойного интеграла

$$I \;:=\; \int_0^1\!\!\int_0^1 \frac{1}{1-xy}\,dx\,dy.$$

Первый способ состоит в разложении $\frac{1}{1-xy}$ в геометрический ряд и представлении слагаемых в виде легко интегрируемых произведений:

$$\begin{aligned} I \;&=\; \int_0^1\!\!\int_0^1 \sum_{n\geq 0}(xy)^n\,dx\,dy \;=\; \sum_{n\geq 0}\int_0^1\!\!\int_0^1 x^n y^n\,dx\,dy \\ &=\; \sum_{n\geq 0}\Big(\int_0^1 x^n dx\Big)\Big(\int_0^1 y^n dy\Big) \;=\; \sum_{n\geq 0}\frac{1}{n+1}\,\frac{1}{n+1} \\ &=\; \sum_{n\geq 0}\frac{1}{(n+1)^2} \;=\; \sum_{n\geq 1}\frac{1}{n^2} \;=\; \zeta(2). \end{aligned}$$





Формула замены

Для вычисления двойного интеграла

$$I \;=\; \int\limits_S f(x,y)\,dx\,dy$$

можно применить замену переменных

$$x = x(u,v) \quad y = y(u,v),$$

если отображение $(u,v) \in T$ в $(x,y) \in S$ биективно и непрерывно дифференцируемо. Тогда I равен

$$\int\limits_T f(x(u,v),y(u,v))\Big|\frac{d(x,y)}{d(u,v)}\Big|\,du\,dv,$$

где $\frac{d(x,y)}{d(u,v)}$ — определитель Якоби (якобиан):

$$\frac{d(x,y)}{d(u,v)} \;=\; \det\begin{pmatrix} \frac{dx}{du} & \frac{dx}{dv} \\ \frac{dy}{du} & \frac{dy}{dv} \end{pmatrix}.$$

Это вычисление показывает также, что двойной интеграл I (от положительной функции с полюсом в точке $x = y = 1$) конечен. Заметим, что преобразования легко провести и в обратном направлении, сводя вычисление $\zeta(2)$ к двойному интегралу I.

Второй способ вычисления I основан на замене переменных

$$u \;:=\; \frac{y+x}{2} \qquad \text{и} \qquad v \;:=\; \frac{y-x}{2},$$

переводящей область интегрирования в квадрат со стороной длины $\frac{1}{2}\sqrt{2}$ с помощью поворота старой области на $45°$ и сжатия в $\sqrt{2}$ раз. С помощью подстановки $x = u - v$ и $y = u + v$ получаем

$$\frac{1}{1-xy} \;=\; \frac{1}{1-u^2+v^2}.$$

Поскольку наша линейная замена переменных уменьшает площадь в два раза (что равно значению определителя Якоби преобразования, см. вставку), при преобразовании интеграла мы должны заменить $dx\,dy$ на $2\,du\,dv$. Новая область интегрирования и подынтегральная функция симметричны относительно оси u, так что остается вычислить лишь удвоенный (здесь появляется еще один множитель 2!) интеграл по верхней половине области. Мы разбиваем ее на две части самым естественным образом:

$$I \;=\; 4\int\limits_0^{1/2}\Big(\int\limits_0^{u}\frac{dv}{1-u^2+v^2}\Big)du \;+\; 4\int\limits_{1/2}^{1}\Big(\int\limits_0^{1-u}\frac{dv}{1-u^2+v^2}\Big)du.$$

Используя формулу $\displaystyle\int\frac{dx}{a^2+x^2} = \frac{1}{a}\operatorname{arctg}\frac{x}{a} + C$, отсюда получаем

$$\begin{aligned} I \;=\;& 4\int\limits_0^{1/2}\frac{1}{\sqrt{1-u^2}}\operatorname{arctg}\Big(\frac{u}{\sqrt{1-u^2}}\Big)\,du \\ &+\; 4\int\limits_{1/2}^{1}\frac{1}{\sqrt{1-u^2}}\operatorname{arctg}\Big(\frac{1-u}{\sqrt{1-u^2}}\Big)\,du. \end{aligned}$$

Эти интегралы можно упростить и вычислить в явном виде с помощью замен $u = \sin\theta$ и $u = \cos\theta$ соответственно. Но мы поступим проще: заметим, что производная функции $g(u) := \operatorname{arctg}\left(\frac{u}{\sqrt{1-u^2}}\right)$ есть $g'(u) = \frac{1}{\sqrt{1-u^2}}$, а производная функции $h(u) := \operatorname{arctg}\left(\frac{1-u}{\sqrt{1-u^2}}\right) = \operatorname{arctg}\left(\sqrt{\frac{1-u}{1+u}}\right)$ равна $h'(u) = -\frac{1}{2}\frac{1}{\sqrt{1-u^2}}$. Поэтому, используя равенство $\int_a^b f'(x)f(x)dx = \left[\frac{1}{2}f(x)^2\right]_a^b = \frac{1}{2}f(b)^2 - \frac{1}{2}f(a)^2$, находим:

$$\begin{aligned} I \;&=\; 4\int_0^{1/2} g'(u)g(u)\,du \;+\; 4\int_{1/2}^{1} -2h'(u)h(u)\,du \\ &=\; 2\Big[g(u)^2\Big]_0^{1/2} \;-\; 4\Big[h(u)^2\Big]_{1/2}^{1} \\ &=\; 2g(\tfrac{1}{2})^2 \;-\; 2g(0)^2 \;-\; 4h(1)^2 \;+\; 4h(\tfrac{1}{2})^2 \\ &=\; 2\big(\tfrac{\pi}{6}\big)^2 - 0 - 0 + 4\big(\tfrac{\pi}{6}\big)^2 \;=\; \tfrac{\pi^2}{6}. \end{aligned}$$

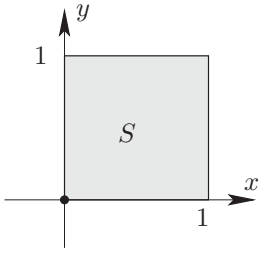
□

В приведенном доказательстве значение ряда Эйлера получилось из интеграла посредством довольно простой замены переменных. Позднее Бейкерс, Калаби и Колк [2] нашли остроумный вариант этого доказательства с совершенно нетривиальной заменой переменных. Они начинают с разбиения суммы $\sum_{n\ge1}\frac{1}{n^2}=\zeta(2)$ на две суммы по четным и нечетным значениям n. Ясно, что сумма по четным числам $\frac{1}{2^2}+\frac{1}{4^2}+\frac{1}{6^2}+\ldots=\sum_{k\ge1}\frac{1}{(2k)^2}$ равна $\frac14\zeta(2)$, так что сумма по нечетным числам $\frac{1}{1^2}+\frac{1}{3^2}+\frac{1}{5^2}+\ldots=\sum_{k\ge0}\frac{1}{(2k+1)^2}$ равна $\frac34\,\zeta(2)$. Следовательно, теорема о ряде Эйлера эквивалентна следующему утверждению.

$$\sum_{k\ge0}\frac{1}{(2k+1)^2} \;=\; \frac{\pi^2}{8}\,.$$

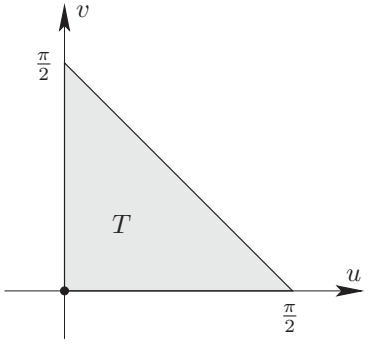
■ **Доказательство.** Как и выше, мы можем представить рассматриваемую сумму в виде двойного интеграла, а именно,

$$J \;=\; \int_0^1\!\!\int_0^1 \frac{1}{1-x^2y^2}\,dx\,dy \;=\; \sum_{k\ge0}\frac{1}{(2k+1)^2}\,.$$



Поэтому нам нужно вычислить интеграл J. И для этого Бейкерс, Калаби и Колк предложили новую замену переменных:

$$u \;:=\; \arccos\sqrt{\frac{1-x^2}{1-x^2y^2}},\quad v \;:=\; \arccos\sqrt{\frac{1-y^2}{1-x^2y^2}}\,.$$



При вычислении двойного интеграла можно пренебречь границей области и рассматривать x,y изменяющимися в пределах $0<x<1$ и $0<y<1$. Тогда точки (u,v) будут принадлежать треугольнику $u>0$, $v>0$, $u+v<\pi/2$. Замену переменных можно обратить:

$$x \;=\; \frac{\sin u}{\cos v} \qquad \text{и} \qquad y \;=\; \frac{\sin v}{\cos u}\,.$$

Легко проверить, что эти формулы определяют биективное преобразование координат между внутренностью единичного квадрата $S=\{(x,y):0\le x,y\le1\}$ и внутренностью треугольника $T=\{(u,v):u,v\ge0,\ u+v\le\pi/2\}$.

Теперь вычислим якобиан замены переменных; при этом волшебным образом оказывается, что он равен

$$\det\begin{pmatrix} \frac{\cos u}{\cos v} & \frac{\sin u\sin v}{\cos^2 v} \\ \frac{\sin u\sin v}{\cos^2 u} & \frac{\cos v}{\cos u}\end{pmatrix} \;=\; 1-\frac{\sin^2u\sin^2v}{\cos^2u\cos^2v} \;=\; 1-x^2y^2.$$

Но тогда интеграл, который мы хотим вычислить, преобразуется в

$$J \;=\; \int_0^{\pi/2}\!\!\int_0^{\pi/2-u} 1\;du\,dv,$$

что есть как раз площадь $\frac12(\frac{\pi}{2})^2=\frac{\pi^2}{8}$ треугольника T. □

Этот метод доказательства не только красив, но и применим к вычислению $\zeta(2k)$ с помощью $2k$-мерных интегралов для всех $k \geq 1$. Мы отсылаем читателя к оригинальной статье Вейкера, Калаби и Колка [2] и к гл. 23, в которой тот же результат получается другим способом с помощью приема Герглотца и первоначального подхода Эйлера.

После двух доказательств с заменами переменных мы не можем устоять перед искушением рассказать о совершенно другом и абсолютно элементарном доказательстве формулы $\sum_{n\geq 1} \frac{1}{n^2} = \frac{\pi^2}{6}$. Оно появилось в виде цепочки упражнений в сборнике задач [7] близнецов Акивы и Исаака Ягломов, изданном в 1954 году. Варианты этого замечательного доказательства переоткрывали Холм (1970), Пападимитриу (1973) и Рэнсфорд (1982), который приписывает его Джону Скоулсу.

■ **Доказательство.** Сначала установим замечательное соотношение для суммы квадратов значений котангенса: при любом целом $m \geq 1$

$$\operatorname{ctg}^2\left(\tfrac{\pi}{2m+1}\right) + \operatorname{ctg}^2\left(\tfrac{2\pi}{2m+1}\right) + \ldots + \operatorname{ctg}^2\left(\tfrac{m\pi}{2m+1}\right) \;=\; \tfrac{2m(2m-1)}{6}. \qquad (1)$$

Чтобы доказать его, воспользуемся равенством $e^{ix} = \cos x + i \sin x$. Переходя к его n-й степени $e^{inx} = (e^{ix})^n$, находим, что

$$\cos nx + i \sin nx \;=\; (\cos x + i \sin x)^n.$$

Приравняем мнимые части:

$$\sin nx \;=\; \binom{n}{1} \sin x \cos^{n-1} x - \binom{n}{3} \sin^3 x \cos^{n-3} x \pm \ldots \qquad (2)$$

Для $m = 1, 2, 3$ из формулы (1) получаем: $\operatorname{ctg}^2 \frac{\pi}{3} = \frac{1}{3}$,
$\operatorname{ctg}^2 \frac{\pi}{5} + \operatorname{ctg}^2 \frac{2\pi}{5} = 2$,
$\operatorname{ctg}^2 \frac{\pi}{7} + \operatorname{ctg}^2 \frac{2\pi}{7} + \operatorname{ctg}^2 \frac{3\pi}{7} = 5$.

Теперь положим $n = 2m+1$, а для x рассмотрим m различных значений $x = \frac{r\pi}{2m+1}$, $r = 1, 2, \ldots, m$. Для каждого из них $nx = r\pi$ и, следовательно, $\sin nx = 0$, в то время как из неравенств $0 < x < \frac{\pi}{2}$ вытекает, что $\sin x$ принимает m различных положительных значений.

Поэтому, разделив обе части (2) для каждого из выбранных значений x на $\sin^n x$, мы получим равенства

$$0 = \binom{n}{1} \operatorname{ctg}^{n-1} x - \binom{n}{3} \operatorname{ctg}^{n-3} x \pm \ldots,$$

или

$$0 = \binom{2m+1}{1} \operatorname{ctg}^{2m} x - \binom{2m+1}{3} \operatorname{ctg}^{2m-2} x \pm \ldots$$

Таким образом, для многочлена степени m

$$p(t) := \binom{2m+1}{1} t^m - \binom{2m+1}{3} t^{m-1} \pm \ldots + (-1)^m \binom{2m+1}{2m+1}$$

нам известны m различных корней

$$a_r = \operatorname{ctg}^2\left(\tfrac{r\pi}{2m+1}\right), \quad r = 1, 2, \ldots, m.$$

Следовательно, многочлен $p(t)$ совпадает с произведением

$$p(t) \;=\; \binom{2m+1}{1} \left(t - \operatorname{ctg}^2\left(\tfrac{\pi}{2m+1}\right)\right) \cdot \ldots \cdot \left(t - \operatorname{ctg}^2\left(\tfrac{m\pi}{2m+1}\right)\right).$$

Сравнение коэффициентов при t^{m-1} в обеих частях этого равенства показывает, что сумма корней многочлена $p(t)$ есть

$$a_1 + \ldots + a_r \;=\; \frac{\binom{2m+1}{3}}{\binom{2m+1}{1}} \;=\frac{2m(2m-1)}{6}\,,$$

Сравнение коэффициентов: если $p(t) = c(t-a_1)\cdots(t-a_m)$, то коэффициент при t^{m-1} равен $-c(a_1+\ldots+a_m)$.

что совпадает с (1).

Нам потребуется также другое тождество того же типа для косеканса $\operatorname{cosec} x = \frac{1}{\sin x}$:

$$\operatorname{cosec}^2\left(\tfrac{\pi}{2m+1}\right) + \operatorname{cosec}^2\left(\tfrac{2\pi}{2m+1}\right) + \ldots + \operatorname{cosec}^2\left(\tfrac{m\pi}{2m+1}\right) = \tfrac{2m(2m+2)}{6}\,. \quad (3)$$

Но

$$\operatorname{cosec}^2 x = \frac{1}{\sin^2 x} = \frac{\cos^2 x + \sin^2 x}{\sin^2 x} = \operatorname{ctg}^2 x + 1,$$

так что (3) можно вывести из (1), прибавив m к обеим частям этого равенства.

Теперь подготовка полностью закончена. Воспользуемся тем, что в интервале $0 < y < \frac{\pi}{2}$ выполняются неравенства

$$0 \;<\; \sin y \;<\; y \;<\; \operatorname{tg} y,$$

Из $0 < a < b < c$ следует, что $0 < \frac{1}{c} < \frac{1}{b} < \frac{1}{a}$

и, следовательно,

$$0 \;<\; \operatorname{ctg} y \;<\; \tfrac{1}{y} \;<\; \operatorname{cosec} y,$$

откуда вытекает, что

$$\operatorname{ctg}^2 y \;<\; \tfrac{1}{y^2} \;<\; \operatorname{cosec}^2 y.$$

Запишем это двойное неравенство для каждого из m выбранных значений x и сложим результаты. Используя (1) для выражения в левой части и (3) для суммы в правой части, получаем

$$\tfrac{2m(2m-1)}{6} \;<\; \left(\tfrac{2m+1}{\pi}\right)^2 + \left(\tfrac{2m+1}{2\pi}\right)^2 + \ldots + \left(\tfrac{2m+1}{m\pi}\right)^2 \;<\; \tfrac{2m(2m+2)}{6}\,,$$

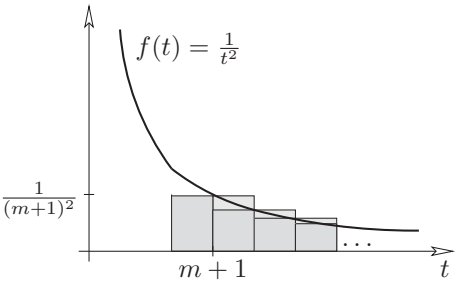
т. е.

$$\tfrac{\pi^2}{6}\,\tfrac{2m}{2m+1}\,\tfrac{2m-1}{2m+1} \;<\; \tfrac{1}{1^2} + \tfrac{1}{2^2} + \ldots + \tfrac{1}{m^2} \;<\; \tfrac{\pi^2}{6}\,\tfrac{2m}{2m+1}\,\tfrac{2m+2}{2m+1}\,.$$

При $m \to \infty$ выражения в левой и правой частях сходятся к $\frac{\pi^2}{6}$. Доказательство закончено. □

Как быстро ряд $\sum \frac{1}{n^2}$ сходится к $\pi^2/6$? Для ответа на этот вопрос мы должны оценить разность

$$\frac{\pi^2}{6} \;-\; \sum_{n=1}^{\infty} \frac{1}{n^2} \;\;=\;\; \sum_{n=m+1}^{\infty} \frac{1}{n^2}\,.$$



Это очень просто сделать методом «сравнения с интегралом», который мы уже использовали в приложении к гл. 2 (с. 19). Он дает неравенства

$$\sum_{n=m+1}^{\infty} \frac{1}{n^2} \;<\; \int_m^{\infty} \frac{1}{t^2}dt \;=\; \frac{1}{m}$$

для верхней оценки и

$$\sum_{n=m+1}^{\infty} \frac{1}{n^2} \;>\; \int_{m+1}^{\infty} \frac{1}{t^2}dt \;=\; \frac{1}{m+1}$$

для нижней оценки «хвоста ряда» — или даже

$$\sum_{n=m+1}^{\infty} \frac{1}{n^2} \;>\; \int_{m+\frac{1}{2}}^{\infty} \frac{1}{t^2}dt \;=\; \frac{1}{m+\frac{1}{2}}\,,$$

если вы хотите немного уточнить оценку с помощью выпуклости функции $f(t) = \frac{1}{t^2}$.

Это показывает, что наш ряд сходится не очень быстро: если сложить первую тысячу слагаемых, то погрешность будет в третьем десятичном знаке после запятой, если сложить первый миллион слагаемых, $m = 1000000$, то погрешность будет в шестом десятичном знаке, и т. д. Однако здесь нас ожидает большой сюрприз: с точностью до 45 знаков

$$\begin{aligned} \pi^2/6 &= 1.64493406684822643647241516664602518921894990 1, \\ \sum_{n=1}^{10^6} \frac{1}{n^2} &= 1.64493306684872643630574849997939185588561654 4. \end{aligned}$$

Таким образом, шестой знак после запятой неверен (меньше на 1), но *следующие шесть знаков правильные*! Далее один знак неверен (больше на 5), а следующие пять знаков опять правильные. Это удивительное открытие сделал Рой Норт из Колорадо Спрингс в 1988 году. (В 1982 году Мартину Повеллу, школьному учителю в Эмершэме, Бакингемшир, Англия, не удалось обнаружить описанный эффект в полной мере из-за того, что компьютеры тогда были маломощными.) Совпадения слишком странные, чтобы быть случайными... Погрешность, выписанная опять с 45 знаками после запятой:

$$\sum_{n=10^6+1}^{\infty} \frac{1}{n^2} \;=\; 0.000000999999500000166666666666633333333333357,$$

показывает, что здесь действительно имеет место закономерность. Вы можете переписать это последнее число в виде

$$+\,10^{-6} \;-\; \tfrac{1}{2}10^{-12} \;+\; \tfrac{1}{6}10^{-18} \;-\; \tfrac{1}{30}10^{-30} \;+\; \tfrac{1}{42}10^{-42} \;+\; \ldots,$$

где коэффициенты $(1, -\frac{1}{2}, \frac{1}{6}, 0, -\frac{1}{30}, 0, \frac{1}{42})$ при 10^{-6k} образуют начало последовательности *чисел Бернулли* , которые еще появятся в гл.23. Мы отсылаем наших читателей к статье Борвейна, Борвейна и Дилчера [3], содержащей другие удивительные «совпадения» — и доказательства.

Приложение: Дзета-функция Римана

Дзета-функция Римана $\zeta(s)$ для действительных $s > 1$ определяется равенством

$$\zeta(s) \;:=\; \sum_{n\geq 1} \frac{1}{n^s}\,.$$

Из оценок чисел H_n (см. с. 19) следует, что ряд для $\zeta(1)$ расходится, но для любого действительного $s > 1$ он сходится. Дзета-функция имеет каноническое продолжение на всю комплексную плоскость (с одним простым полюсом в точке $s = 1$), которое можно построить с помощью разложений в степенные ряды. Получающаяся функция комплексной переменной имеет крайне важное значение для теории простых чисел. Укажем четыре разных связи $\zeta(s)$ с этой теорией.

(1) Замечательное тождество

$$\zeta(s) \;=\; \prod_{p} \frac{1}{1-p^{-s}}\,,$$

принадлежащее Эйлеру, эквивалентно тому, что каждое натуральное число единственным (!) образом разлагается на простые множители. Последний факт позволяет вывести тождество Эйлера как простое следствие разложения в геометрический ряд

$$\frac{1}{1-p^{-s}} \;=\; 1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\frac{1}{p^{3s}}+\dots$$

(2) Следующее замечательное рассуждение Дон Загира позволяет выразить $\zeta(4)$ через $\zeta(2)$. Для целых чисел $m, n \geqslant 1$ рассмотрим функцию

$$f(m,n) = \frac{2}{m^3 n} + \frac{1}{m^2 n^2} + \frac{2}{m n^3}\,.$$

Легко проверить, что для всех m и n

$$f(m,n) - f(m+n,n) - f(m,m+n) = \frac{2}{m^2 n^2}\,.$$

Суммируем эти равенства по всем $m, n \geqslant 1$. Если $i \neq j$, то (i,j) имеет вид либо $(m+n,n)$, либо $(m,m+n)$, где $m, n \geqslant 1$. Таким образом, в сумме левых частей сократятся все слагаемые $f(i,j)$ с $i \neq j$, и поэтому сумма левых частей равна

$$\sum_{n\geqslant 1} f(n,n) = \sum_{n\geqslant 1} \frac{5}{n^4} = 5\zeta(4).$$

Для суммы правых частей мы получаем

$$\sum_{m,n\geqslant 1} \frac{2}{m^2 n^2} = 2 \sum_{m\geqslant 1} \frac{1}{m^2} \cdot \sum_{n\geqslant 1} \frac{1}{n^2} = 2\zeta(2)^2,$$

и поэтому $5\zeta(4) = 2\zeta(2)^2$. Так как $\zeta(2) = \frac{\pi^2}{6}$, то $\zeta(4) = \frac{\pi^4}{90}$.

Другой вывод, использующий числа Бернулли, приведен в гл. 23.

(3) Уже давно известно, что если s — четное целое число, $s \geq 2$, то $\zeta(s)$ — рациональное кратное π^s и, следовательно, иррационально (см. гл.23). Однако иррациональность $\zeta(3)$ была доказана Роджером Апери лишь в 1979 году.

Несмотря на значительные усилия, картина относительно $\zeta(s)$ для других нечетных целых s, $s = 2t + 1 \geqslant 5$, остается весьма неполной. Недавно Кейт Болл и Тангуй Ривол [1] доказали, что бесконечно много значений $\zeta(2t + 1)$ являются иррациональными. Более того, хотя иррациональность $\zeta(s)$ не доказана ни для одного нечетного значения $s \geq 5$, Вадим Зудилин [9] доказал, что по меньшей мере одно из четырех значений $\zeta(5), \zeta(7), \zeta(9)$ или $\zeta(11)$ иррационально. Мы отсылаем читателя к замечательному обзору Фишлера [4].

(4) Описание расположения комплексных нулей дзета-функции составляет содержание «гипотезы Римана» — одной из наиболее известных и важных нерешенных задач математики. Она утверждает, что все нетривиальные нули $s \in \mathbb{C}$ дзета-функции удовлетворяют условию $\mathrm{Re}(s) = \frac{1}{2}$. (Дзета-функция обращается в нуль также во всех отрицательных четных целых числах, которые называются «тривиальными нулями».)

Совсем недавно Джеф Лагариас доказал неожиданную теорему о том, что гипотеза Римана эквивалентна следующему элементарному утверждению: для всех $n \geq 1$

$$\sum_{d \,|\, n} d \;\leq\; H_n \;+\; \exp(H_n) \log(H_n),$$

где, как и раньше, H_n есть n-е гармоническое число, и равенство выполняется только для $n = 1$.

Литература

[1] Ball K., Rivoal T. *Irrationalité d'une infinité de valeurs de la fonction zêta aux entiers impairs.* Inventiones math., **146** (2001), 193–207.

[2] Beukers F., Kolk J. A. C., Calabi E. *Sums of generalized harmonic series and volumes.* Nieuw Archief voor Wiskunde (4), **11** (1993), 217–224.

[3] Borwein J. M., Borwein P. B., Dilcher K. *Pi, Euler numbers, and asymptotic expansions.* Amer. Math. Monthly, **96** (1989), 681–687.

[4] Fischler S. *Irrationalité de valeurs de zêta (d'après Apéry, Rivoal, ...),* Bourbaki Seminar, No. 910, November 2002; Astérisque, **294** (2004), 27–62.

[5] Lagarias J. C. *An elementary problem equivalent to the Riemann hypothesis.* Amer. Math. Monthly, **109** (2002), 534–543.

[6] LeVeque W. J. *Topics in Number Theory, Vol. I.* Addison-Wesley, Reading MA, 1956.

[7] Яглом А.М., Яглом И.М. *Неэлементарные задачи в элементарном изложении.* ГИТТЛ, М., 1954.

[8] Zagier D. *Values of zeta functions and their applications.* Proc. First European Congress of Mathematics, Vol. II (Paris 1992), Progress in Math., **120**, Birkhäuser, Basel 1994, 497-512.

[9] Zudilin W. *Arithmetic of linear forms involving odd zeta values.* J. Théorie Nombres Bordeaux, **16** (2004), 251-291.

Геометрия

«Платоновы тела — детская игра!»

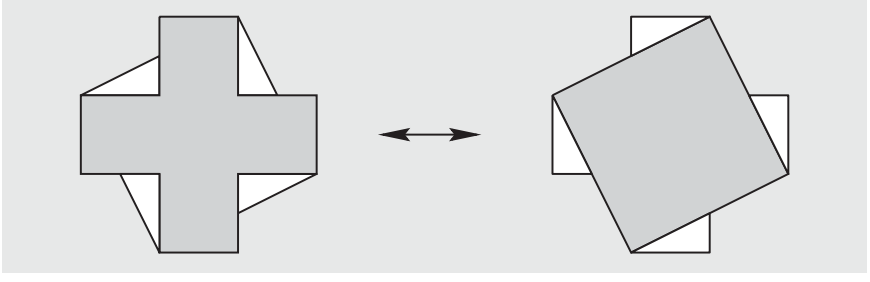
Глава 9 Третья проблема Гильберта: разбиения многогранников

Давид Гильберт

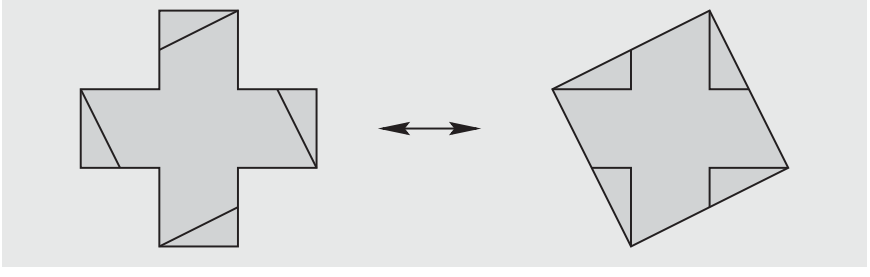
В 1900 году Давид Гильберт в своем знаменитом докладе на Международном конгрессе математиков в Париже ([5], [7*]) предложил — как третью из его двадцати трех проблем — построить

> *«два тетраэдра с равными основаниями и равными высотами, которые никаким способом нельзя разбить на конгруэнтные тетраэдры и которые нельзя дополнить конгруэнтными тетраэдрами до двух многогранников, разбиваемых на конгруэнтные тетраэдры».*

Эта проблема возникала в двух письмах Карла Фридриха Гаусса в 1844 году (опубликованных в 1900 году в собрании его сочинений). Существование разбиения тетраэдров равного объема на конгруэнтные части стало бы «элементарным» доказательством теоремы Евклида XII.5 [10*] о том, что пирамиды с равными основаниями и высотами имеют одинаковые объемы. Это дало бы элементарное определение объема многогранника, не зависящее от математического анализа и от рассуждений, связанных с непрерывностью. В планиметрии такое определение существует: теорема Бойяи – Гервина [1, §2.7] утверждает, что плоские многоугольники одновременно *равносоставлены* (их можно разбить на конгруэнтные треугольники) и *равнодополняемы* (их можно дополнить до конгруэнтных добавлением конгруэнтных треугольников) тогда и только тогда, когда их площади равны.



Крест и квадрат одинаковой площади равнодополняемы: добавляя к ним одни и те же 4 треугольника, мы делаем их равносоставленными (более того, конгруэнтными).



На самом деле крест и квадрат даже равносоставлены.

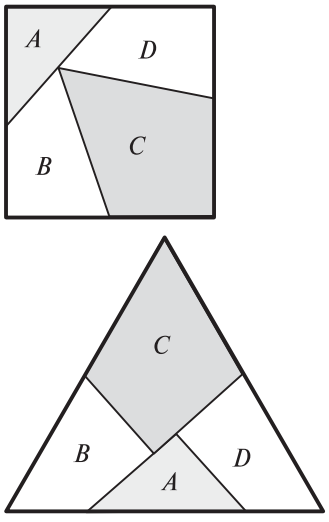
Гильберт, как видно из его формулировки проблемы, считал, что аналога этой теоремы для размерности 3 нет, и он был прав. Третья проблема Гильберта была полностью решена его учеником Максом Деном в двух работах: первая работа с доказательством существования не равносоставленных тетраэдров с одинаковыми основаниями и высотами появилась уже в 1900 году, а вторая работа, в которой рассматривается также равнодополняемость, появилась в 1902 году. Однако статьи Дена трудны для понимания, и довольно сложно убедиться в том, что его рассуждения обходят логические ловушки, в которые попадали другие: Рауль Брикар (в 1896(!) году он получил очень элегантное, но, к сожалению, ошибочное доказательство), Мешковский (в 1960) и, вероятно, кто-нибудь еще. Доказательство Дена было переработано и упрощено другими математиками, и после объединения идей нескольких авторов возникло «классическое доказательство», приведенное в книге Болтянского [1] о третьей проблеме Гильберта, а также в предыдущих изданиях нашей книги.

Далее, однако, мы используем решающее упрощение, найденное одесским математиком В. Ф. Каганом еще в 1903 году: из его замечания о целочисленности, которое мы назвали здесь «леммой о конусе», следует «лемма о бусинках» (приведенная здесь в последней версии, предложенной Бенко), из которой выводится корректное и полное доказательство «условия Брикара» (содержавшегося в работе Брикара 1896 года). После его применения к нескольким примерам мы легко получим решение третьей проблемы Гильберта.

В приложении к этой главе содержатся основы теории полиэдров.

Как и ранее, мы называем два полиэдра P и Q *равносоставленными*, если их можно разбить на такие конечные множества полиэдров $P_1, \dots, P_n$ и $Q_1, \dots, Q_n$, что при любом i полиэдры P_i и Q_i конгруэнтны. Два полиэдра называются *равнодополняемыми*, если существуют равносоставленные полиэдры $\widetilde{P} = P_1'' \cup \ldots \cup P_n''$ и $\widetilde{Q} = Q_1'' \cup \ldots \cup Q_n''$, у которых есть также содержащие P и Q разбиения вида $\widetilde{P} = P \cup P_1' \cup \ldots \cup P_m'$ и $\widetilde{Q} = Q \cup Q_1' \cup \ldots \cup Q_m'$, где полиэдры P_k' и Q_k' конгруэнтны при любом k (примером являются большие фигуры на предыдущей странице). Из доказанной в 1844 году теоремы Герлинга [1, § 12] следует, что для этих определений не существенно, считаются или нет конгруэнтными фигуры, симметричные относительно прямой.

Аналогично определяются равносоставленность и равнодополняемость для плоских многоугольников.

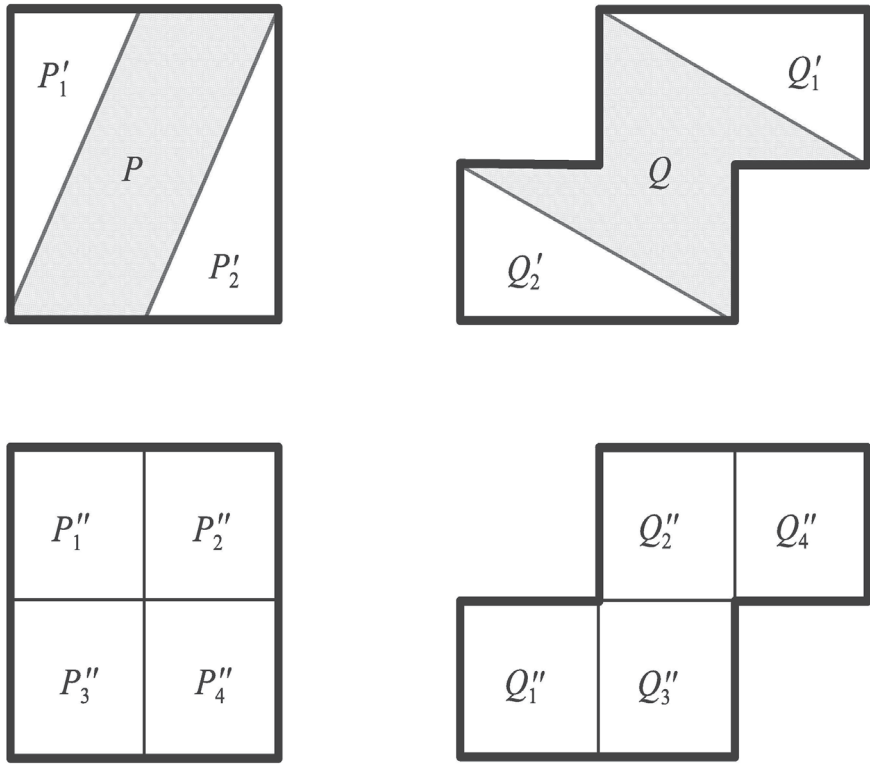


Эти разбиения квадрата и равностороннего треугольника на 4 попарно одинаковых куска построил Г.Дьюдени в 1902 году.
Короткий отрезок в середине равностороннего треугольника — это пересечение кусков A и C, но оно не является стороной ни одного из них.

Очевидно, равносоставленные объекты являются равнодополняемыми (в этом случае $m = 0$), но обратное далеко не очевидно. Мы используем «условие Брикара» для того, чтобы убедиться в справедливости предположения Гильберта о том, что некоторые тетраэдры равного объема являются не равнодополняемыми, и, в частности, не равносоставленными.

Перед началом работы с трехмерными полиэдрами мы докажем лемму о бусинках, которая интересна также для плоских разбиений. В ней рассматриваются *сегменты* разбиения: в любом разбиении ребра одного куска могут разбиваться на части вершинами или ребрами других кусков; эти части мы называем сегментами. Таким образом, в двумер-

ном случае любой конец сегмента является вершиной какого-нибудь куска. В трехмерном случае концом сегмента может быть также пересечение двух ребер. В любом случае все внутренние точки сегмента принадлежат одному и тому же множеству ребер кусков.



Для равнодополняемых параллелограмма P и невыпуклого шестиугольника Q на рисунке показаны 4 разных разбиения.

Лемма о бусинках. *Если P и Q равносоставлены, то можно разместить на каждом сегменте разбиений $P = P_1 \cup \cdots \cup P_N$ и $Q = Q_1 \cup \cdots \cup Q_n$ положительное число бусинок (т. е. приписать каждому сегменту натуральное число) так, чтобы при любом k на каждом ребре куска P_k оказалось такое же число бусинок, как на соответствующем ребре Q_k.*

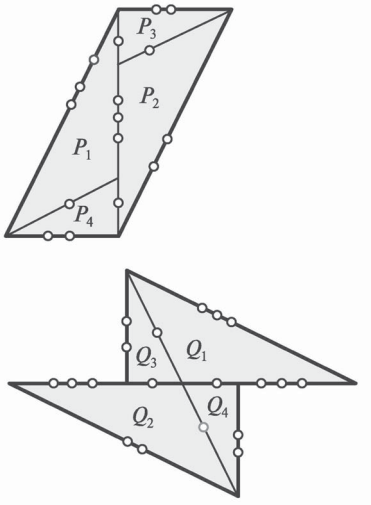
■ **Доказательство.** Припишем переменную x_i каждому сегменту в разбиении P и переменную y_j каждому ребру в разбиении Q. Теперь нам нужно найти такие положительные *целочисленные* значения переменных x_i и y_j, что сумма x_i-переменных, соответствующих сегментам любого ребра любого P_k равна сумме y_j-переменных, приписанных сегментам соответствующего ребра Q_k. Значит, должны выполняться условия вида «сумма некоторых x_i-переменных равна сумме некоторых y_j-переменных», а именно,

$$\sum_{i:\, s_i \subseteq e} x_i - \sum_{j:\, s_j' \subseteq e'} y_j = 0,$$

где s_i — все части, на которые разбито ребро $e \subset P$, а s_j' — все части, на которые разбито соответствующее ребро $e' \subset Q$. Это линейное уравнение с целыми коэффициентами.

Заметим, что положительные *действительные* числа, удовлетворяющие всем этим условиям, существуют: например, (действительные) длины всех сегментов! Следующая лемма показывает, что сделанное замечание на самом деле завершает доказательство. □

Изображенные на предыдущем рисунке многоугольники P и Q являются даже равносоставленными. На рисунке на полях показаны их разбиения и возможное расположение бусинок.



Лемма о конусе. *Если однородная система линейных уравнений с целыми коэффициентами имеет положительное* ***действительное*** *решение, то она имеет также положительное* ***целочисленное*** *решение.*

■ **Доказательство.** Название леммы оправдывается тем, что множество

$$C = \{\mathbf{x} \in \mathbb{R}^{\mathbb{N}} : \mathbb{A}\mathbf{x} = \mathbf{0},\ \mathbf{x} > \mathbf{0}\},$$

где $A \in \mathbb{Z}^{\mathbb{M}\times\mathbb{N}}$ — целочисленная матрица, определяет (открытый) рациональный конус. Нам нужно показать, что если он не пуст, то он содержит также целочисленные точки: $C \cap \mathbb{N}^{\mathbb{N}} \neq \varnothing$.

Если C не пусто, то не пусто и множество $\overline{C} = \{\mathbf{x} \in \mathbb{R}^{\mathbb{N}} : \mathbb{A}\mathbf{x} = \mathbf{0},\ \mathbf{x} > \mathbf{1}\}$, где $\mathbf{1}$ обозначает вектор, все координаты которого равны 1. В самом деле, для любого положительного вектора существует число, после умножения на которое все его координаты окажутся не меньше 1. Поэтому достаточно показать, что $\overline{C} \subseteq C$ содержит какую-нибудь точку с *рациональными* координатами, поскольку тогда умножение на наименьшее общее кратное знаменателей всех координат даст точку в $\overline{C} \subseteq C$ с целочисленными координатами.

Это можно доказать разными способами. Мы пройдем по хорошо утоптанному пути, который впервые использовали Фурье и Мотцкин [8, лекция 1]: с помощью «исключения Фурье–Мотцкина» мы покажем, что лексикографически наименьшее решение системы

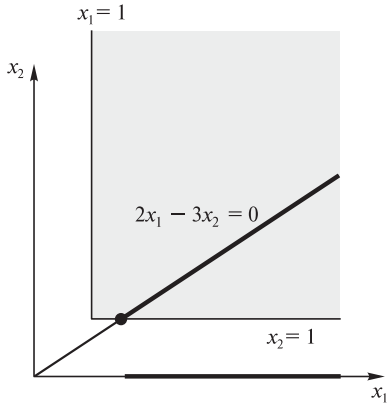
$$A\mathbf{x} = \mathbf{0},\ \mathbf{x} \geqslant \mathbf{1},$$

существует и является рациональным, если матрица A целочисленная.

Действительно, любое линейное уравнение $\mathbf{a^T x} = \mathbf{0}$ эквивалентно системе из двух неравенств $\mathbf{a^T x} \geqslant \mathbf{0}$, $-\mathbf{a^T x} \geqslant \mathbf{0}$. (Здесь $\mathbf{a}$ обозначает вектор-столбец и $\mathbf{a^T}$ — его транспонирование.) Значит, достаточно доказать, что любая система вида

$$A\mathbf{x} \geqslant \mathbf{b}, \quad \mathbf{x} \geqslant \mathbf{1},$$

с целочисленными A и $\mathbf{b}$ имеет лексикографически наименьшее решение, являющееся рациональным, если эта система имеет хотя бы одно действительное решение.

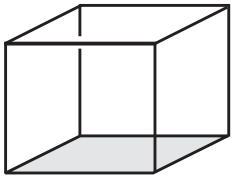


Пример: Здесь $\overline{C}$ задано условиями $2x_1 - 3x_2 = 0$, $x_i \geqslant 1$. Исключение x_2 дает неравенство $x_1 \geqslant \frac{3}{2}$. Лексикографически минимальным решением системы является $(\frac{3}{2}, 1)$.

Для этого воспользуемся индукцией по N. Случай $N = 1$ очевиден. В случае $N > 1$ представим все неравенства, содержащие x_N, в виде нижних или верхних оценок для x_N через $x_1, \ldots, x_{N-1}$ (в частности, среди них будет неравенство $x_N \geqslant 1$). Теперь образуем новую систему $A'\mathbf{x}' \geqslant \mathbf{b}'$, $\mathbf{x}' \geqslant \mathbf{1}$, относительно $N-1$ неизвестных, состоящую из всех неравенств системы $A\mathbf{x} \geqslant \mathbf{b}$, в которые не входит x_N, а также из всех

неравенств, получающихся из того, что каждая верхняя оценка для x_N (если такие существуют) должна быть не меньше каждой нижней оценки для x_N (что включает условие $x_N \geqslant 1$). Эта система относительно $N-1$ неизвестных имеет действительное решение, и по предположению индукции она имеет лексикографически наименьшее решение x'_*, которое является рациональным. Тогда легко найти наименьшее значение x_N, совместимое с этим решением x'_*; оно определяется линейным уравнением или неравенством с целыми коэффициентами и поэтому тоже является рациональным числом. □

Теперь перейдем к разложениям трехмерных полиэдров. Важную роль в следующей теореме играют *двугранные углы*, т. е. углы между соседними гранями.

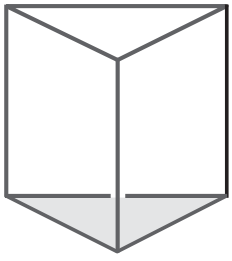


В кубе все двугранные углы равны $\frac{\pi}{2}$.

Теорема («условие Брикара»). *Если трехмерные полиэдры P и Q с двугранными углами $\alpha_1, \ldots, \alpha_r$ и $\beta_1, \ldots, \beta_s$ соответственно являются равносоставленными, то существуют такие положительные целые числа m_i и n_j, что*

$$m_1\alpha_1 + \ldots + m_r\alpha_r = n_1\beta_1 + \ldots + n_s\beta_s + k\pi.$$

Это верно и для более общего случая равнодополняемых P и Q.



В призме с правильным треугольником в основании двугранные углы равны $\frac{\pi}{3}$ и $\frac{\pi}{2}$.

■ **Доказательство.** Пусть сначала P и Q равносоставлены и имеют разложения $P = P_1 \cup \ldots \cup P_n$ и $Q = Q_1 \cup \ldots \cup Q_n$, в которых P_i конгруэнтен Q_i. Припишем положительные числа бусинок каждому сегменту в обоих разложениях, как в лемме о бусинках.

Пусть Σ_1 — это сумма всех двугранных углов при всех бусинках на ребрах разложения P. Если на ребре куска P_i находится несколько бусинок, то двугранный угол при этом ребре появится в сумме Σ_1 несколько раз.

Если бусинка содержится в общем ребре нескольких кусков, то ей в сумме соответствует несколько двугранных углов, которые измеряются плоскими углами в плоскости, проходящей через бусинку перпендикулярно ее сегменту. Если сегмент содержится в ребре P, то сложение дает (внутренний) двугранный угол α_j при этом ребре. Сложение дает π, если сегмент лежит на границе P, но не на ребре. Если бусинка/сегмент лежит внутри P, то сумма двугранных углов дает 2π или π. (Последняя ситуация возникает в случае, когда бусинка лежит внутри грани одного из кусков P_i.)

Таким образом, мы получаем представление

$$\Sigma_1 = m_1\alpha_1 + \ldots + m_r\alpha_r + k_1\pi$$

с положительными целыми m_j $(1 \leqslant j \leqslant r)$ и неотрицательным k_1. Аналогично, для суммы Σ_2 всех углов при бусинках в разложении Q получаем

$$\Sigma_2 = n_1\beta_1 + \ldots + n_s\beta_s + k_2\pi$$

с положительными целыми n_j $(1 \leqslant j \leqslant s)$ и неотрицательным k_2.

Мы можем также получить суммы Σ_1 и Σ_2 сложением всех вкладов отдельных кусков P_i и Q_i. Так как P_i и Q_i конгруэнтны, мы измеряем одни и те же двугранные углы при соответствующих гранях, и лемма

о бусинках гарантирует, что мы получим одинаковые числа бусинок в разложениях P и Q на соответствующих ребрах. Следовательно, имеет место равенство $\Sigma_1 = \Sigma_2$, что соответствует условию Брикара (с $k = k_2 - k_1 \in \mathbb{Z}$) в случае равносоставленности.

Пусть теперь P_i и Q_i равнодополняемы, т. е. имеют место разложения

$$\widetilde{P} = P \cup P'_1 \cup \ldots \cup P'_m \quad \text{и} \quad \widetilde{Q} = Q \cup Q'_1 \cup \ldots \cup Q'_m,$$

где P'_i и Q'_i конгруэнтны, а $\widetilde{P}$ и $\widetilde{Q}$ равносоставлены:

$$\widetilde{P} = P''_1 \cup \ldots \cup P''_m \quad \text{и} \quad \widetilde{Q} = Q''_1 \cup \ldots \cup Q''_m,$$

где P''_i и Q''_i конгруэнтны (как на рисунке на стр. с Леммой о бусинках). Снова, используя лемму о бусинках, разместим бусинки на всех сегментах во всех четырех разложениях, потребовав дополнительно, чтобы на каждом ребре $\widetilde{P}$ в обоих его разложениях находилось одно и то же число бусинок, и аналогично для $\widetilde{Q}$. (Доказательство леммы о бусинках с помощью леммы о конусе можно провести и с этим дополнительным условием!) Обозначим суммы углов при бусинках через Σ'_1, Σ'_2, Σ''_1 и Σ''_2 соответственно.

Суммы углов Σ''_1 и Σ''_2 построены по разложениям разных полиэдров $\widetilde{P}$ и $\widetilde{Q}$ в *одно и то же множество кусков*, поэтому, как и раньше, мы получаем равенство $\Sigma''_1 = \Sigma''_2$.

Суммы углов Σ'_1 и Σ''_1 построены по разным разложениям *одного и того же* полиэдра $\widetilde{P}$. Так как мы расположили одно и то же число бусинок на ребрах $\widetilde{P}$ в обоих разложениях, из приведенных выше рассуждений следует, что $\Sigma'_1 = \Sigma''_1 + l_1\pi$ при некотором целом $l_1 \in \mathbb{Z}$. Аналогично приходим к равенству $\Sigma'_2 = \Sigma''_2 + l_2\pi$ при некотором целом $l_2 \in \mathbb{Z}$. Таким образом,

$$\Sigma'_2 = \Sigma'_1 + l\pi \quad \text{при} \quad l = l_2 - l_1 \in \mathbb{Z}.$$

Но Σ'_1 и Σ'_2 построены по разложениям $\widetilde{P}$ и $\widetilde{Q}$ на одни и те же куски, за исключением того, что в первом случае в качестве куска используется P, а во втором — Q. Поэтому, вычитая вклады P'_i и Q'_i из соответствующих частей равенства, мы приходим к требуемому заключению: вклады P и Q в соответствующие суммы углов

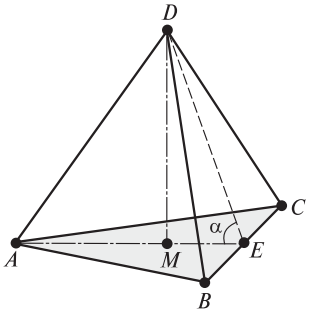
$$m_1\alpha_1 + \ldots + m_r\alpha_r \quad \text{и} \quad n_1\beta_1 + \ldots + n_s\beta_s$$

(где m_j — число бусинок на ребрах с двугранным углом α_j в P, а n_j — число бусинок на ребрах с двугранным углом β_j в Q) различаются на целое кратное π, именно, на $l\pi$. □

Используя условие Брикара, мы получим полное решение третьей проблемы Гильберта; для этого нужно найти двугранные углы в нескольких примерах.

Пример 1. С помощью чертежа на полях найдем двугранные углы правильного тетраэдра T_0 с длинами сторон ℓ. Центр M треугольника в основании делит высоту AE в отношении 1:2, и так как $|AE| = |DE|$, мы находим, что $\cos\alpha = \frac{1}{3}$, и поэтому

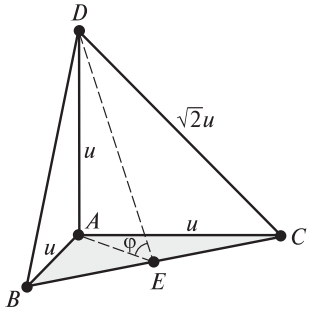
$$\alpha = \arccos\tfrac{1}{3}.$$



Тем самым мы доказали, что *правильный тетраэдр и куб не являются ни равносоставленными, ни равнодополняемыми.* Действительно, все двугранные углы куба равны $\frac{\pi}{2}$, и согласно условию Брикара в случае равносоставленности или равнодополняемости при некоторых положительных целых m_1, n_1 и целом k должно выполняться равенство

$$m_1 \arccos \tfrac{1}{3} = n_1 \tfrac{\pi}{2} + k\pi.$$

Но это невозможно, так как мы знаем из теоремы 3 главы 7, что число $\frac{1}{\pi} \arccos \frac{1}{3}$ иррационально.



Пример 2. Пусть T_1 — тетраэдр, натянутый на три попарно ортогональных ребра AB, AC и AD длины u. Этот тетраэдр имеет три прямых двугранных угла и еще три равных двугранных угла, величину φ которых мы вычислим с помощью чертежа на полях. Имеем:

$$\cos\varphi \;=\; \frac{|AE|}{|DE|} \;=\; \frac{\frac{1}{2}\sqrt{2}u}{\frac{1}{2}\sqrt{3}\,\sqrt{2}u} \;=\; \frac{1}{\sqrt{3}}\,.$$

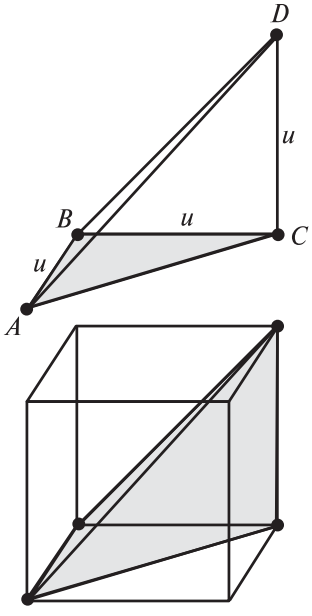
Отсюда следует, что

$$\varphi \;=\; \arccos\frac{1}{\sqrt{3}}\,.$$

Значит, все двугранные углы в T_1 равны либо π, либо $\frac{\pi}{2}$, либо $\arccos\frac{1}{\sqrt{3}}$. Условие Брикара показывает, что этот тетраэдр тоже не равнодополняем с кубом того же объема; теперь это следует из иррациональности числа

$$\tfrac{\pi}{2} \arccos \tfrac{1}{\sqrt{3}}\,,$$

что было доказано в главе 7 (в теореме 3 нужно положить $n = 3$).



Пример 3. Пусть, наконец, T_2 — тетраэдр, имеющий цепочку из трех взаимно ортогональных последовательных ребер AB, BC и CD («ортосхема») одинаковой длины u.

Углы этого тетраэдра легко найти (три угла равны $\frac{\pi}{2}$, два угла равны $\frac{\pi}{4}$ и один угол равен $\frac{\pi}{6}$), если заметить, что куб с ребром длины u можно разбить на 6 тетраэдров такого вида (3 конгруэнтные копии и 3 их зеркальных образа)[1]. Таким образом, все двугранные углы в T_2 являются рациональными кратными π; поэтому, как и выше, из результатов об иррациональности в главе 7 и условия Брикара следует, что T_2 не является ни равносоставленным, ни равнодополняемым с T_0 и T_1.

Это решает третью проблему Гильберта, так как T_1 и T_2 имеют конгруэнтные основания и равные высоты.

Приложение: политопы и многогранники

Выпуклый политоп в пространстве $\mathbb{R}^d$ есть выпуклая оболочка конечного множества $S = \{\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n\}$, т. е. множество вида

$$P \;=\; \operatorname{conv}(S) \;:=\; \Big\{ \sum_{i=1}^{n} \lambda_i \boldsymbol{s}_i : \lambda_i \ge 0,\ \sum_{i=1}^{n} \lambda_i = 1 \Big\}.$$

[1] Эти 6 тетраэдров порождаются диагональю куба и шестью его ребрами, не имеющими общих точек с этой диагональю. — *Прим. ред.*

Политопы — это хорошо известные объекты: простыми примерами являются выпуклые *многоугольники* (двумерные выпуклые политопы) и выпуклые *многогранники* (трехмерные выпуклые политопы).

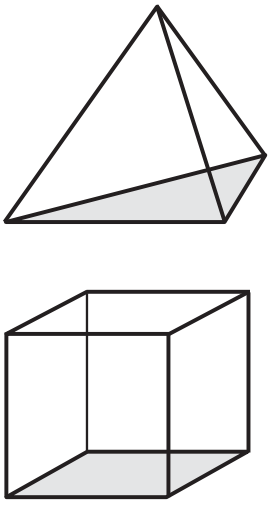
Существует несколько типов многогранников, которые естественным образом обобщаются на более высокие размерности. Например, если S — аффинно независимое множество[2] из $d+1$ точек, то $\mathrm{conv}(S)$ есть *d-мерный симплекс* (или *d-симплекс*). В случае $d=2$ это треугольник, для $d=3$ — тетраэдр. Аналогично, квадраты и кубы являются частными случаями d-кубов, примером которых является *единичный d-куб* $C_d = [0,1]^d \subseteq \mathbb{R}^d$.

Общий политоп определяется как конечное объединение выпуклых политопов. В этой книге невыпуклые многогранники появятся в гл. 13 в связи с теоремой Коши о жесткости, а невыпуклые многоугольники — в гл. 12 в связи с теоремой Пика и еще раз в гл. 35, когда мы будем обсуждать теорему о художественной галерее.

Выпуклые политопы можно определить другим способом как ограниченные множества решений конечных систем линейных неравенств. Значит, каждый выпуклый политоп $P \subseteq \mathbb{R}^d$ имеет представление вида

$$P \;=\; \{\boldsymbol{x} \in \mathbb{R}^d : A\boldsymbol{x} \le \boldsymbol{b}\}$$

с некоторыми матрицей $A \in \mathbb{R}^{m\times d}$ и вектором $\boldsymbol{b} \in \mathbb{R}^m$. Другими словами, P есть множество решений системы m линейных неравенств $\boldsymbol{a}_i^T\boldsymbol{x} \le b_i$, где $\boldsymbol{a}_i^T$ есть i-я строка матрицы A. Обратно, каждое ограниченное множество решений является выпуклым политопом, и поэтому его можно представить в виде выпуклой оболочки конечного множества точек.



Хорошо известные политопы: тетраэдр, куб

Для многоугольников и многогранников мы используем обычные понятия *вершины*, *ребра* и *2-грани*. Для выпуклого политопа $P \in \mathbb{R}^d$ его *грань* есть подмножество $F \subseteq P$ вида $P \cap \{\boldsymbol{x} \in \mathbb{R}^d : \boldsymbol{a}^T\boldsymbol{x} = b\}$, где $\boldsymbol{a}^T\boldsymbol{x} \le b$ — линейное неравенство, справедливое для всех точек $\boldsymbol{x} \in P$.

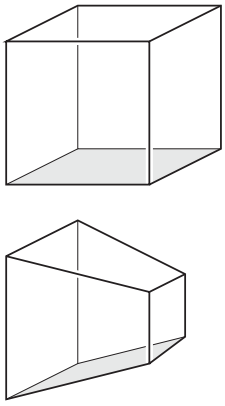
Все грани политопа являются политопами. Множество V вершин (0-мерных граней) выпуклого политопа является также минимальным по включению множеством, для которого $\mathrm{conv}(V) = P$. Если $P \subseteq \mathbb{R}^d$ есть d-мерный политоп, то его *гиперграни* ($(d-1)$-мерные грани) определяют минимальное множество гиперплоскостей и, следовательно, полупространств, которые содержат P и пересечение которых есть P. Отсюда, в частности, вытекает следующий факт, который нам потребуется позднее. Пусть F — гипергрань политопа P; обозначим через H_F определенную ею гиперплоскость, а через H_F^+ и H_F^- — два замкнутых полупространства с границей H_F. Тогда одно из этих двух полупространств содержит P (а другое не содержит).

Пермутоэдрон имеет 24 вершины, 36 ребер и 14 граней

Граф $G(P)$ выпуклого политопа P задается множеством вершин V и множеством E ребер (одномерных граней). Если P имеет размерность 3, то этот граф — плоский и приводит к знаменитой «формуле Эйлера для многогранников» (см. гл. 12).

Два политопа $P, P' \subseteq \mathbb{R}^d$ называются *конгруэнтными*, если существует сохраняющее длины аффинное отображение, которое преобразует P в P'. Такое отображение может обратить ориентацию простран-

[2] Ни одна его точка не лежит в аффинном подпространстве, натянутом на остальные точки. — *Прим. перев.*



Комбинаторно эквивалентные политопы

ства, как отражение P относительно гиперплоскости, переводящее политоп P в его зеркальный образ. Политопы P, P' *комбинаторно эквивалентны*, если существует биекция множества граней политопа P в множество граней политопа P', сохраняющая размерность и пересечения граней. Понятие комбинаторной эквивалентности слабее понятия конгруэнтности. Например, изображенные на полях единичный и «скошенный» кубы комбинаторно эквивалентны (и, следовательно, их можно называть кубами), но они, конечно, не конгруэнтны.

Политоп (или более общее подмножество в $\mathbb{R}^d$) называется *центрально симметричным*, если существует такая точка $\boldsymbol{x}_0 \in \mathbb{R}^d$, что

$$\boldsymbol{x}_0 + \boldsymbol{x} \in P \quad \Longleftrightarrow \quad \boldsymbol{x}_0 - \boldsymbol{x} \in P.$$

В этом случае мы называем $\boldsymbol{x}_0$ *центром* политопа P.

Литература

[1] Болтянский В. Г. *Третья проблема Гильберта.* М.: Наука, 1977.

[2] Benko D. *A new approach to Hilbert's third problem.* Amer. Math. Monthly, **144**, 2007, 665–676.

[3] Dehn M. *Ueber raumgleiche Polyeder.* Nachrichten von der Königl. Gesellschaft der Wissenschaften, Mathematisch-physikalische Klasse, 1900, 345–354.

[4] Dehn M. *Ueber den Rauminhalt.* Mathematische Annalen, **55**, 1902, 465–478.

[5] Gauss C. F. *«Congruenz und Symmetrie»: Briefwechsel mit Gerling.* pp. 240–249, in: Werke, Band VIII, Königl. Gesellschaft der Wissenschaften zu Göttingen; B. G. Teubner, Leipzig, 1900.

[6] Hilbert D. *Mathematical Problems.* Lecture delivered at the International Congress of Mathematicians at Paris in 1900, Bulletin Amer. Math. Soc., **8**, 1902, 437–479.

[7] Kagan B. *Über die Transformation der Polyeder.* Mathematische Annalen, **57**, 1903, 421–424.

[8] Ziegler G. M. *Lectures on Polytopes.* Graduate Texts in Mathematics, **152**, Springer-Verlag, New York, 1995/1998.

[9*] Александров П. С. , ред. *Проблемы Гильберта.* М.: Наука, 1969.

[10*] Евклид. *Начала, кн. XI–XV.* М.-Л.: ГИТТЛ, 1950.

Прямые на плоскости и разложения графов

Глава 10

Возможно, наиболее известная задача о конфигурациях прямых была поставлена Сильвестром в 1893 году [5] в колонке для математических задач.

QUESTIONS FOR SOLUTION.

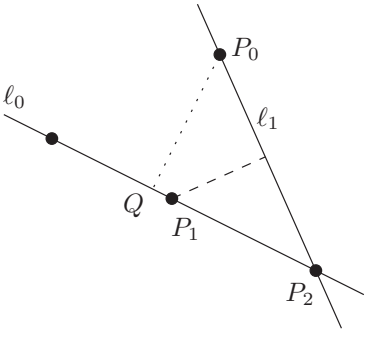
11851. (Professor Sylvester.)—Prove that it is not possible to arrange any finite number of real points so that a right line through every two of them shall pass through a third, unless they all lie in the same right line.

Не ясно, знал ли сам Сильвестр решение этой задачи; корректное доказательство примерно через сорок лет нашел Тибор Галлаи (Грюнвальд) [3]. Поэтому следующую теорему называют теоремой Сильвестра–Галлаи. После доказательства Галлаи появилось еще несколько других, но приведенное ниже рассуждение, принадлежащее Л. М. Келли (см. [2]), возможно, «просто наилучшее».

Дж. Сильвестр

Теорема 1. *Для любого множества из $n \geq 2$ точек на плоскости, не лежащих на одной прямой, найдется прямая, содержащая ровно две точки.*

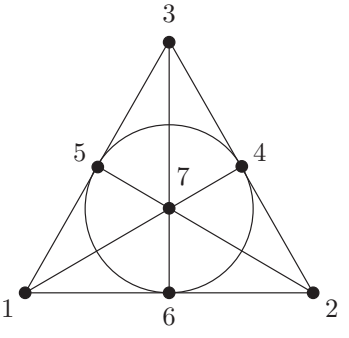
■ **Доказательство.** Пусть $\mathcal{P}$ — заданное множество точек. Рассмотрим множество $\mathcal{L}$ всех прямых, которые проходят, по крайней мере, через две точки из $\mathcal{P}$. Из всех пар (P, ℓ), где $\ell \in \mathcal{L}$, $P \in \mathcal{P}$, P не лежит на l, выберем такую пару (P_0, ℓ_0), что расстояние от P_0 до ℓ_0 минимальное. Пусть Q — точка на ℓ_0, ближайшая к P_0 (т. е. основание перпендикуляра, опущенного из P_0 на ℓ_0).



Утверждение. *Прямая ℓ_0 — искомая.*

Допустим, что это не так. Тогда ℓ_0 содержит по крайней мере три точки из $\mathcal{P}$, и тогда две из них (обозначим их P_1 и P_2) расположены по одну сторону от Q. Предположим, что P_1 находится между Q и P_2, причем P_1, возможно, совпадает с Q. (Чертеж на полях поясняет расположение точек.)

Отсюда следует, что расстояние от P_1 до прямой ℓ_1, проходящей через P_0 и P_2, меньше расстояния от P_0 до ℓ_0, а это противоречит нашему выбору ℓ_0 и P_0. □



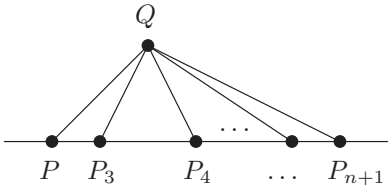
В доказательстве мы использовали аксиомы планиметрии: метрические аксиомы (кратчайшее расстояние) и аксиомы порядка (P_1 лежит между Q и P_2). Действительно ли необходимы эти свойства, кроме обычных аксиом инцидентности точек и прямых? Да, некоторые дополнительные условия требуются, как показывает известная *плоскость Фано*, изображенная на полях. Здесь $\mathcal{P} = \{1, 2, \ldots, 7\}$ и $\mathcal{L}$ состоит из семи трехточечных прямых, включая и «прямую» $\{4, 5, 6\}$. Любые две точки определяют единственную прямую, так что аксиомы инцидентности выполняются, но двухточечные прямые отсутствуют. Поэтому согласно теореме Сильвестра–Галлаи конфигурацию Фано нельзя

вложить в евклидову плоскость так, чтобы каждая из семи коллинеарных в конфигурации Фано троек лежала на своей прямой: одна из «прямых» должна быть «скрученной».

Кокстер [2] показал, однако, что доказательство теоремы Сильвестра–Галлаи можно провести, добавив к аксиомам инцидентности аксиомы порядка. Таким образом, существует доказательство, которое не использует метрические свойства; см. также доказательство в гл. 12, основанное на формуле Эйлера.

Из теоремы Сильвестра–Галлаи непосредственно вытекает и другой известный результат о точках и прямых на плоскости, принадлежащий Паулю Эрдёшу и Николасу Г. де Брёйну [1]. Но, как заметили еще Эрдёш и де Брёйн, этот результат справедлив для более общих произвольных систем точек и прямых. Чуть позже мы обсудим этот более общий результат.

Теорема 2. *Пусть $\mathcal{P}$ — множество из $n \geq 3$ точек на плоскости, не лежащих на одной прямой. Тогда множество $\mathcal{L}$ прямых, проходящих по крайней мере через две точки из $\mathcal{P}$, содержит не менее n прямых.*



■ **Доказательство.** В случае $n = 3$ доказательство не требуется. Далее применим индукцию по n. Пусть $|\mathcal{P}| = n+1$. Согласно предыдущей теореме существует прямая $\ell_0 \in \mathcal{L}$, содержащая ровно две точки P и Q из $\mathcal{P}$. Рассмотрим множество $\mathcal{P}' = \mathcal{P}\backslash\{Q\}$ и множество $\mathcal{L}'$ прямых, определяемое точками $\mathcal{P}'$. Если не все точки $\mathcal{P}'$ лежат на одной и той же прямой, то в силу индукции $|\mathcal{L}'| \geq n$ и, следовательно, $|\mathcal{L}| \geq n+1$, так как входящая в $\mathcal{L}$ прямая ℓ_0 не принадлежит $\mathcal{L}'$. Если, с другой стороны, все точки $\mathcal{P}'$ лежат на одной прямой ℓ, то через Q проходит «пучок» из n прямых, который вместе с ℓ образует в точности $n+1$ прямых. □

Теперь, как и обещали, докажем утверждение, применимое к значительно более общим «геометриям инцидентности».

Теорема 3. *Пусть множество X состоит из $n \geq 3$ элементов, а $A_1, \ldots, A_m$ — такие собственные подмножества множества X, что каждая пара элементов X содержится только в одном из подмножеств A_i. Тогда $m \geq n$.*

■ **Доказательство.** Следующее доказательство, приписываемое как Моцкину, так и Конвею, очень короткое и в полном смысле слова вдохновляющее. Пусть $x \in X$ и r_x — число множеств A_i, содержащих x. (Заметим, что $2 \leq r_x < m$ в силу условий теоремы[1].) Далее, если $x \notin A_i$, то $r_x \geq |A_i|$, так как $|A_i|$ множеств, содержащих x и один из элементов A_i, должны быть разными. Предположим, что $m < n$, тогда $m|A_i| < n\,r_x$, так что $m(n - |A_i|) > n(m - r_x)$ при $x \notin A_i$, и

$$1 = \sum_{x\in X} \frac{1}{n} = \sum_{x\in X} \sum_{i:x\notin A_i} \frac{1}{n(m-r_x)} > \sum_{i=1}^{m} \sum_{x:x\notin A_i} \frac{1}{m(n-|A_i|)} = \sum_{i=1}^{m} \frac{1}{m} = 1,$$

что невозможно. □

[1] Если $r_x = m$, то $x \in A_i$ при $i = 1, \ldots, m$. Пусть $y \in A_1$, $z \in X \setminus A_1$ и A_j — множество, содержащее пару y, z. Тогда $j \neq 1$, $x \in A_j$, т. е. пара x, y входит как в A_1, так и в A_j. — *Прим. ред.*

Существует еще одно очень короткое доказательство этой теоремы, использующее линейную алгебру. Пусть B — *матрица инцидентности* набора $(X; A_1, \ldots, A_m)$, т. е. строки матрицы B нумеруются элементами множества X, а столбцы — множествами $A_1, \ldots, A_m$, и

$$B_{x,A} := \begin{cases} 1, & \text{если} \quad x \in A, \\ 0, & \text{если} \quad x \notin A. \end{cases}$$

Рассмотрим произведение[2] BB^T. Если $x, x' \in X$ и $x \neq x'$, то $(BB^T)_{xx'} = 1$, так как пара x, x' содержится лишь в одном из множеств A_i. Поэтому

$$BB^T = \begin{pmatrix} r_{x_1}-1 & 0 & \ldots & 0 \\ 0 & r_{x_2}-1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \ldots & 0 & r_{x_n}-1 \end{pmatrix} + \begin{pmatrix} 1 & 1 & \ldots & 1 \\ 1 & 1 & & \vdots \\ \vdots & & \ddots & \\ 1 & \ldots & & 1 \end{pmatrix},$$

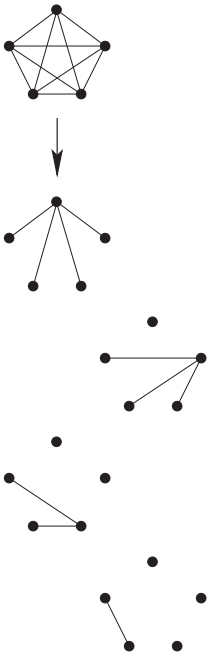
где r_x — те же, что и выше. Так как первая матрица положительно определена (она имеет лишь положительные собственные числа), а вторая матрица неотрицательно определена (ее собственные числа принимают значения n и 0), то BB^T положительно определена и поэтому, в частности, обратима, в силу чего $\operatorname{rank}(BB^T) = n$. Отсюда следует, что ранг $(n \times m)$-матрицы B не меньше n. Значит, $n \leq m$, поскольку ранг матрицы не может превышать число ее столбцов.

Выйдем немного за пределы рассмотренных задач и обратимся к теории графов. (Сводка основных понятий, связанных с графами, приводится в приложении к этой главе.) Несложно показать равносильность следующего утверждения и теоремы 3.

> *Если полный граф K_n разложен*[3] *на m клик, отличных от K_n, причем каждое ребро принадлежит единственной клике, то $m \geq n$.*

Действительно, достаточно отождествить множество X из теоремы 3 с множеством вершин графа K_n, а множества A_i — с множествами вершин клик.

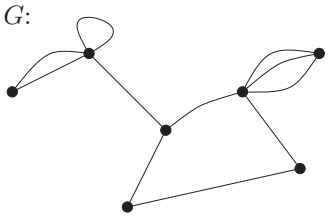
Наша следующая задача — найти такое разложение K_n на полные двудольные графы, что каждое его ребро принадлежит ровно одному из этих графов. Простой способ сделать это состоит в следующем. Занумеруем вершины K_n числами от 1 до n. Вначале возьмем полный двудольный граф, соединив вершину 1 со всеми другими вершинами. Таким образом мы получим граф $K_{1,n-1}$, который называется *звездой*. Далее, соединив вершину 2 с вершинами $3, \ldots, n$, получим звезду $K_{1,n-2}$. Продолжая подобным образом, мы разложим K_n на звезды $K_{1,n-1}, K_{1,n-2}, \ldots, K_{1,1}$. Это разложение использует $n-1$ полных двудольных графов. Можно ли разложить K_n на меньшее число графов? Следующий результат Рона Грэхема и Генри О. Поллака [4] показывает, что нельзя.



Разложение K_5 на четыре полных двудольных графа.

[2] B^T — транспонированная матрица B, $(BB^T)_{xx'}$ — элемент BB^T в строке x и столбце x'. — *Прим. перев.*

[3] Граф $G = (V, E)$ разлагается на графы $G_i = (V_i, E_i)$, $i = 1, \ldots, m$, если $E = \bigcup_{i=1}^{m} E_i$ и $E_i \cap E_j = \varnothing$, $1 \leq i < j \leq m$. — *Прим. перев.*



Граф G с семью вершинами и одиннадцатью ребрами. Он имеет одну петлю, одно двойное ребро и одно тройное ребро.

Теорема 4. *Если K_n разложен на полные двудольные подграфы $H_1, \ldots, H_m$, то $m \geq n-1$.*

Интересно, что в отличие от теоремы Эрдёша – де Брёйна комбинаторное доказательство этого утверждения неизвестно! Во всех доказательствах так или иначе используется линейная алгебра. Из различных доказательств, основанных на более или менее эквивалентных идеях, рассмотрим (возможно, наиболее прозрачное) доказательство Тверберга [6].

■ **Доказательство.** Обозначим множество вершин K_n через $\{1, \ldots, n\}$, а через L_j, R_j обозначим подмножества вершин (доли) полного двудольного графа H_j, $j = 1, \ldots, m$. Поставим в соответствие вершине i переменную x_i (а ребру, соединяющему вершины i и j, поставим в соответствие одночлен $x_i x_j$). Так как $H_1, \ldots, H_m$ представляют собой части разложения K_n, то

$$\sum_{i<j} x_i x_j \;=\; \sum_{k=1}^{m} \left(\sum_{a \in L_k} x_a \cdot \sum_{b \in R_k} x_b \right). \tag{1}$$

Предположим теперь, что теорема неверна и $m < n-1$. Тогда в однородной системе линейных уравнений

$$\begin{aligned} x_1 + \ldots + x_n &= 0, \\ \sum_{a \in L_k} x_a &= 0 \qquad (k = 1, \ldots, m) \end{aligned}$$

число уравнений меньше числа неизвестных. Следовательно, она имеет нетривиальное решение $(c_1, \ldots, c_n)$. Из (1) мы находим, что

$$\sum_{i<j} c_i c_j \;=\; 0.$$

Но отсюда вытекает, что

$$0 \;=\; (c_1 + \ldots + c_n)^2 \;=\; \sum_{i=1}^{n} c_i^2 + 2 \sum_{i<j} c_i c_j \;=\; \sum_{i=1}^{n} c_i^2 \;>\; 0.$$

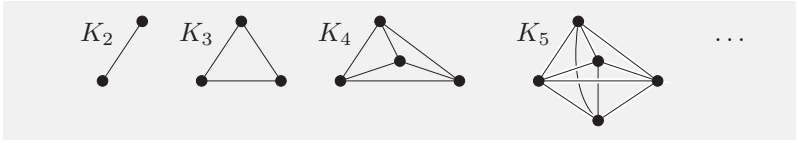
Полученное противоречие завершает доказательство. □

Приложение: основные понятия теории графов

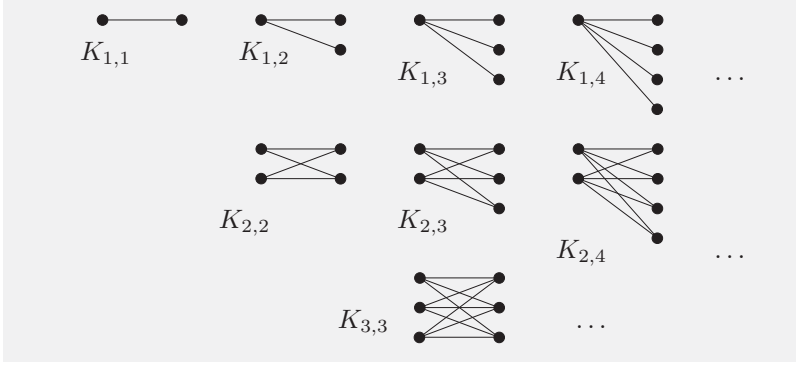
Графы — одна из наиболее фундаментальных математических структур. Поэтому они имеют много модификаций, представлений и реализаций. Формально *граф* можно определить как пару $G = (V, E)$, где V — множество *вершин*, E — множество *ребер*, и каждое ребро «соединяет» две вершины $v, w \in V$. В этой книге рассматриваются только конечные графы, в которых множества V и E конечны.

Обычно мы имеем дело с *простыми графами*: в таких графах не должны существовать *петли* (т.е. ребра, у которых оба конца совпадают), и *кратные ребра* (т.е. ребра, соединяющие одни и те же две вершины). Вершины графа называются *смежными* или *соседними*, если они являются концами некоторого ребра. Вершина и ребро называются *инцидентными*, если вершина является одним из концов ребра.

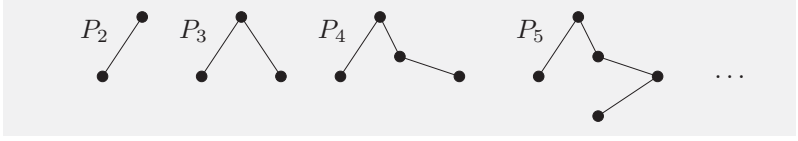
Приведем небольшую коллекцию важных (простых) графов:



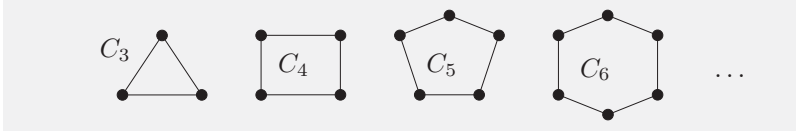
Полные графы K_n с n вершинами и $\binom{n}{2}$ ребрами



Полные двудольные графы $K_{m,n}$ с $m+n$ вершинами и mn ребрами

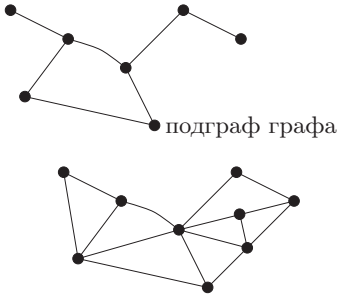


Пути P_n с n вершинами



Циклы C_n с n вершинами

Два графа $G = (V, E)$ и $G' = (V', E')$ называются *изоморфными*, если существуют биекции $V \to V'$ и $E \to E'$, сохраняющие инцидентности между ребрами и вершинами. (Важная нерешенная проблема: существует ли эффективный способ, позволяющий определять, являются ли два данных графа изоморфными?) Понятие изоморфизма позволяет говорить, например, о полном графе K_5 с пятью вершинами (независимо от его конкретной реализации).



Граф $G' = (V', E')$ есть *подграф* графа $G = (V, E)$, если $V' \subseteq V, E' \subseteq E$ и каждое ребро $e \in E'$ имеет те же самые концевые вершины в G', что и в G. Граф G' есть *индуцированный подграф*, если, кроме того, *все* ребра G, которые соединяют вершины G', являются также ребрами графа G'.

Многие понятия, связанные с графами, интуитивно очевидны. Например, граф G называется *связным*, если любые две его различные вершины соединены путем, или, что то же, если $G = (V, E)$ нельзя разбить на два непустых подграфа с не пересекающимися множествами вершин. Любой граф распадается на *связные компоненты*.

Мы завершим этот обзор основных теоретико-графовых понятий еще несколькими терминами. *Клика* в G есть его полный подграф. *Независимое множество* в G — это индуцированный подграф без ребер, т. е. такое подмножество множества вершин, что никакие две из этих вершин не соединены ребром графа G. Граф называется *лесом*, если он не имеет циклов. *Дерево* — связный лес. Наконец, граф $G = (V, E)$ называется

двудольным, если он изоморфен подграфу полного двудольного графа, т. е. если множество его вершин можно записать в виде объединения $V = V_1 \cup V_2$ двух независимых множеств.

Литература

[1] de Bruijn N. G., Erdős P. *On a combinatorial problem.* Proc. Kon. Ned. Akad. Wetensch, **51** (1948), 1277–1279.

[2] Coxeter H. S. M. *A problem of collinear points.* Amer. Math. Monthly, **55** (1948), 26–28 (содержит доказательство Келли).

[3] Erdős P. *Problem 4065 — Three point collinearity.* Amer. Math. Monthly, **51** (1944), 169–171 (содержит доказательство Галлаи).

[4] Graham R. L., Pollak H. O. *On the addressing problem for loop switching.* Bell Syst. Tech. J., **50** (1971), 2495–2519.

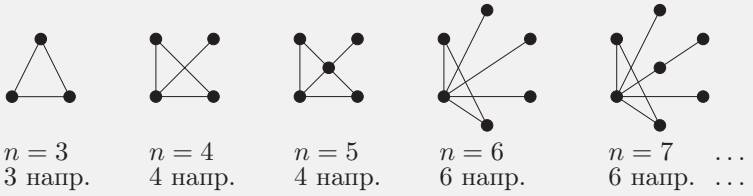
[5] Sylvester J. J. *Mathematical Question 11851.* The Educational Times, **46** (1893), 156.

[6] Tverberg H. *On the decomposition of K_n into complete bipartite graphs.* J. Graph Theory, **6** (1982), 493–494.

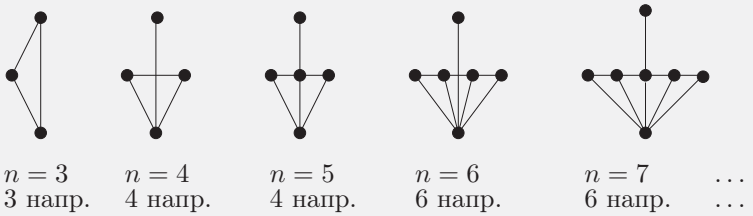
Задача о направлениях

Глава 11

Попробуйте — прежде чем читать дальше — построить конфигурацию точек на плоскости, которая определяет «относительно мало» направлений[1]. При этом, конечно, предполагается, что не все $n \geq 3$ точек лежат на одной прямой. Напомним теорему Эрдёша и де Брёйна из гл. 10 «Прямые на плоскости»: n точек определяют не менее n различных прямых. Однако многие из этих прямых могут быть параллельными и, следовательно, определять одно и то же направление.



или



Эксперименты с малыми n, вероятно, приведут Вас к последовательностям, аналогичным изображенным здесь.

После нескольких попыток отыскать конфигурации с меньшим числом направлений Вы можете предположить (как Скотт в 1970 году), что имеет место следующая теорема.

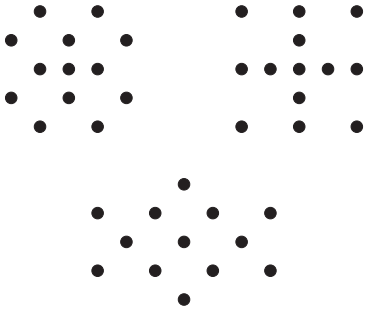
Теорема. *Если $n \geq 3$ точек на плоскости не лежат на одной прямой, то они определяют не менее $n - 1$ различных направлений, причем равенство возможно только если n нечетно и $n \geq 5$.*

Приведенные выше примеры (рисунки соответствуют нескольким первым конфигурациям в двух бесконечных последовательностях примеров) показывают, что утверждение теоремы нельзя улучшить: для

[1] Число направлений, определяемых конфигурацией точек, — это максимальное число попарно не параллельных прямых, каждая из которых содержит хотя бы две точки конфигурации. — *Прим. перев.*

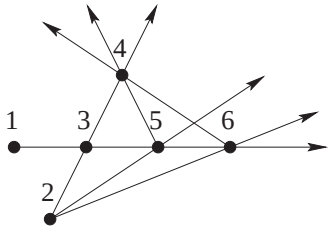
любого нечетного $n \geq 5$ существует конфигурация, определяющая ровно $n-1$ различных направлений, а для любого другого $n \geq 3$ существует конфигурация с n направлениями.

Однако эти примеры не исчерпывают всех возможностей. Например, Джемисон и Хилл описали четыре бесконечных семейства конфигураций с нечетным числом n точек, которые определяют лишь $n-1$ направлений («конфигурации, критические по направлениям»). Кроме того, они составили каталог из 102 «спорадических» конфигураций, которые, по-видимому, не входят ни в одно бесконечное семейство. Бóльшая часть этих конфигураций была найдена с помощью длительного компьютерного поиска.



Три изящных спорадических примера из каталога Джемисона – Хилла

Обычный здравый смысл подсказывает, что если экстремальные конфигурации разнообразны и нерегулярны, то точное решение соответствующих экстремальных задач может быть очень трудным. Действительно, можно многое сказать о структуре конфигураций, критических по направлениям (см. [2]), но полная их классификация представляется недостижимой. Тем не менее, сформулированная выше теорема имеет простое доказательство, состоящее из двух главных частей: сведения к эквивалентной комбинаторной схеме, принадлежащего Эли Гудману и Рикки Поллаку, и прекрасного завершающего рассуждения, которое нашел Петер Унгар в 1982 году.

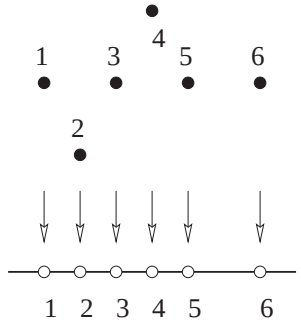


Эта конфигурация из $n = 6$ точек определяет $t = 6$ различных направлений.

■ **Доказательство. (1)** Достаточно показать, что каждое «четное» множество из $n = 2m$ ($m \geq 2$) точек на плоскости определяет не менее n направлений. В самом деле, случай $n = 3$ тривиален, а для произвольного множества из $n = 2m + 1 \geq 5$ точек (не лежащего на одной прямой) можно найти подмножество из $n - 1 = 2m$ точек, которые не лежат на одной прямой и уже определяют $n - 1$ направлений.

Поэтому в дальнейшем мы рассматриваем конфигурацию из $n = 2m$ точек на плоскости, определяющую $t \geq 2$ различных направлений.

(2) Комбинаторная модель получается построением периодической последовательности перестановок. Для этого выберем на плоскости направление, отличающееся от направлений, определенных конфигурацией, и присвоим точкам номера $1, \ldots, n$ в том порядке, в котором они появляются при их одномерной проекции вдоль этого направления. Таким образом, перестановка $\pi_0 = 123...n$ задает порядок точек для начального направления.



Здесь начальное вертикальное направление дает $\pi_0 = 123456$.

Пусть теперь выбранное направление поворачивается против часовой стрелки; проследим за изменениями проекций точек и их перестановок. Изменения порядка проекций точек происходят в те моменты, когда направление проходит через какое-нибудь из направлений конфигурации.

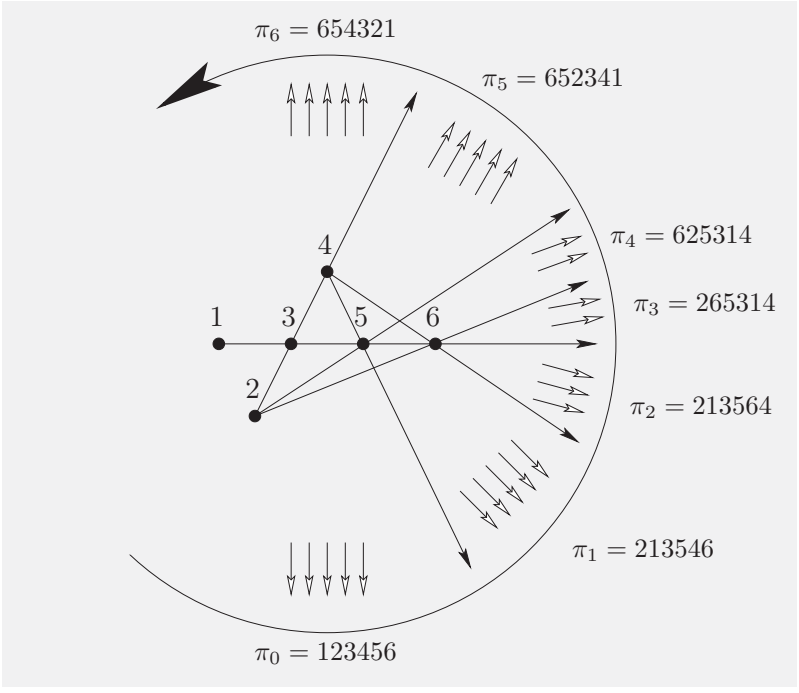
Но эти изменения совсем не случайны и не произвольны; при повороте направления на 180° мы получим последовательность перестановок

$$\pi_0 \to \pi_1 \to \pi_2 \to \ldots \to \pi_{t-1} \to \pi_t,$$

обладающую следующими свойствами:

- Последовательность начинается с $\pi_0 = 123...n$ и заканчивается перестановкой $\pi_t = n...321$.
- Длина t последовательности равна числу направлений, определяемых конфигурацией точек.

- При прохождении по последовательности для каждой пары $i < j$ порядок следования ее элементов изменяется ровно один раз. Это значит, что на пути от $\pi_0 = 123...n$ до $\pi_t = n...321$ изменяется порядок только в *возрастающих* цепочках.
- Каждое изменение состоит в инверсии одной или более не пересекающихся цепочек (соответствующих одной или нескольким прямым, через направление которых в этот момент происходит переход).



Последовательность перестановок для нашего простого примера

Продолжая вращение, мы можем рассматривать нашу последовательность перестановок как часть бесконечной в обе стороны периодической последовательности

$$\ldots \to \pi_{-1} \to \pi_0 \to \ldots \to \pi_t \to \pi_{t+1} \to \ldots \to \pi_{2t} \to \ldots,$$

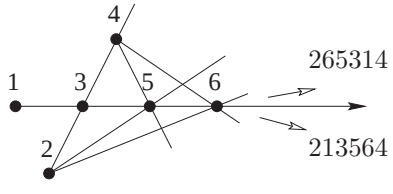
в которой при любом i перестановка π_{i+t} получается из перестановки π_i изменением порядка элементов на противоположный; значит, $\pi_{i+2t} = \pi_i$ для всех $i \in \mathbb{Z}$.

Мы покажем, что для *каждой* последовательности с указанными свойствами (при $t \geq 2$) должно выполняться неравенство $t \geq n$.

(3) Ключ к доказательству состоит в том, чтобы разделить каждую перестановку на «левую» и «правую» половины равного объема $m = \frac{n}{2}$ и подсчитать количество символов, которые пересекают воображаемую *границу* между левой и правой половинами.

Назовем переход $\pi_i \to \pi_{i+1}$ *пересекающим*, если хотя бы одна из пар, порядок элементов которых изменяется, содержит символы по обе стороны границы. Пересекающий переход имеет *порядок* d, если он перемещает через границу $2d$ символов, т. е. если при этом переходе ровно d символов перемещаются через границу в одну сторону и ровно d символов — в другую. Так, в нашем примере переход

$$\pi_2 \;=\; 2\underline{13:56}4 \longrightarrow 2\overline{65:31}4 \;=\; \pi_3$$



Пересекающий переход

является пересекающим и имеет порядок $d = 2$ (он перемещает символы $1, 3, 5, 6$ через границу, обозначенную знаком «:»), переход

$$65\underline{2:34}1 \longrightarrow 65\overline{4:32}1$$

является пересекающим порядка $d = 1$, а, например, переход

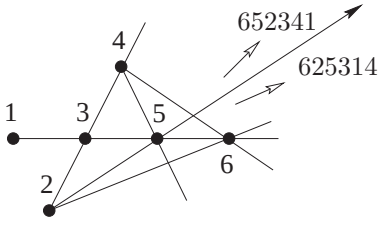
$$6\underline{25}:3\underline{14} \longrightarrow 6\overline{52}:3\overline{41}$$

не является пересекающим.

В последовательности $\pi_0 \to \pi_1 \to \ldots \to \pi_t$ каждый из символов $1, 2, \ldots, n$ должен пересечь границу хотя бы раз. Отсюда следует, что если $d_1, \ldots, d_c$ обозначают порядки c пересекающих переходов, то

$$\sum_{i=1}^{c} 2d_i \;=\; \#\{\text{символы, пересекающие границу}\} \;\geq\; n.$$

Отсюда следует также, что существует не менее двух пересекающих переходов, так как пересекающий переход с $2d_i = n$ возможен только тогда, когда все точки находятся на одной прямой, т. е. в случае $t = 1$. Геометрически пересекающие переходы соответствуют направлениям прямых, которые соединяют точки конфигурации и по каждую сторону от которых лежит меньше m точек.

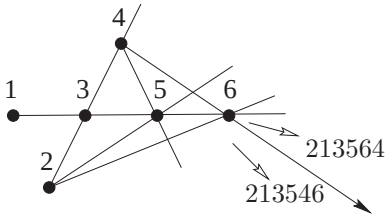


Касательный переход

(4) Назовем переход *касательным*, если он перемещает символы цепочки, примыкающей к границе, но не пересекающей ее. Например, переход

$$\pi_4 \;=\; 6\underline{25}:3\underline{14} \longrightarrow 6\overline{52}:3\overline{41} \;=\; \pi_5$$

— касательный. Геометрически касательный переход соответствует направлению прямой, соединяющей точки конфигурации, имеющей ровно m точек с одной стороны и, следовательно, не больше $m - 2$ точек с другой.



Обыкновенный переход

Переходы, не являющиеся ни пересекающими, ни касательными, будем называть *обыкновенными*. Примером такого перехода является

$$\pi_1 \;=\; 213{:}5\underline{46} \longrightarrow 213{:}5\overline{64} \;=\; \pi_2.$$

Таким образом, каждый переход является либо касательным, либо пересекающим, либо обыкновенным, и для обозначения этих типов мы будем использовать буквы T, C, O.[2] Запись $C(d)$ будет обозначать пересекающий переход порядка d. В частности, в нашем простом примере мы получаем

$$\pi_0 \xrightarrow{T} \pi_1 \xrightarrow{O} \pi_2 \xrightarrow{C(2)} \pi_3 \xrightarrow{O} \pi_4 \xrightarrow{T} \pi_5 \xrightarrow{C(1)} \pi_6,$$

и эту последовательность можно записать еще короче: $T, O, C(2), O, T, C(1)$.

(5) Для завершения доказательства нам потребуются следующие два утверждения:

[2] T, C, O — первые буквы слов *touching* (касательный), *crossing* (пересекающий) и *ordinary* (обыкновенный). — *Прим. перев.*

Между любыми двумя пересекающими переходами имеется хотя бы один касательный.

Между любым пересекающим переходом порядка d и следующим касательным переходом имеется не менее $d-1$ обыкновенных переходов.

Действительно, после пересекающего перехода порядка d граница находится в центре симметричной убывающей цепочки длины $2d$, имеющей по d символов с каждой стороны границы. Перед следующим пересекающим переходом центральная граница должна находиться в возрастающей цепочке длины не меньше 2. Но этого можно добиться только касательными переходами. Отсюда следует первое утверждение.

Чтобы доказать второе утверждение, заметим, что при каждом обыкновенном переходе (обращающем некоторую *возрастающую* цепочку) убывающая $2d$-цепочка может укоротиться не более чем на один символ с каждой стороны. И до тех пор, пока убывающая цепочка имеет не меньше четырех символов, касательный переход невозможен. Это доказывает второе утверждение.

Если построить последовательность перестановок, начав с той же самой исходной проекции, но используя вращение по часовой стрелке, то получится та же последовательность перестановок в обратном порядке. Следовательно, размеченная нами последовательность должна также удовлетворять обращению второго утверждения, а именно:

Между касательным переходом и следующим пересекающим переходом порядка d имеется не менее $d-1$ обыкновенных переходов.

(6) Для построенной в **(2)** бесконечной последовательности ее T-O-C-образ получается повторением T-O-C-образа длины t последовательности $\pi_0 \longrightarrow \ldots \longrightarrow \pi_t$. Учитывая утверждения из **(5)**, находим, что в бесконечной последовательности переходов каждый пересекающий переход порядка d вложен в T-O-C-образ типа

$$T, \underbrace{O, O, \ldots, O,}_{\geq\, d-1} C(d), \underbrace{O, O, \ldots, O,}_{\geq\, d-1} \qquad (*)$$

длины не менее $1 + (d-1) + 1 + (d-1) = 2d$.

В бесконечной последовательности можно рассмотреть конечный участок длины t, начинающийся с касательного перехода. Этот участок состоит из цепочек типа $(*)$, между которыми, возможно, есть дополнительные символы T. Следовательно, его длина t удовлетворяет неравенству

$$t \;\geq\; \sum_{i=1}^{c} 2d_i \;\geq\; n,$$

что завершает доказательство. $\square$

Литература

[1] Goodman J. E., Pollack R. *A combinatorial perspective on some problems in geometry.* Congressus Numerantium, **32** (1981), 383–394.

[2] Jamison R. E., Hill D. *A catalogue of slope-critical configurations.* Congressus Numerantium, **40** (1983), 101–125.

[3] Scott P. R. *On the sets of directions determined by n points.* Amer. Math. Monthly, **77** (1970), 502–505.

[4] Ungar P. $2N$ *noncollinear points determine at least* $2N$ *directions.* J. Combinatorial Theory, Ser. A, **33** (1982), 343–347.

Три применения формулы Эйлера

Глава 12

Граф называется *планарным*, если его можно начертить на плоскости $\mathbb{R}^2$ (или, что то же самое, на двумерной сфере S^2) без пересечений ребер. Мы говорим о *плоском* графе, если такой чертеж задан и фиксирован. Любой плоский граф разбивает плоскость или сферу на конечное число связных областей, включая внешнюю (неограниченную) область; эти области называют *гранями*.

Формула Эйлера указывает связь между числами вершин, ребер и граней, справедливую для любого плоского графа. Эйлер упомянул этот результат в письме своему другу Гольдбаху в 1750 году, но тогда у него не было полного доказательства. Из многих доказательств формулы Эйлера мы выбрали приятное и «самодвойственное» доказательство, в котором не используется индукция. Оно восходит к книге фон Штаудта «Geometrie der Lage», изданной в 1847 году [4].

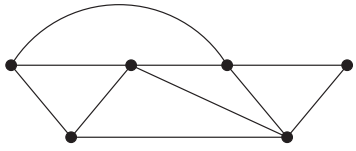
Формула Эйлера. *Если G — связный плоский граф с n вершинами, e ребрами и f гранями, то*

$$n - e + f \;=\; 2.$$

Леонард Эйлер

■ **Доказательство.** Пусть E — множество всех ребер графа G и $T \subseteq E$ — множество ребер остовного дерева графа G, т. е. множество ребер минимального подграфа, связывающего все вершины графа G. Ввиду условия минимальности этот граф не содержит циклов.

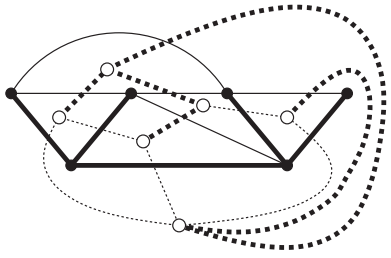
Нам потребуется теперь *двойственный* (или дуальный) *граф* G^* графа G. Граф G^* имеет по одной вершине во внутренности каждой грани графа G; вершины графа G^* соединены тогда и только тогда, когда содержащие их грани графа G имеют общие граничные ребра.



Плоский граф G:
$n = 6$, $e = 10$, $f = 6$

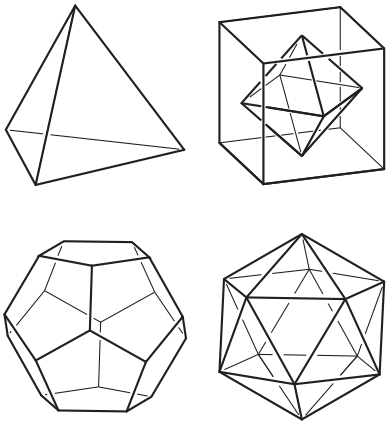
Если две грани графа G имеют несколько общих граничных ребер, то в двойственном графе мы проводим столько же ребер, связывающих соответствующую пару вершин[1]. (Следовательно, G^* может иметь кратные ребра даже тогда, когда исходный граф G простой.)

Пусть E^* — множество ребер графа G^*. Рассмотрим совокупность $T^* \subseteq E^*$ ребер в двойственном графе, которые соответствуют ребрам из $E \backslash T$. Ребра из T^* связывают все грани, так как T не имеет циклов; но T^* также не содержит циклов, так как иначе T^* отделял бы некоторые вершины графа G внутри цикла от вершин вне его (а этого не может быть, поскольку T — остовный подграф и ребра графов T и T^* не пересекаются). Следовательно, T^* — остовное дерево для G^*.



Двойственные остовные деревья в G и G^*

[1] Граф G^* называют также *геометрически двойственным*. Описание построения двойственного графа G^* не совсем точно (ср. с изложением в [6*]): не учитывается возможность появления в G^* петель, порождаемых, например, концевыми вершинами в G. Но на справедливость формулы Эйлера это не влияет, и при доказательстве можно предполагать, что G не имеет концевых вершин. — *Прим. перев.*



Пять платоновых тел

Число вершин каждого дерева на единицу больше числа его ребер. Чтобы убедиться в этом, выберем одну вершину в качестве корня и зададим на всех ребрах направление от корня. Сопоставляя каждому ребру вершину, в которую оно входит, мы получим биекцию между некорневыми вершинами и ребрами.

Для дерева T это дает $n = e_T + 1$, в то время как для дерева T^* имеем $f = e_{T^*} + 1$ (здесь e_T и e_{T^*} — числа ребер в T и T^*). Складывая два равенства, находим $n + f = (e_T + 1) + (e_{T^*} + 1) = e + 2$, так как, очевидно, $e_T + e_{T^*} = e$. □

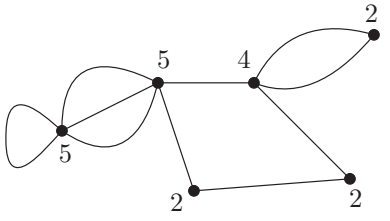
Таким образом, формула Эйлера дает содержательное *количественное* следствие из *геометрико-топологической ситуации*: число вершин, ребер и граней конечного графа G удовлетворяет равенству $n-e+f = 2$ всякий раз, когда граф начерчен или *может быть* начерчен на плоскости или на сфере без пересечений ребер.

Из формулы Эйлера можно вывести ряд известных и важных утверждений. В их числе классификация правильных выпуклых многогранников (платоновых тел), предложение о том, что K_5 и $K_{3,3}$ не планарны (см. ниже), и теорема о пяти красках, согласно которой каждую планарную карту можно раскрасить не более чем пятью цветами так, что любые две соседние области будут окрашены в разные цвета. Но для последней теоремы известно значительно лучшее доказательство, не использующее формулу Эйлера (см. гл. 34).

В настоящей главе приведены три другие прекрасные доказательства, основанные на формуле Эйлера. Первые два — доказательства теоремы Сильвестра – Галлаи и теоремы о конфигурациях точек, раскрашенных в два цвета, — используют формулу Эйлера в остроумном сочетании с другими арифметическими соотношениями для базисных параметров графа. Рассмотрим вначале эти параметры.

Степень вершины есть число выходящих из нее ребер, причем петли считают дважды. Пусть n_i обозначает число вершин степени i в графе G. Считая вершины в соответствии с их степенями, мы получаем

$$n \;=\; n_0 + n_1 + n_2 + n_3 + \dots \tag{1}$$



Здесь рядом с каждой вершиной записана ее степень. Подсчет чисел вершин данной степени дает: $n_2 = 3$, $n_3 = 0$, $n_4 = 1$, $n_5 = 2$.

С другой стороны, каждое ребро имеет два конца, так что оно вносит в сумму всех степеней вершин вклад 2, и мы находим

$$2e \;=\; n_1 + 2n_2 + 3n_3 + 4n_4 + \dots \tag{2}$$

Это тождество можно интерпретировать как перечисление двумя способами концов ребер, т. е. инциденций «ребро-вершина».

Средняя степень $\overline{d}$ вершин, следовательно, равна

$$\overline{d} \;=\; \frac{2e}{n}.$$

Далее, перечислим грани плоского графа в соответствии с числом их сторон: *k-грань* — это грань, ограниченная k ребрами (ребро, по обе стороны от которого лежит одна и та же область, должно быть подсчитано дважды!). Пусть f_k есть число k-граней. Перечисляя грани каждого вида, находим

$$f \;=\; f_1 + f_2 + f_3 + f_4 + \ldots \tag{3}$$

Подсчитывая ребра в соответствии с гранями, для которых они являются сторонами, получаем

$$2e \;=\; f_1 + 2f_2 + 3f_3 + 4f_4 + \ldots \tag{4}$$

Это равенство тоже можно интерпретировать как нахождение числа инциденций ребро-грань двумя способами. Заметим, что среднее число сторон граней задается выражением

$$\overline{f} \;=\; \frac{2e}{f}.$$

Отсюда и из формулы Эйлера легко вывести, что полный граф K_5 и полный двудольный граф $K_{3,3}$ не являются планарными. Для предполагаемого плоского изображения графа K_5 имеем $n = 5$, $e = \binom{5}{2} = 10$, так что $f = e + 2 - n = 7$ и $\overline{f} = \frac{2e}{f} = \frac{20}{7} < 3$. Но если среднее число сторон граней меньше трех, то укладка графа на плоскость должна иметь грань с не более чем двумя сторонами, что для графа K_5 невозможно.

Подобным образом для $K_{3,3}$ получаем $n = 6$, $e = 9$, $f = e+2-n = 5$, следовательно, $\overline{f} = \frac{2e}{f} = \frac{18}{5} < 4$, но этого невозможно, так как $K_{3,3}$ — простой двудольный граф, в силу чего длины циклов не меньше 4.

Аналогия между равенствами (3) и (4) для чисел f_i и равенствами (1) и (2) для величин n_i не случайна. Они преобразуются одно в другое при переходе от G к описанному выше двойственному графу G^*. Из этих равенств вытекают «локальные» следствия формулы Эйлера.

Предложение. *Пусть G — произвольный непустой простой плоский граф с $n > 2$ вершинами. Тогда*

(A) *число ребер графа G не превосходит $3n - 6$;*

(B) *G имеет вершину степени не более 5;*

(C) *если каждое ребро графа G окрашено одним из двух цветов, то в G существует вершина, при обходе вокруг которой цвета инцидентных ей ребер изменяются не более двух раз.*

■ **Доказательство.** При доказательстве каждого из трех утверждений можно предполагать, что G является связным.

(A) Каждая грань имеет не менее трех сторон (так как граф G простой), так что (3) и (4) принимают вид:

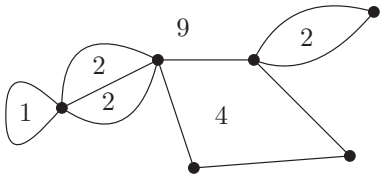
$$\begin{aligned} f &= f_3 + f_4 + f_5 + \ldots \\ 2e &= 3f_3 + 4f_4 + 5f_5 + \ldots \end{aligned}$$

и, следовательно, $2e - 3f \geq 0$. Теперь согласно формуле Эйлера

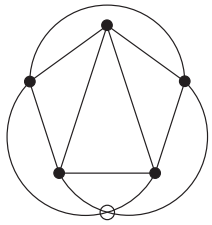
$$3n - 6 = 3e - 3f \geqslant e.$$

(B) Согласно части (A) средняя степень вершин $\overline{d}$ удовлетворяет соотношению

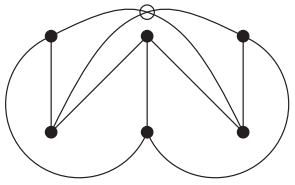
$$\overline{d} = \frac{2e}{n} \leqslant \frac{6n - 12}{n} < 6.$$



В каждой области записано число ее сторон. Перечисление граней с данным числом сторон дает: $f_1 = 1$, $f_2 = 3$, $f_4 = 1$, $f_9 = 1$ и $f_i = 0$ в остальных случаях.



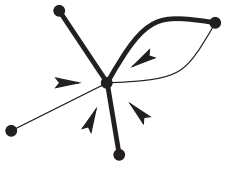
K_5 изображен с одним пересечением.



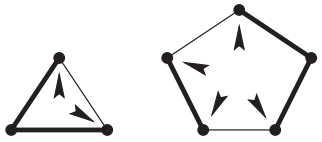
$K_{3,3}$ изображен с одним пересечением.

Поэтому должна существовать вершина с кратностью не больше 5.

(C) Пусть c — число углов между соседними ребрами с общей вершиной, в которых изменяется цвет ребер. Предположим, что утверждение (C) не верно.



Стрелки указывают углы с изменением цвета ребер.



Тогда $c \geq 4n$, так как около каждой вершины цвет меняется четное число раз. Далее, каждая грань с $2k$ или $2k+1$ сторонами может иметь не более $2k$ таких углов, и, снова используя (3) и (4), находим

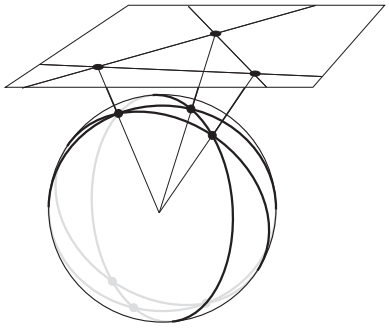
$$\begin{aligned} 4n \;\leq\; c \;&\leq\; 2f_3 + 4f_4 + 4f_5 + 6f_6 + 6f_7 + 8f_8 + \dots \\ &\leq\; 2f_3 + 4f_4 + 6f_5 + 8f_6 + 10f_7 + \dots \\ &=\; 2(3f_3 + 4f_4 + 5f_5 + 6f_6 + 7f_7 + \dots) \\ &\quad\; -4(f_3 + f_4 + f_5 + f_6 + f_7 + \dots) \\ &=\; 4e - 4f. \end{aligned}$$

Тогда $e \geq n + f$, что снова противоречит формуле Эйлера. □

1. Теорема Сильвестра – Галлаи, новое доказательство

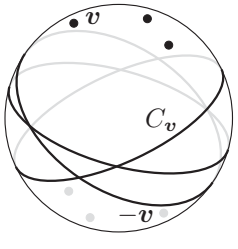
Кажется, Норман Стинрод первым заметил [5], что часть (A) предыдущего Предложения дает поразительно простое доказательство теоремы Сильвестра – Галлаи (см. гл. 10).

Теорема Сильвестра – Галлаи. *Для любого множества из $n \geq 3$ точек на плоскости, не лежащих на одной прямой, найдется прямая, содержащая ровно две точки.*



■ **Доказательство.** (Сильвестр – Галлаи; используется формула Эйлера.) Пусть S^2 — единичная сфера в $\mathbb{R}^3$. Вложим плоскость $\mathbb{R}^2$ в $\mathbb{R}^3$ так, как показано на рисунке на полях. Тогда прямые, проходящие через центр сферы, будут сопоставлять каждой точке на $\mathbb{R}^2$ пару точек-антиподов на S^2, а каждой прямой в $\mathbb{R}^2$ — большую окружность[2] на S^2. Следовательно, теорема Сильвестра–Галлаи равносильна следующему утверждению.

Для любого множества $n \geq 3$ пар точек-антиподов на сфере, не лежащих на одной большой окружности, найдется большая окружность, содержащая ровно две пары точек-антиподов.



Теперь, переходя к двойственному утверждению, заменим каждую пару $\pm\boldsymbol{v} \in S^2$ точек-антиподов большой окружностью на сфере $C_{\boldsymbol{v}} := \{\boldsymbol{x} \in S^2 : \langle \boldsymbol{x}, \boldsymbol{v} \rangle = 0\}$. ($C_{\boldsymbol{v}}$ является экватором, если рассматривать $\boldsymbol{v}$ как северный полюс сферы.)

Поэтому теорему Сильвестра–Галлаи можно переформулировать так:

Для любой совокупности из $n \geq 3$ больших окружностей на S^2, не проходящих через одну и ту же точку[3], найдется точка, принадлежащая ровно двум большим окружностям.

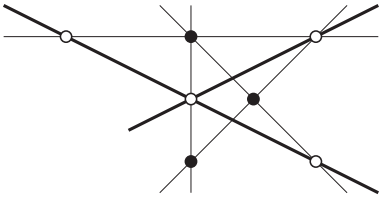
[2] *Большой окружностью* на S^2 называется линия пересечения сферы и плоскости, проходящей через ее центр. — *Прим. перев.*

[3] Если точки $\boldsymbol{v}_1$, $\boldsymbol{v}_2$, ... принадлежат экватору сферы S^2, то соответствующие им окружности $C_{\boldsymbol{v}_1}, C_{\boldsymbol{v}_2}, \dots$, пересекаются в северном и южном полюсах. — *Прим. перев.*

Но конфигурация больших окружностей определяет простой плоский граф на S^2, вершинами которого являются точки пересечения больших окружностей, делящие большие окружности на ребра. Степени всех вершин четны, и по построению наименьшая степень не меньше четырех. Поэтому из части (B) Предложения на с.85 следует существование вершины степени 4. Это всё! □

2. Монохроматические прямые

Следующая «раскрасочная» родственница теоремы Сильвестра – Галлаи принадлежит Дону Чакеряну [1].



Теорема. *Для любой конечной конфигурации «черных» и «белых» точек на плоскости, не лежащих на одной прямой, найдется «монохроматическая» (одноцветная) прямая, содержащая не менее двух точек одного цвета и не содержащая точек другого цвета.*

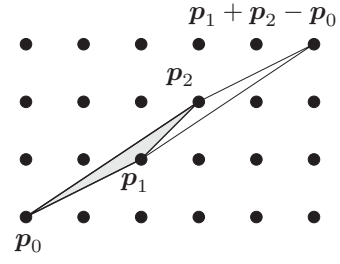
■ **Доказательство.** Как и при доказательстве теоремы Сильвестра – Галлаи, перенесем конфигурацию на единичную сферу и перейдем к двойственному утверждению. Значит, достаточно доказать следующее:

> *Для любой конечной совокупности «черных» и «белых» больших окружностей на сфере, не пересекающихся в одной точке, найдется точка пересечения, принадлежащая либо лишь белым, либо лишь черным большим окружностям.*

В такой форме утверждение непосредственно следует из части (C) Предложения, так как в каждой точке пересечения больших окружностей разных цветов имеется не менее четырех углов с разноцветными сторонами. □

3. Теорема Пика

Теорема Пика, доказанная в 1899 году [3], красива и удивительна; кроме того, она является «классическим» следствием формулы Эйлера[4]. Далее будем называть выпуклый многоугольник $P \subset \mathbb{R}^2$, все вершины которого находятся в узлах целочисленной решетки $\mathbb{Z}^2$, *элементарным*, если он не содержит внутри себя или на границе других точек решетки.

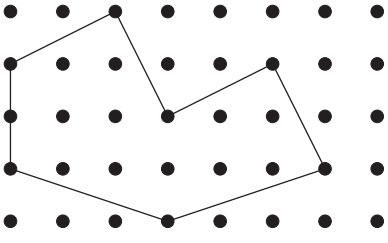


Лемма. *Каждый элементарный треугольник Δ с вершинами $\boldsymbol{p}_0, \boldsymbol{p}_1, \boldsymbol{p}_2 \in \mathbb{Z}^2$ имеет площадь $A(\Delta) = \frac{1}{2}$.*

■ **Доказательство.** Как параллелограмм P с вершинами $\boldsymbol{p}_0, \boldsymbol{p}_1, \boldsymbol{p}_2, \boldsymbol{p}_1 + \boldsymbol{p}_2 - \boldsymbol{p}_0$, так и решетка $\mathbb{Z}^2$ инвариантны относительно отображения

$$\sigma : \ \boldsymbol{x} \ \longmapsto \ \boldsymbol{p}_1 + \boldsymbol{p}_2 - \boldsymbol{x}$$

(симметрии относительно центра отрезка, соединяющего $\boldsymbol{p}_1$ и $\boldsymbol{p}_2$). Следовательно, параллелограмм $P = \Delta \cup \sigma(\Delta)$ также является элементарным, и его параллельные переносы на векторы с целочисленными координатами покрывают (подобно черепице) всю плоскость без пересечений. Поэтому $\{\boldsymbol{p}_1 - \boldsymbol{p}_0, \boldsymbol{p}_2 - \boldsymbol{p}_0\}$ есть базис решетки $\mathbb{Z}^2$, его определитель



$n_{int} = 11$, $n_{bd} = 8$, так что $A = 14$

[4] Доказательство теоремы Пика без явного использования формулы Эйлера содержится в [7*], задача 110. — *Прим. перев.*

Базисы решетки

Базис $\mathbb{Z}^2$ — любая такая пара линейно не зависимых векторов $\boldsymbol{e}_1, \boldsymbol{e}_2$, что

$$\mathbb{Z}^2 \;=\; \{\lambda_1 \boldsymbol{e}_1 + \lambda_2 \boldsymbol{e}_2 : \lambda_1, \lambda_2 \in \mathbb{Z}\}.$$

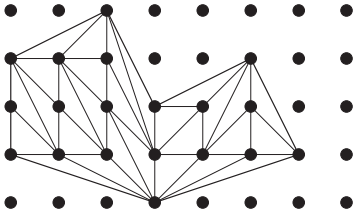
Пусть $\boldsymbol{e}_1 = \binom{a}{b}$ и $\boldsymbol{e}_2 = \binom{c}{d}$, тогда площадь параллелограмма, натянутого на $\boldsymbol{e}_1$ и $\boldsymbol{e}_2$, равна $A(\boldsymbol{e}_1, \boldsymbol{e}_2) = |\det(\boldsymbol{e}_1, \boldsymbol{e}_2)| = |\det \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)|$.
Если $\boldsymbol{f}_1 = \binom{r}{s}$, и $\boldsymbol{f}_2 = \binom{t}{u}$ — другой базис решетки, то существует обратимая целочисленная матрица Q, для которой $\left(\begin{smallmatrix} r & t \\ s & u \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) Q$. Так как $QQ^{-1} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ и определители — целые числа, то $|\det Q| = 1$, в силу чего $|\det(\boldsymbol{f}_1, \boldsymbol{f}_2)| = |\det(\boldsymbol{e}_1, \boldsymbol{e}_2)|$. Следовательно, все базисные параллелограммы имеют одну и ту же площадь, равную 1, поскольку $A\left(\binom{1}{0}, \binom{0}{1}\right) = 1$.

равен ± 1, параллелограмм P имеет площадь, равную 1, и Δ имеет площадь $\frac{1}{2}$. (Объяснение использованных терминов см. во вставке.) □

Теорема. *Площадь любого (не обязательно выпуклого) многоугольника $Q \subset \mathbb{R}^2$ с вершинами в $\mathbb{Z}^2$ определяется формулой*

$$A(Q) \;=\; n_{\text{int}} + \frac{1}{2} n_{\text{bd}} - 1,$$

где n_{int} и n_{bd} — числа точек решетки $\mathbb{Z}^2$ внутри и на границе многоугольника Q соответственно.



■ **Доказательство.** Каждый многоугольник с вершинами в $\mathbb{Z}^2$ можно триангулировать, используя все n_{int} точек решетки внутри и все n_{bd} точек решетки на границе многоугольника Q. (Это не вполне очевидно, если не требовать выпуклости многоугольника Q, но рассуждение, приведенное в гл. 35 в связи с задачей о художественной галерее, доказывает возможность триангуляции.)

Теперь рассмотрим триангуляцию как плоский граф, который разбивает плоскость на одну неограниченную область и $f-1$ треугольников площадью $\frac{1}{2}$ каждый, так что

$$A(Q) \;=\; \frac{1}{2}(f-1).$$

Всякий треугольник имеет три стороны, причем каждое из e_{int} внутренних ребер служит границей двух треугольников, а каждое из e_{bd} граничных для Q ребер появляется лишь в одном-единственном треугольнике. Поэтому $3(f-1) = 2e_{\text{int}} + e_{\text{bd}}$, так что $f = 2(e-f) - e_{\text{bd}} + 3$, где $e = e_{\text{int}} + e_{\text{bd}}$ — общее число ребер триангуляции. Далее, число граничных ребер и число вершин одинаковы: $e_{\text{bd}} \;=\; n_{\text{bd}}$. Эти два факта вместе с формулой Эйлера показывают, что

$$\begin{aligned} f \;&=\; 2(e-f) - e_{\text{bd}} + 3 \\ &=\; 2(n-2) - n_{\text{bd}} + 3 \;=\; 2n_{\text{int}} + n_{\text{bd}} - 1, \end{aligned}$$

и, следовательно,

$$A(Q) \;=\; \tfrac{1}{2}\,(f-1) \;=\; n_{\mathrm{int}} + \tfrac{1}{2}\,n_{\mathrm{bd}} - 1. \qquad \square$$

Литература

[1] Chakerian G. D. *Sylvester's problem on collinear points and a relative.* Amer. Math. Monthly, **77** (1970), 164–167.

[2] Eppstein D. *Nineteen proofs of Euler's formula: $V - E + F = 2$.* Geometry Junkyard, http://www.ics.uci.edu/∼eppstein/junkyard/euler/

[3] Pick G. *Geometrisches zur Zahlenlehre.* Sitzungsberichte Lotos (Prag), Natur-med. Verein für Böhmen, **19** (1899), 311–319.

[4] von Staudt K. G. C. *Geometrie der Lage.* Verlag der Fr. Korn'schen Buchhandlung, Nürnberg, 1847.

[5] Steenrod N. E. *Solution 4065/Editorial Note.* Amer. Math. Monthly, **51** (1944), 170–171.

[6*] Харари Ф. *Теория графов.* М.: Мир, 1973.

[7*] Яглом А. М., Яглом И. М. *Неэлементарные задачи в элементарном изложении.* М.: ГИТТЛ, 1954.

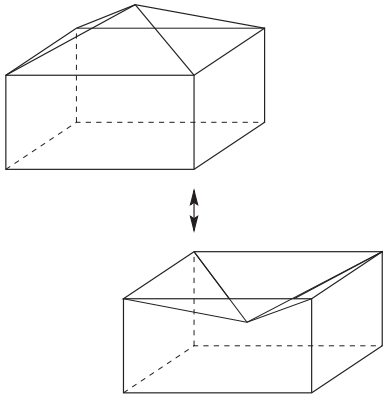
Глава 13 Теорема Коши о жесткости

Огюст Коши

Известный результат, основанный на формуле Эйлера (а именно, на части (C) Предложения из предыдущей главы), — теорема Коши о жесткости для трехмерных многогранников.

Определения используемых ниже понятий конгруэнтности и комбинаторной эквивалентности приведены в приложении о политопах и многогранниках к главе о третьей проблеме Гильберта (см. с. 68).

> **Теорема.** *Если два трехмерных выпуклых многогранника P и P' комбинаторно эквивалентны, а их соответствующие грани конгруэнтны, то углы между соответствующими парами смежных граней равны (и, следовательно, многогранник P конгруэнтен многограннику P').*



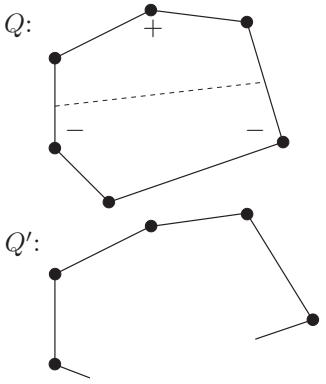
На полях изображены два трехмерных комбинаторно эквивалентных многогранника, у которых соответствующие грани конгруэнтны. Но многогранники не конгруэнтны, и лишь один из них выпуклый. Таким образом, предположение о выпуклости в теореме Коши существенно!

■ **Доказательство.** По существу мы приведем первоначальное доказательство Коши [1]. Пусть даны два выпуклых комбинаторно эквивалентных многогранника P и P' с конгруэнтными гранями. Раскрасим ребра многогранника P: сделаем ребро черным (или «положительным»), если соответствующий ему внутренний угол между двумя смежными гранями в P' больше, чем в P, и белым (или «отрицательным»), если соответствующий угол в P' меньше, чем в P.

Множество черных и белых ребер многогранника P образует 2-окрашенный плоский граф на его поверхности. Этот граф с помощью центральной проекции из внутренней точки многогранника P можно отобразить на поверхность единичной сферы. Если у многогранников P и P' есть неравные соответствующие углы, то этот граф не пуст. Из части (C) Предложения из предыдущей главы следует, что существует вершина p многогранника P, которая является концом хотя бы одного черного или белого ребра и при циклическом обходе вокруг которой происходит не более двух изменений цвета ребер.

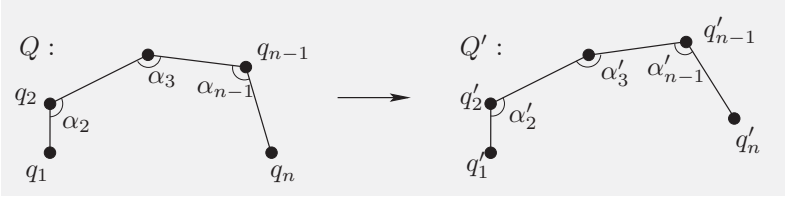
Теперь пересечем многогранник P сферой S_ε малого радиуса ε с центром в вершине p, а многогранник P' пересечем сферой S'_ε такого же радиуса ε с центром в соответствующей вершине p'. При этом на S_ε и S'_ε образуются выпуклые сферические многоугольники Q и Q', у которых соответствующие стороны (дуги) имеют равные длины, поскольку грани P и P' конгруэнтны, а сферы S_ε и S'_ε равны.

Отметим знаком + углы многоугольника Q, для которых соответствующие углы в Q' больше, и знаком − углы, которым в Q' соответствуют меньшие углы. Таким образом, при переходе от Q к Q' положительные углы «раскрываются», отрицательные углы «закрываются», а длины всех дуг и величины не отмеченных углов не изменяются.



Согласно выбору вершины p в Q *существуют* вершины, помеченные знаками + или −, и при циклическом обходе вершин Q происходит не более двух изменений знака. Если бы все пометки имели один тип (+ или −), то это противоречило бы доказанной ниже лемме, согласно которой одно ребро должно изменить свою длину. Если бы существовали пометки обоих типов, то (так как при обходе знак изменяется лишь дважды) существовала бы «граница» (дуга большого круга), соединяющая середины двух сторон многоугольника и отделяющая все знаки + от всех знаков −. Но это противоречит той же лемме, поскольку согласно ей «граница» в Q' должна была бы быть одновременно как короче, так и длиннее, чем в Q. □

Лемма Коши о шарнире. *Пусть Q и Q' — выпуклые (плоские или сферические) n-угольники, помеченные так же, как на чертеже, длины их соответствующих*

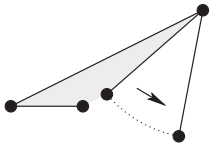


сторон одинаковы ($\overline{q_iq_{i+1}} = \overline{q'_iq'_{i+1}}$, $1 \le i \le n-1$), а углы удовлетворяют условиям $\alpha_i \le \alpha'_i$, $2 \le i \le n-1$. Тогда для длины «отсутствующего» ребра справедливо неравенство

$$\overline{q_1q_n} \;\le\; \overline{q'_1q'_n},$$

и равенство имеет место тогда и только тогда, когда $\alpha_i = \alpha'_i$ для всех i.

Интересно, что доказательство леммы, предложенное Коши, было неверным: как показывает рисунок на полях, непрерывное движение, которое раскрывает углы и сохраняет фиксированными длины сторон, может нарушить выпуклость! С другой стороны, и лемма, и приведенное здесь доказательство (взятое из письма И. Шоенберга С. К. Зарембе) справедливо как для плоских, так и для сферических многоугольников.

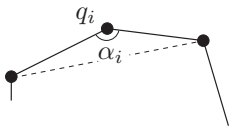


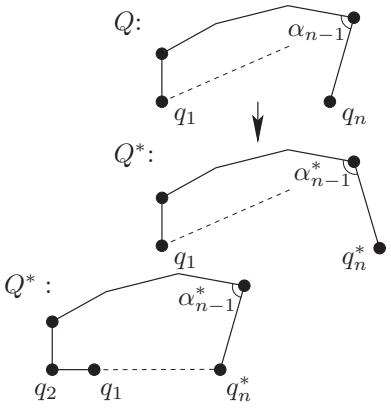
■ **Доказательство.** Воспользуемся индукцией по n. Случай $n = 3$ прост: если в треугольнике увеличить угол γ между двумя сторонами фиксированных длин a и b, то длина противолежащей стороны также возрастет. Аналитически это следует из теоремы косинусов

$$c^2 \;=\; a^2 + b^2 - 2ab\cos\gamma$$

в плоском случае и из аналогичного равенства

$$\cos c \;=\; \cos a\cos b + \sin a\sin b\cos\gamma$$





в сферической тригонометрии. Здесь длины a, b, c измеряются по поверхности сферы единичного радиуса и поэтому принимают значения из промежутка $[0, \pi]$.

Пусть теперь $n \geq 4$ и лемма справедлива для многоугольников с числом вершин, меньшим n. Если для какого-нибудь $i \in \{2, \dots, n-1\}$ справедливо равенство $\alpha_i = \alpha'_i$, то соответствующие вершины можно отсечь диагоналями, связывающими q_{i-1} и q_{i+1} (соответственно, q'_{i-1} и q'_{i+1}), и так как $\overline{q_{i-1}q_{i+1}} = \overline{q'_{i-1}q'_{i+1}}$, то шаг индукции в этом случае обоснован. Поэтому нам осталось рассмотреть случай, когда $\alpha_i < \alpha'_i$ при всех $2 \leq i \leq n-1$.

Построим по Q новый многоугольник Q^*, заменив угол α_{n-1} наибольшим возможным углом $\alpha^*_{n-1} \leq \alpha'_{n-1}$, при котором сохраняется выпуклость Q^*. Для этого заменим в Q вершину q_n вершиной q^*_n, сохраняя фиксированными все другие вершины q_i, длины сторон и величины углов.

Если $Q*$ остается выпуклым даже при $\alpha^*_{n-1} = \alpha'_{n-1}$, то неравенства $\overline{q_1q_n} < \overline{q_1q^*_n} \leq \overline{q'_1q'_n}$ можно доказать, используя для первого перехода случай $n = 3$, а для второго, как и выше, индукцию.

В противном случае после указанного не тождественного преобразования, приводящего к неравенству

$$\overline{q_1q^*_n} \;>\; \overline{q_1q_n}, \tag{1}$$

мы «застреваем» в положении, когда q_2, q_1 и q^*_n коллинеарны и

$$\overline{q_2q_1} + \overline{q_1q^*_n} \;=\; \overline{q_2q^*_n}. \tag{2}$$

Применяя предположение индукции к многоугольникам Q^* и Q' без вершин q_1 и q'_1, получаем

$$\overline{q_2q^*_n} \;\leq\; \overline{q'_2q'_n}. \tag{3}$$

Следовательно,

$$\overline{q'_1q'_n} \overset{(*)}{\geq} \overline{q'_2q'_n} - \overline{q'_1q'_2} \overset{(3)}{\geq} \overline{q_2q^*_n} - \overline{q_1q_2} \overset{(2)}{=} \overline{q_1q^*_n} \overset{(1)}{>} \overline{q_1q_n},$$

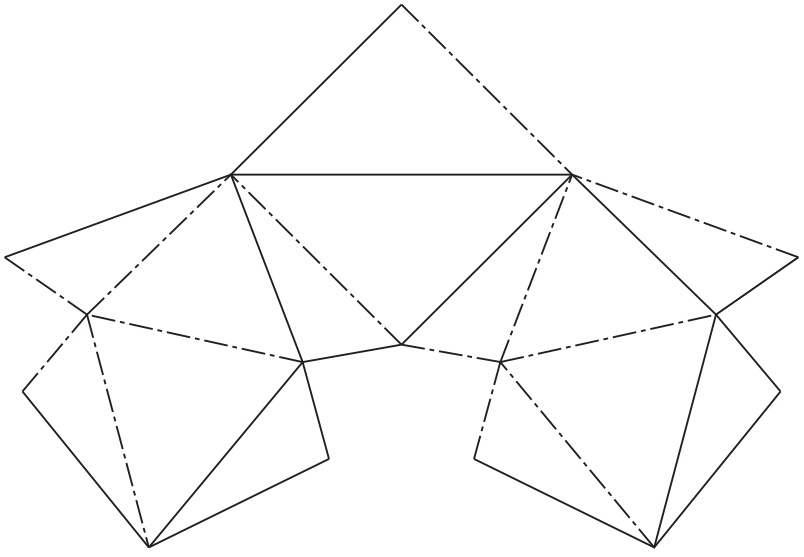
где переход $(*)$ — просто неравенство треугольника, а все остальные соотношения уже были доказаны. □

Мы приводили пример *невыпуклых* многогранников, для которых теорема Коши неверна. Особенностью этого примера является то, что один многогранник переводится в другой разрывным «щелчком», который сохраняет грани конгруэнтными, но двугранные углы изменяет скачкообразно. Возникает вопрос:

> *Существует ли* непрерывное *преобразование некоторого невыпуклого многогранника, сохраняющее его грани плоскими и конгруэнтными?*

Предполагалось, что не существует триангулируемых поверхностей, выпуклых или нет, допускающих такое преобразование. Поэтому оказалось настоящим сюрпризом, когда в 1977 году — более чем через 160

лет после работы Коши — Роберт Коннелли [2] построил контрпримеры: вложенные в $\mathbb{R}^3$ без самопересечений замкнутые многогранники с треугольными гранями, которые эластичны, т. е. допускают непрерывное преобразование, сохраняющее длины всех ребер и, следовательно, конгруэнтность треугольных граней.



Замечательный пример гибкой поверхности, который построен Клаусом Стеффеном. В этой модели для вырезания из бумаги пунктирные линии представляют ребра невыпуклых областей. По сплошным линиям нужно согнуть лист так, чтобы получились «хребты», а по пунктирным — чтобы получились «впадины». Длины ребер в этой модели принимают значения 5, 10, 11, 12 и 17 единиц.

Теория жесткости поверхностей имеет в запасе еще много сюрпризов: лишь совсем недавно Иджаду Сабитову [4] удалось доказать, что при деформации любой такой гибкой поверхности ограниченный ею объем должен быть постоянным. Его доказательство замечательно также использованием алгебраических преобразований полиномов и определителей (однако оно слишком сложно для этой книги).

Литература

[1] Cauchy A. *Sur les polygones et les polyèdres, seconde mémoire.* J. École Polytechnique XVIe Cahier, Tome IX (1813), 87–98; Œuvres Complètes, IIe Série, Vol. 1, Paris, 1905, 26–38.

[2] Connelly R. *A counterexample to the rigidity conjecture for polyhedra.* Publication Mathématiques de l'Inst. Haut. Etud. Sci., **47** (1978), 333–338.

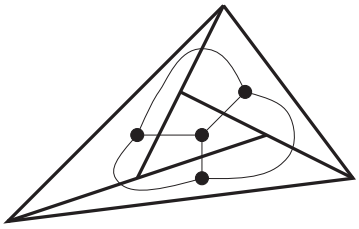
[3] Connelly R. *The rigidity of polyhedral surfaces.* Mathematics Magazine, **52** (1979), 275–283.

[4] Sabitov I. Kh. *The volume as a metric invariant of polyhedra.* Discrete Comput. Geometry, **20** (1998), 405–425.

[5] Schoenberg J., Zaremba S. K. *On Cauchy's lemma concerning convex polygons.* Canadian J. Math., **19** (1967), 1062–1071.

Глава 14 Касание симплексов

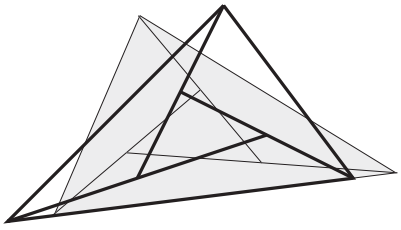
Какое максимальное число d-мерных симплексов можно расположить в $\mathbb{R}^d$ так, чтобы они попарно касались, т. е. так, чтобы все их попарные пересечения были $(d-1)$-мерными?



$f(2) \geq 4$

Это старый и очень естественный вопрос. Обозначим искомое число через $f(d)$. Очевидно, что $f(1) = 2$. Для $d = 2$ конфигурация четырех треугольников, изображенная на полях, показывает, что $f(2) \geq 4$. Аналогичных конфигураций с пятью треугольниками не существует, так как в противном случае построение двойственного графа (который в нашем примере с четырьмя треугольниками дает укладку на плоскость графа K_4) дало бы укладку графа K_5 на плоскости, что невозможно (см. стр. 85). Таким образом,

$$f(2) = 4.$$



$f(3) \geq 8$

Легко показать, что в трехмерном случае $f(3) \geq 8$. Для этого используем изображенную на полях конфигурацию восьми треугольников. Все точки четырех затененных треугольников соединим с некоторой точкой x, находящейся ниже плоскости чертежа, что дает четыре тетраэдра, касающихся плоскости снизу. Аналогично точки четырех светлых треугольников соединим с некоторой точкой y, находящейся выше плоскости чертежа. В результате мы получим конфигурацию восьми касающихся тетраэдров в $\mathbb{R}^3$, т. е. $f(3) \geq 8$.

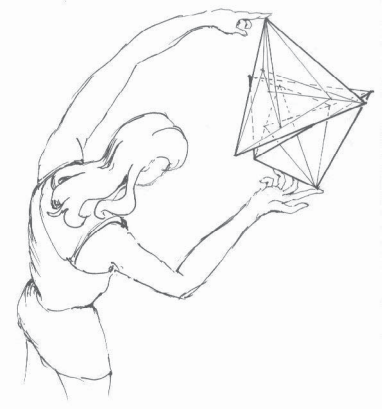
В 1965 году Бастон написал книгу [2], в которой доказал, что $f(3) \leq 9$, а в 1991 году Закс написал другую книгу [5], посвященную доказательству равенства

$$f(3) = 8.$$

Равенства $f(1) = 2, f(2) = 4$ и $f(3) = 8$ приводят к естественной гипотезе, которую впервые сформулировал в 1956 году Багемил [1].

Гипотеза. *Максимальное число попарно касающихся d-мерных симплексов в $\mathbb{R}^d$ есть*

$$f(d) = 2^d.$$

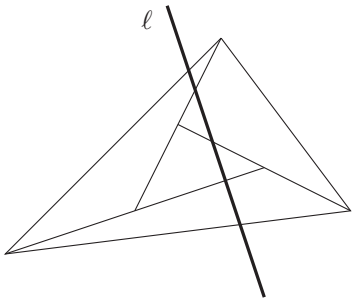


«Касание симплексов»

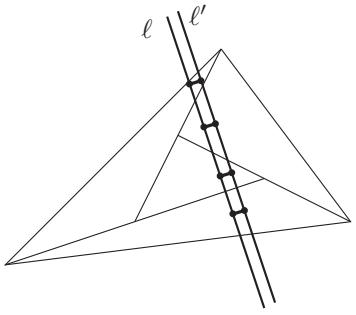
Нижнюю оценку $f(d) \geq 2^d$ легко получить, если выбрать правильный путь. Он состоит в том, чтобы, искусно используя аффинные преобразования координат, а также индукцию по размерности, установить следующий более сильный результат, принадлежащий Заксу [4].

Теорема 1. *Для каждого $d \geq 2$ существует семейство из 2^d попарно касающихся d-симплексов в $\mathbb{R}^d$ и секущей прямой, которая проходит через внутренние точки всех симплексов.*

■ **Доказательство.** В случае $d = 2$ для рассмотренной нами системы из четырех треугольников такая секущая прямая существует. Рассмотрим произвольную конфигурацию из 2^d соприкасающихся d-мерных симплексов с секущей прямой ℓ. Любая достаточно близкая прямая ℓ', параллельная ℓ, тоже является секущей. Выберем параллельные секущие ℓ и ℓ', и для каждого симплекса выберем содержащийся в нем перпендикуляр, соединяющий ℓ и ℓ'. В симплексы конфигурации попадает лишь ограниченная часть прямых ℓ и ℓ'; добавим два соединяющих эти прямые перпендикуляра вне конфигурации так, чтобы ограниченный ими и отрезками прямых ℓ и ℓ' прямоугольник содержал все остальные выбранные перпендикуляры. Тем самым мы получим «лестницу», четыре конца которой лежат вне конфигурации симплексов и которая имеет по одной ступеньке в каждом симплексе.



Главный шаг теперь состоит в применении (аффинного) преобразования координат, отображающего $\mathbb{R}^d$ в $\mathbb{R}^d$, а прямоугольник, покрытый лестницей, — в изображенный на рисунке прямоугольник (половину квадрата), определенный равенством

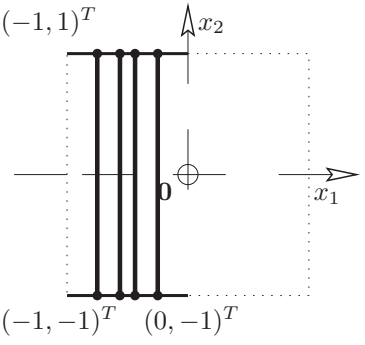


$$R^1 \;=\; \{(x_1, x_2, 0, \ldots, 0)^T : -1 \le x_1 \le 0; -1 \le x_2 \le 1\}.$$

Полученная конфигурация Σ^1 касающихся симплексов в $\mathbb{R}^d$ имеет в качестве секущей прямой ось x_1 и расположена так, что внутри каждого симплекса существует (при некотором α, $-1 < \alpha < 0$) отрезок вида

$$S^1(\alpha) \;=\; \{(\alpha, x_2, 0, \ldots, 0)^T : -1 \le x_2 \le 1\},$$

а начало координат $\mathbf{0}$ лежит вне всех симплексов.



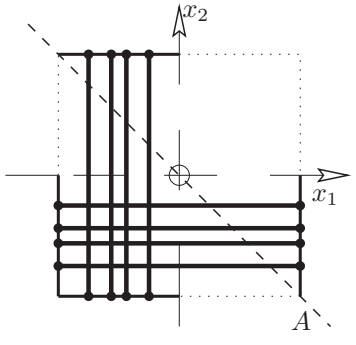
Построим теперь второй экземпляр Σ^2 этой конфигурации, симметричный Σ^1 относительно гиперплоскости $x_1 = x_2$. Конфигурация Σ^2 имеет в качестве секущей прямой ось x_2, и внутри каждого ее симплекса содержится (при некотором $-1 < \beta < 0$) отрезок

$$S^2(\beta) \;=\; \{(x_1, \beta, 0, \ldots, 0)^T : -1 \le x_1 \le 1\}.$$

Но каждый отрезок $S^1(\alpha)$ пересекает каждый отрезок $S^2(\beta)$, поэтому любые два симплекса из Σ^1 и Σ^2 имеют общую внутреннюю для обоих симплексов точку. Значит, если добавить $(d+1)$-ю координату x_{d+1} и построить новую конфигурацию Σ по формуле

$$\{\mathrm{conv}(P_i \cup \{-\boldsymbol{e}_{d+1}\}) : P_i \in \Sigma^1\} \;\cup\; \{\mathrm{conv}(P_j \cup \{\boldsymbol{e}_{d+1}\}) : P_j \in \Sigma^2\},$$

то в $\mathbb{R}^{d+1}$ получится конфигурация касающихся $(d+1)$-мерных симплексов. Далее, антидиагональ



$$A \;=\; \{(x, -x, 0, \ldots, 0)^T : x \in \mathbb{R}\} \;\subseteq\; \mathbb{R}^d$$

пересекает все отрезки $S^1(\alpha)$ и $S^2(\beta)$. Небольшим «шевелением» можно перевести ее в прямую

$$L_\varepsilon \;=\; \{(x, -x, 0, \ldots, 0, \varepsilon x)^T : x \in \mathbb{R}\} \;\subseteq\; \mathbb{R}^{d+1},$$

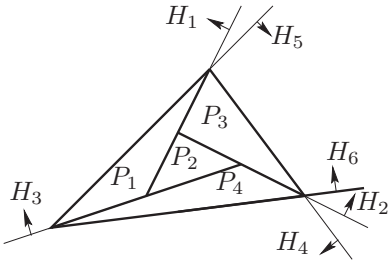
которая при любом достаточно малом $\varepsilon > 0$ пересекает все симплексы из Σ. Это замечание завершает шаг индукции. □

В отличие от экспоненциальной нижней оценки получить точные верхние оценки труднее. Простое индуктивное рассуждение (рассмотрение всех гиперплоскостей граней касающихся симплексов по отдельности) приводит лишь к оценке

$$f(d) \;\le\; \frac{2}{3}(d+1)!,$$

весьма далекой от нижней оценки теоремы 1. Но Миша Перлес [3] нашел «магическое» доказательство значительно лучшей оценки.

Теорема 2. *Для всех $d \ge 1$ справедливо неравенство* $f(d) < 2^{d+1}$.



■ **Доказательство.** Пусть дана конфигурация r касающихся d-мерных симплексов $P_1, P_2, \dots, P_r$ в $\mathbb{R}^d$. Сначала перенумеруем различные гиперплоскости $H_1, H_2, \dots, H_s$, содержащие грани симплексов, для каждой из них произвольно выберем положительную сторону H_i^+, а другую сторону обозначим H_i^-.

Например, для изображенной на полях двумерной конфигурации $r = 4$ треугольников имеем $s = 6$ гиперплоскостей (которые в случае $d = 2$ являются прямыми).

По этому набору построим *B-матрицу* размера $(r \times s)$ с элементами из множества $\{+1, -1, 0\}$:

$$B_{ij} := \begin{cases} +1, & \text{если } P_i \text{ имеет грань в } H_j, \text{ и } P_i \subseteq H_j^+, \\ -1, & \text{если } P_i \text{ имеет грань в } H_j, \text{ и } P_i \subseteq H_j^-, \\ 0, & \text{если } P_i \text{ не имеет грани в } H_j. \end{cases}$$

Например, двумерная конфигурация на полях определяет матрицу

$$B = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ -1 & -1 & 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 1 & 0 & 0 \\ 0 & -1 & -1 & 0 & 0 & 1 \end{pmatrix}.$$

Отметим три свойства этой B-матрицы. Во-первых, поскольку каждый d-мерный симплекс имеет $d+1$ граней, любая строка матрицы B имеет ровно $d+1$ ненулевых элементов и, значит, ровно $s-(d+1)$ нулевых элементов. Во-вторых, так как в конфигурации симплексы попарно касаются, то для каждой пары строк существует столбец, с которым одна строка пересекается по $+1$, а другая — по -1. Значит, строки различаются *по одним только ненулевым элементам*. В-третьих, строки матрицы B «представляют» симплексы P_i равенствами

$$P_i \;=\; \bigcap_{j:B_{ij}=1} H_j^+ \;\cap\; \bigcap_{j:B_{ij}=-1} H_j^-. \qquad (*)$$

Построим по B матрицу C, заменяя каждую строку матрицы B всеми вектор-строками, которые получаются из нее при замене каждого нуля либо на $+1$, либо на -1. Так как каждая строка B содержит $s-d-1$ нулей, а B имеет r строк, то матрица C имеет $2^{s-d-1}r$ строк.

В нашем примере матрица C имеет размер (32×6), и ее первыми строками являются

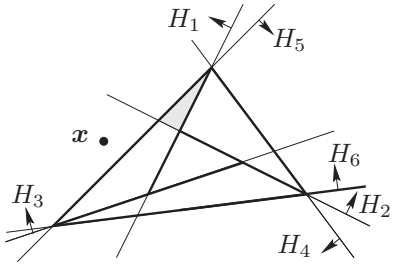
$$C = \left(\begin{array}{rrrrrr} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 \\ \hline -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 & 1 & -1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{array}\right).$$

Первые восемь строк матрицы C получены из первой строки матрицы B, следующие восемь строк — из второй строки B, и т. д.

Заметим теперь, что все строки матрицы C различны: если две ее строки получены из одной и той же строки матрицы B, то они различны, поскольку множество нулей заменялось разными наборами ± 1; если же эти строки матрицы C получены из разных строк матрицы B, то они различаются при любом способе замены нулей. Однако строки матрицы C — это (± 1)-векторы размерности s, и число таких векторов равно 2^s. Так как все строки матрицы C различны, то их число не больше 2^s, т. е.

$$2^{s-d-1}r \;\leq\; 2^s.$$

Далее, среди строк матрицы C появляются не все возможные (± 1)-векторы; поэтому верно строгое неравенство $2^{s-d-1}r < 2^s$, и $r < 2^{d+1}$. Действительно, любая строка матрицы C представляет пересечение полупространств — точно так же, как ранее строки матрицы B по формуле $(*)$ представляли симплексы. Это пересечение есть подмножество симплекса P_i, который определялся строкой матрицы B, порождающей строку матрицы C. Выберем точку $\boldsymbol{x} \in \mathbb{R}^d$, не принадлежащую ни одной из гиперплоскостей H_j и ни одному из симплексов P_i. По точке $\boldsymbol{x}$ построим (± 1)-вектор, который для каждого j указывает, какое из соотношений $\boldsymbol{x} \in H_j^+$ и $\boldsymbol{x} \in H_j^-$ выполняется. Этот (± 1)-вектор отсутствует среди строк матрицы C, так как согласно $(*)$ соответствующее ему пересечение полупространств содержит точку $\boldsymbol{x}$ и поэтому не содержится ни в одном из симплексов P_i. □



Первая строка матрицы C представляет заштрихованный треугольник, а вторая — пустое пересечение полупространств. Точка $\boldsymbol{x}$ соответствует вектору

$$\begin{pmatrix} 1 & -1 & 1 & 1 & -1 & 1 \end{pmatrix},$$

который не является строкой матрицы C.

Литература

[1] Bagemihl F. *A conjecture concerning neighboring tetrahedra.* Amer. Math. Monthly, **63** (1956) 328–329.

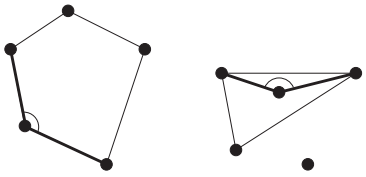
[2] Baston V. J. D. *Some Properties of Polyhedra in Euclidean Space.* Pergamon Press, Oxford, 1965.

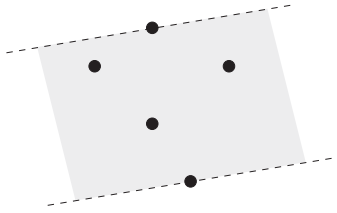
[3] Perles M. A. *At most* 2^{d+1} *neighborly simplices in* E^d. Annals of Discrete Math., **20** (1984), 253–254.

[4] Zaks J. *Neighborly families of* 2^d *d-simplices in* E^d. Geometriae Dedicata, **11** (1981), 279–296.

[5] Zaks J. *No Nine Neighborly Tetrahedra Exist.* Memoirs Amer. Math. Soc., No. 447, Vol. 91, 1991.

Глава 15 Каждое большое точечное множество имеет тупой угол





Около 1950 года Пауль Эрдёш предположил, что если множество в пространстве $\mathbb{R}^d$ имеет более 2^d точек, то в нем есть по крайней мере один *тупой угол*, т. е. угол, который строго больше $\frac{\pi}{2}$. Другими словами, любое множество точек в $\mathbb{R}^d$, образующих только острые или прямые углы, содержит не более 2^d точек[1]. Математическое общество Нидерландов установило приз за решение этой задачи, однако доказательства были получены лишь для $d = 2$ и $d = 3$.

В случае $d = 2$ это простая задача. Пять точек могут определять выпуклый пятиугольник, который всегда имеет тупой угол (более того, по крайней мере один его угол не меньше 108°). В противном случае существует точка, лежащая внутри треугольника, образованного тремя другими точками. Но эта точка «видит» стороны треугольника под тремя углами, сумма которых равна 360°, так что один из этих углов не меньше 120°. (Второй случай включает также ситуацию, когда три точки лежат на одной прямой и, следовательно, существует угол, равный 180°.)

Независимо от этого несколькими годами позже Виктор Кли поставил, а Эрдёш распространил вопрос о том, какое максимальное число точек может содержать точечное множество в $\mathbb{R}^d$, если для *любых* двух его точек существуют две такие проходящие через них параллельные гиперплоскости, что в ограниченном ими слое лежат все остальные точки множества.

Затем в 1962 году Людвиг Данцер и Бранко Грюнбаум [1] нашли решение обеих задач, занимающее одну строку: они включили объемы обоих максимальных множеств точек в цепочку неравенств, которая начинается и заканчивается числом 2^d. Таким образом, ответ равен 2^d как для задачи Эрдёша, так и для задачи Кли.

В дальнейшем мы рассматриваем (конечные) множества точек $S \subseteq \mathbb{R}^d$, их выпуклые оболочки $\mathrm{conv}(S)$ и общие выпуклые политопы $Q \subseteq \mathbb{R}^d$. (Основные определения и свойства политопов приведены в приложении к гл. 8.) Мы предполагаем, что эти множества имеют полную размерность d, т. е. они не содержатся ни в какой гиперплоскости. Два выпуклых множества *касаются*, если они имеют хотя бы одну общую граничную точку, но их внутренности не пересекаются. Для любого множества $Q \subseteq \mathbb{R}^d$ и любого вектора $\boldsymbol{s} \in \mathbb{R}^d$ обозначим через $Q + \boldsymbol{s}$ сдвиг Q на $\boldsymbol{s}$, т. е. образ Q при параллельном переносе, переводящем $\mathbf{0}$ в $\boldsymbol{s}$. Аналогично, сдвиг $Q - \boldsymbol{s}$ есть образ Q при параллельном переносе, переводящем $\boldsymbol{s}$ в начало координат.

Не пугайтесь: эта глава — экскурс в d-мерную геометрию, но в дальнейшем рассуждения не потребуют какой-либо «многомерной интуи-

[1] Примером такого множества является совокупность вершин d-мерного куба, см. доказательство теоремы 1 ниже. — *Прим. ред.*

ции», так как за ними можно проследить, рисуя (и, следовательно, *понимая*) трехмерные или даже двумерные картинки. Поэтому наши рисунки будут иллюстрировать доказательство для $d = 2$ (где «гиперплоскость» есть просто прямая), а Вы можете сделать собственные рисунки для $d = 3$ (где «гиперплоскость» является плоскостью).

Теорема 1. *Для каждого d справедлива следующая цепочка неравенств:*

$$
\begin{aligned}
2^d &\overset{(1)}{\leq} \max\left\{\#S \,\middle|\, S \subseteq \mathbb{R}^d,\ \sphericalangle(\boldsymbol{s}_i, \boldsymbol{s}_j, \boldsymbol{s}_k) \leq \tfrac{\pi}{2} \text{ для любых } \boldsymbol{s}_i, \boldsymbol{s}_j, \boldsymbol{s}_k \subseteq S\right\} \\
&\overset{(2)}{\leq} \max\left\{\#S \,\middle|\, S \subseteq \mathbb{R}^d,\ \begin{array}{l}\text{для любых двух точек } \boldsymbol{s}_i, \boldsymbol{s}_j \in S \\ \text{существует слой, ограниченный про-} \\ \text{ходящими через них параллельными ги-} \\ \text{перплоскостями и содержащий множе-} \\ \text{ство } S\end{array}\right\} \\
&\overset{(3)}{=} \max\left\{\#S \,\middle|\, S \subseteq \mathbb{R}^d,\ \begin{array}{l}\text{сдвиги } P - \boldsymbol{s}_i \text{ выпуклой оболочки} \\ P := \mathrm{conv(S)} \text{ имеют общую точку, но} \\ \text{лишь касаются в ней}\end{array}\right\} \\
&\overset{(4)}{\leq} \max\left\{\#S \,\middle|\, S \subseteq \mathbb{R}^d,\ \begin{array}{l}\text{сдвиги } Q + \boldsymbol{s}_i \text{ некоторого } d\text{-мерного вы-} \\ \text{пуклого политопа } Q \subseteq \mathbb{R}^d \text{ попарно каса-} \\ \text{ются}\end{array}\right\} \\
&\overset{(5)}{=} \max\left\{\#S \,\middle|\, S \subseteq \mathbb{R}^d,\ \begin{array}{l}\text{сдвиги } Q^* + \boldsymbol{s}_i \text{ некоторого } d\text{-мерного цен-} \\ \text{трально симметричного выпуклого по-} \\ \text{литопа } Q^* \subseteq \mathbb{R}^d \text{ попарно касаются}\end{array}\right\} \\
&\overset{(6)}{\leq} 2^d.
\end{aligned}
$$

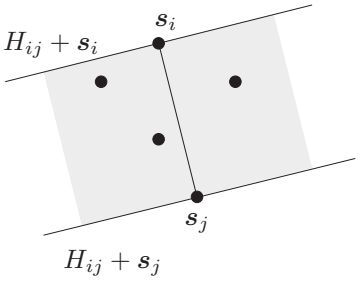
■ **Доказательство.** Мы должны проверить шесть утверждений (равенств и неравенств). Приступим к делу.

(1) Пусть $S := \{0, 1\}^d$ — множество вершин стандартного единичного куба в $\mathbb{R}^d$; выберем точки $\boldsymbol{s}_i, \boldsymbol{s}_j, \boldsymbol{s}_k \in S$. Ввиду симметрии можно предположить, что $\boldsymbol{s}_j = \mathbf{0}$ — нулевой вектор. Поэтому угол можно вычислить, используя равенство

$$\cos \sphericalangle(\boldsymbol{s}_i, \boldsymbol{s}_j, \boldsymbol{s}_k) = \frac{\langle \boldsymbol{s}_i, \boldsymbol{s}_k \rangle}{|\boldsymbol{s}_i||\boldsymbol{s}_k|},$$

правая часть которого, очевидно, неотрицательна. Следовательно, S — множество из $|S| = 2^d$ точек, которые не образуют тупых углов.

(2) Если множество S не содержит тупых углов, то для любых точек $\boldsymbol{s}_i, \boldsymbol{s}_j \in S$ мы можем рассмотреть параллельные гиперплоскости $H_{ij} + \boldsymbol{s}_i$ и $H_{ij} + \boldsymbol{s}_j$, проходящие соответственно через $\boldsymbol{s}_i$ и $\boldsymbol{s}_j$ и ортогональные отрезку $[\boldsymbol{s}_i, \boldsymbol{s}_j]$. Здесь $H_{ij} = \{\boldsymbol{x} \in \mathbb{R}^d : \langle \boldsymbol{x}, \boldsymbol{s}_i - \boldsymbol{s}_j \rangle = 0\}$ — гиперплоскость, *проходящая через начало координат* и ортогональная прямой, проходящей через точки $\boldsymbol{s}_i$ и $\boldsymbol{s}_j$, а $H_{ij} + \boldsymbol{s}_j = \{\boldsymbol{x} + \boldsymbol{s}_j : \boldsymbol{x} \in H_{ij}\}$ — сдвиг гиперплоскости H_{ij}, проходящий через $\boldsymbol{s}_j$, и т. д. Следовательно, полоса между $H_{ij} + \boldsymbol{s}_i$ и $H_{ij} + \boldsymbol{s}_j$ состоит (за исключением $\boldsymbol{s}_i$ и $\boldsymbol{s}_j$) в точности из всех таких точек $\boldsymbol{x} \in \mathbb{R}^d$, для которых углы $\sphericalangle(\boldsymbol{s}_i, \boldsymbol{s}_j, \boldsymbol{x})$ и $\sphericalangle(\boldsymbol{s}_j, \boldsymbol{s}_i, \boldsymbol{x})$ не являются тупыми. Таким образом, полоса содержит все множество S.

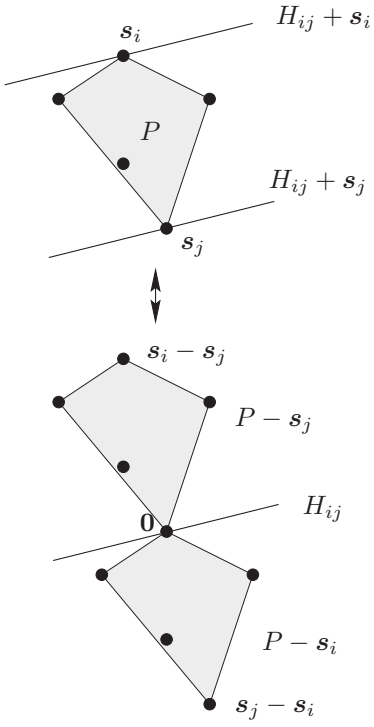


(3) Политоп P целиком лежит по ту же сторону от $H_{ij} + \boldsymbol{s}_j$, что и точка $\boldsymbol{s}_i$, тогда и только тогда, когда $P - \boldsymbol{s}_j$ лежит по ту же сторону

от H_{ij}, что и $\boldsymbol{s}_i - \boldsymbol{s}_j$. Действительно, свойство «объект содержится в полупространстве» сохраняется при параллельном переносе и объекта, и полупространства на один и тот же вектор (именно, на $-\boldsymbol{s}_j$). Аналогично, политоп P целиком лежит по ту же сторону от $H_{ij} + \boldsymbol{s}_i$, что и $\boldsymbol{s}_j$, тогда и только тогда, когда $P - \boldsymbol{s}_i$ лежит по ту же сторону от H_{ij}, что и $\boldsymbol{s}_j - \boldsymbol{s}_i$.

Соединяя эти два утверждения, находим, что политоп P лежит в полосе между $H_{ij} + \boldsymbol{s}_i$ и $H_{ij} + \boldsymbol{s}_j$ тогда и только тогда, когда $P - \boldsymbol{s}_i$ и $P - \boldsymbol{s}_j$ лежат по разные стороны от гиперплоскости H_{ij}.

Это соответствие иллюстрируется наброском на полях.



Кроме того, из условий $\boldsymbol{s}_i \in P = \operatorname{conv}(S)$ мы получаем, что начало координат $\mathbf{0}$ содержится во всех политопах $P - \boldsymbol{s}_i$ ($\boldsymbol{s}_i \in S$). Таким образом, все множества $P - \boldsymbol{s}_i$ имеют общую точку $\mathbf{0}$, но они лишь попарно касаются, так как $P - \boldsymbol{s}_i$ и $P - \boldsymbol{s}_j$ находятся по разные стороны от гиперплоскости H_{ij}.

(4) Это неравенство мы получаем без труда: условия «образы области при параллельных переносах попарно касаются» слабее условия «образы имеют общую точку, но лишь касаются». Аналогично можно ослабить условия, взяв в качестве P произвольный выпуклый d-мерный политоп в $\mathbb{R}^d$. Кроме того, можно заменить S на $-S$.

(5) Здесь неравенство «$\geq$» тривиально, но не представляет для нас интереса. Пусть конфигурация $S \subseteq \mathbb{R}^d$ и произвольный d-мерный политоп $Q \subseteq \mathbb{R}^d$ таковы, что сдвиги $Q + \boldsymbol{s}_i$ ($\boldsymbol{s}_i \in S$) попарно касаются. Утверждение состоит в том, что тогда мы можем вместо Q использовать множество

$$Q^* := \left\{ \tfrac{1}{2}(\boldsymbol{x} - \boldsymbol{y}) \in \mathbb{R}^d : \boldsymbol{x}, \boldsymbol{y} \in Q \right\}.$$

Заметим прежде всего, что множество Q^* является d-мерным, выпуклым и центрально-симметричным. Нетрудно проверить, что Q^* — политоп (его вершины имеют вид $\frac{1}{2}(\boldsymbol{q}_i - \boldsymbol{q}_j)$, где $\boldsymbol{q}_i, \boldsymbol{q}_j$ — вершины политопа Q), но это для нас не существенно.

Теперь покажем, что сдвиги $Q + \boldsymbol{s}_i$ и $Q + \boldsymbol{s}_j$ касаются *тогда и только тогда*, когда касаются $Q^* + \boldsymbol{s}_i$ и $Q^* + \boldsymbol{s}_j$. Для этого заметим, следуя Минковскому [3], что

$$\begin{aligned}
&(Q^* + \boldsymbol{s}_i) \cap (Q^* + \boldsymbol{s}_j) \neq \varnothing \\
&\quad \iff \exists\, \boldsymbol{q}_i', \boldsymbol{q}_i'', \boldsymbol{q}_j', \boldsymbol{q}_j'' \in Q : \tfrac{1}{2}(\boldsymbol{q}_i' - \boldsymbol{q}_i'') + \boldsymbol{s}_i = \tfrac{1}{2}(\boldsymbol{q}_j' - \boldsymbol{q}_j'') + \boldsymbol{s}_j \\
&\quad \iff \exists\, \boldsymbol{q}_i', \boldsymbol{q}_i'', \boldsymbol{q}_j', \boldsymbol{q}_j'' \in Q : \tfrac{1}{2}(\boldsymbol{q}_i' + \boldsymbol{q}_j'') + \boldsymbol{s}_i = \tfrac{1}{2}(\boldsymbol{q}_j' + \boldsymbol{q}_i'') + \boldsymbol{s}_j \\
&\quad \iff \exists\, \boldsymbol{q}_i, \boldsymbol{q}_j \in Q : \boldsymbol{q}_i + \boldsymbol{s}_i = \boldsymbol{q}_j + \boldsymbol{s}_j \\
&\quad \iff (Q + \boldsymbol{s}_i) \cap (Q + \boldsymbol{s}_j) \neq \varnothing;
\end{aligned}$$

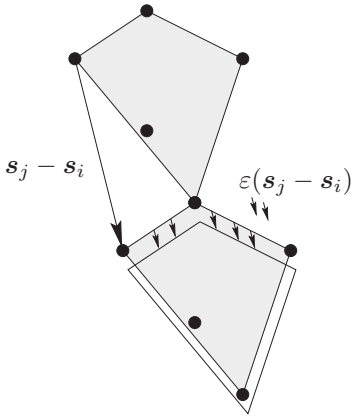
при доказательстве третьего (и главного) перехода «$\iff$» для обоснования «$\Leftarrow$» используется возможность представления любого $\boldsymbol{q} \in Q$ в виде $\boldsymbol{q} = \frac{1}{2}(\boldsymbol{q} + \boldsymbol{q})$, а для обоснования «$\Rightarrow$» — выпуклость политопа Q, в силу которой $\frac{1}{2}(\boldsymbol{q}_i' + \boldsymbol{q}_j'')$, $\frac{1}{2}(\boldsymbol{q}_j' + \boldsymbol{q}_i'') \in Q$.

Таким образом, переход от Q к Q^* (известный как *симметризация Минковского*) сохраняет свойство пересечения сдвигов $Q + \boldsymbol{s}_i$ и $Q + \boldsymbol{s}_j$.

Другими словами, нам достаточно показать, что если Q — любое выпуклое множество, то его сдвиги $Q+\boldsymbol{s}_i$ и $Q+\boldsymbol{s}_j$ пересекаются тогда и только тогда, когда пересекаются сдвиги $Q^*+\boldsymbol{s}_i$ и $Q^*+\boldsymbol{s}_j$.

Следующая характеризация показывает, что симметризация Минковского сохраняет также свойство касания двух сдвигов:

> *$Q+\boldsymbol{s}_i$ и $Q+\boldsymbol{s}_j$ касаются тогда и только тогда, когда они пересекаются и при этом $Q+\boldsymbol{s}_i$ и $Q+\boldsymbol{s}_j+\varepsilon(\boldsymbol{s}_j-\boldsymbol{s}_i)$ не пересекаются при любом $\varepsilon>0$.*



(6) Предположим, что $Q^*+\boldsymbol{s}_i$ и $Q^*+\boldsymbol{s}_j$ касаются. Для каждой точки пересечения

$$\boldsymbol{x}\in(Q^*+\boldsymbol{s}_i)\cap(Q^*+\boldsymbol{s}_j)$$

имеем

$$\boldsymbol{x}-\boldsymbol{s}_i\in Q^* \quad \text{и} \quad \boldsymbol{x}-\boldsymbol{s}_j\in Q^*,$$

так что вследствие центральной симметричности Q^*

$$\boldsymbol{s}_i-\boldsymbol{x}=-(\boldsymbol{x}-\boldsymbol{s}_i)\in Q^*,$$

и поэтому ввиду выпуклости Q^*

$$\tfrac{1}{2}(\boldsymbol{s}_i-\boldsymbol{s}_j)=\tfrac{1}{2}\left((\boldsymbol{x}-\boldsymbol{s}_j)+(\boldsymbol{s}_i-\boldsymbol{x})\right)\in Q^*.$$

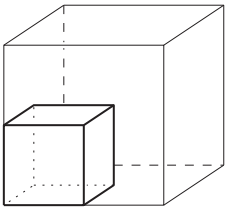
Мы приходим к выводу, что при любом i точка $\frac{1}{2}(\boldsymbol{s}_i+\boldsymbol{s}_j)$ содержится в $Q^*+\boldsymbol{s}_j$. Следовательно, выпуклая оболочка $P:=\operatorname{conv}(S)$ удовлетворяет условию

$$P_j:=\tfrac{1}{2}\,(P+\boldsymbol{s}_j)=\operatorname{conv}\left\{\tfrac{1}{2}\,(\boldsymbol{s}_i+\boldsymbol{s}_j):\boldsymbol{s}_i\in S\right\}\subseteq Q^*+\boldsymbol{s}_j,$$

откуда вытекает, что множества $P_j=\frac{1}{2}\,(P+\boldsymbol{s}_j)$ могут только касаться.

Наконец, множества P_j содержатся в P, так как все точки $\boldsymbol{s}_i$, $\boldsymbol{s}_j$ и $\frac{1}{2}\,(\boldsymbol{s}_i+\boldsymbol{s}_j)$ лежат в P в силу его выпуклости. Но множества P_j на самом деле являются гомотетичными образами политопа P, содержащимися в P. Коэффициент подобия равен $\frac{1}{2}$, и так как мы имеем дело с d-мерными множествами, то

$$\operatorname{vol}(P_j) \;=\; \frac{1}{2^d}\operatorname{vol}(P).$$



Коэффициент подобия $\frac{1}{2}$, $\operatorname{vol}(P_j)=\frac{1}{8}\operatorname{vol}(P)$

Это означает, что в P_j может помещаться не более 2^d непересекающихся множеств P_j, следовательно, $|S|\le 2^d$.

Тем самым наше доказательство завершено: цепочка неравенств замкнулась. □

...но на этом история не кончается. Данцер и Грюнбаум поставили следующий естественный вопрос:

> *Что изменится, если потребовать, чтобы все углы были не просто не тупыми, а острыми, т. е. если запретить и прямые углы?*

Они построили в пространстве $\mathbb{R}^d$ конфигурации из $2d-1$ точек, имеющие только острые углы, и предположили, что лучшего результата добиться нельзя. Грюнбаум доказал, что это действительно верно при

$d \le 3$. Но через двадцать один год, в 1983 г., Пауль Эрдёш и Золтан Фюреди [2] показали, что это предположение не только неверно, но и очень далеко от истины, если размерность высока! Их доказательство дает замечательный пример силы вероятностных рассуждений (см. гл. 40 в качестве введения в «вероятностный метод»). В нашем варианте доказательства используется слегка усовершенствованный выбор параметров, предложенный Дэвидом Бевэном.

Теорема 2. *Для каждого $d \ge 2$ существует множество $S \subseteq \{0,1\}^d$, содержащее $2\lfloor \frac{\sqrt{6}}{9}\big(\frac{2}{\sqrt{3}}\big)^d \rfloor$ точек в $\mathbb{R}^d$ (вершин единичного d-мерного куба), которые образуют только острые углы. В частности, для размерности $d = 34$ существует множество, состоящее из $72 > 2\cdot 34 - 1$ точек, образующих только острые углы.*

■ **Доказательство.** Положим $m := \lfloor \frac{\sqrt{6}}{9}\big(\frac{2}{\sqrt{3}}\big)^d \rfloor$ и рассмотрим $3m$ векторов

$$\boldsymbol{x}(1), \boldsymbol{x}(2), \dots, \boldsymbol{x}(3m) \ \in \ \{0,1\}^d,$$

выбирая все их координаты независимо и случайно так, что каждая из них принимает значения 0 и 1 с вероятностью $\frac{1}{2}$. (Для этого можно $3md$ раз подбросить идеальную монету, однако при большом d это занятие скоро наскучит.)

Мы уже убедились, что все углы, образованные 0/1-векторами, не тупые. Три вектора $\boldsymbol{x}(i), \boldsymbol{x}(j), \boldsymbol{x}(k)$ образуют прямой угол с вершиной в $\boldsymbol{x}(j)$ тогда и только тогда, когда скалярное произведение

$$\big\langle\, \boldsymbol{x}(i) - \boldsymbol{x}(j), \boldsymbol{x}(k) - \boldsymbol{x}(j) \,\big\rangle$$

обращается в нуль, т. е. если для каждой координаты ℓ

$$x(i)_\ell - x(j)_\ell = 0 \quad \text{или} \quad x(k)_\ell - x(j)_\ell = 0.$$

В этом случае назовем тройку (i,j,k) *плохой*. (Если $\boldsymbol{x}(i) = \boldsymbol{x}(j)$ или $\boldsymbol{x}(j) = \boldsymbol{x}(k)$, то угол не определен, но тогда тройка (i,j,k) заведомо плохая.)

Вероятность того, что одна конкретная тройка является плохой, равна $\big(\frac{3}{4}\big)^d$. Действительно, тройка хорошая тогда и только тогда, когда для какой-нибудь (скажем, ℓ-й) из d координат

$$\begin{aligned} &\text{либо} \quad x(i)_\ell = x(k)_\ell = 0, \quad x(j)_\ell = 1, \\ &\text{либо} \quad x(i)_\ell = x(k)_\ell = 1, \quad x(j)_\ell = 0. \end{aligned}$$

Значит, для этой координаты существует шесть плохих из восьми возможных равновероятных наборов значений $x(i)_\ell$, $x(j)_\ell$, $x(k)_\ell$, и тройка оказывается плохой тогда и только тогда, когда для каждой из d координат реализуется один из плохих вариантов (для любой координаты вероятность такого события равна $\frac{3}{4}$).

Число троек, которые нужно рассмотреть, равно $3\binom{3m}{3}$, так как существует $\binom{3m}{3}$ наборов по три вектора и для каждого набора вершину угла можно выбрать тремя способами. Конечно, события, состоящие в том, что различные тройки плохие, не являются независимыми. Но из *линейности математического ожидания* (которое соответствует усреднению по всем возможным выборам, см. приложение) следует,

что *математическое ожидание* числа плохих троек в точности равно $3\binom{3m}{3}\left(\frac{3}{4}\right)^d$. Это означает (именно здесь проявляется сила вероятностного метода!), что существует набор из $3m$ векторов, для которого число плохих троек не больше $3\binom{3m}{3}\left(\frac{3}{4}\right)^d$, причем в силу выбора m

$$3\binom{3m}{3}\left(\tfrac{3}{4}\right)^d \;<\; 3\tfrac{(3m)^3}{6}\left(\tfrac{3}{4}\right)^d \;=\; m^3\left(\tfrac{9}{\sqrt{6}}\right)^2\left(\tfrac{3}{4}\right)^d \;\le\; m.$$

Но если число плохих троек меньше m, то мы можем из $3m$ векторов $\boldsymbol{x}(i)$ удалить такие m векторов, что оставшиеся $2m$ векторов не будут образовывать плохих троек, т. е. они будут образовывать только острые углы. □

«Вероятностную конструкцию» большого множества 0/1-точек, не образующих прямых углов, легко реализовать, используя датчик случайных чисел для «бросания монеты». Дэвид Бевэн построил таким способом в 15-мерном пространстве множество, содержащее 31 точку, все углы между которыми — острые.

Приложение: три инструмента теории вероятностей

Здесь описаны три основных инструмента дискретной теории вероятностей, которые будут использоваться много раз: случайные величины, линейность математического ожидания и неравенство Маркова.

Пусть (Ω, p) — конечное *вероятностное пространство*, т. е. Ω — конечное множество и $p = \mathrm{Prob}$ — такое отображение[2] Ω в отрезок $[0,1]$, что $\sum_{\omega\in\Omega} p(\omega) = 1$. *Случайная величина* X на Ω — это отображение $X : \Omega \longrightarrow \mathbb{R}$. Определим вероятностное пространство на образе $X(\Omega)$, положив $p(X = x) := \sum_{X(\omega)=x} p(\omega)$. Простым примером является идеальный игральный кубик (все $p(\omega) = \frac{1}{6}$); в этом случае $X =$ «число на верхней грани брошенного кубика».

Математическое ожидание EX случайной величины X есть взвешенное среднее ее значений, т. е.

$$EX \;=\; \sum_{\omega\in\Omega} p(\omega)X(\omega).$$

Пусть теперь X и Y — две случайные величины на Ω; тогда сумма $X + Y$ — тоже случайная величина, и

$$\begin{aligned} E(X+Y) \;&=\; \sum_{\omega} p(\omega)(X(\omega)+Y(\omega)) \\ &=\; \sum_{\omega} p(\omega)X(\omega) + \sum_{\omega} p(\omega)Y(\omega) \;=\; EX + EY. \end{aligned}$$

Ясно, что это равенство можно распространить на любую конечную линейную комбинацию случайных величин. Это свойство называется *линейностью математического ожидания*. Заметим, что оно имеет место без предположения о том, что случайные величины «независимы» в том или ином смысле!

[2] В теории вероятностей множество Ω называют *пространством элементарных событий*, а отображение $p = \mathrm{Prob}$ — *распределением вероятностей* или *вероятностной мерой* на Ω. — *Прим. ред.*

Наш третий инструмент можно применять к случайным величинам X, которые принимают лишь неотрицательные значения, что для краткости обозначается $X \geq 0$. Пусть

$$\mathrm{Prob}(X \geq a) \;=\; \sum_{\omega : X(\omega) \geq a} p(\omega)$$

есть вероятность того, что X не меньше некоторого $a > 0$. Тогда

$$EX \;=\; \sum_{\omega : X(\omega) \geq a} p(\omega) X(\omega) \;+\; \sum_{\omega : X(\omega) < a} p(\omega) X(\omega) \;\geq\; a \sum_{\omega : X(\omega) \geq a} p(\omega),$$

и мы доказали *неравенство Маркова*

$$\mathrm{Prob}(X \geq a) \;\leq\; \frac{EX}{a}\,.$$

Литература

[1] Danzer L., Grünbaum B. *Über zwei Probleme bezüglich konvexer Körper von P. Erdös und von V. L. Klee.* Math. Zeitschrift, **79** (1962), 95–99.

[2] Erdős P., Füredi Z. *The greatest angle among n points in the d-dimensional Euclidean space.* Annals of Discrete Math., **17** (1983), 275–283.

[3] Minkowski H. *Dichteste gitterförmige Lagerung kongruenter Körper.* Nachrichten Ges. Wiss. Göttingen, Math.-Phys. Klasse, 1904, 311–355.

Гипотеза Борсука

Глава 16

Статья Карола Борсука 1933 года «Три теоремы об n-мерной евклидовой сфере» (см. [1]) известна тем, что содержит важный результат (сформулированный как гипотеза Станиславом Уламом), который теперь называют теоремой Борсука – Улама.

> *Каждое непрерывное отображение $f : S^d \to \mathbb{R}^d$ отображает две антиподальные точки сферы S^d в одну и ту же точку $\mathbb{R}^d$.*

Эту статью сделала известной также поставленная в ее конце задача, которую назвали гипотезой Борсука:

> *Любое ли множество $S \subseteq \mathbb{R}^d$ ограниченного диаметра $\operatorname{diam}(S) > 0$ можно разбить на не более чем $d+1$ множеств меньшего диаметра?*

Карол Борсук

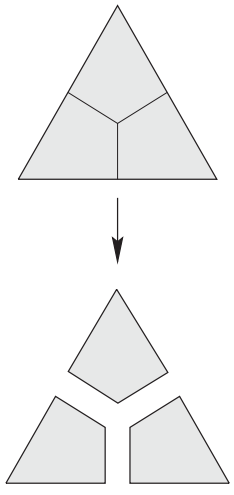
(*Диаметром* множества называется верхняя грань расстояний между его точками. — *Прим. ред.*) Значение $d+1$ является наилучшим из возможных: если S — правильный d-мерный симплекс или просто множество его $d+1$ вершин, то ни одна из частей разбиения, имеющая меньший диаметр, не может содержать более одной вершины симплекса. Пусть $f(d)$ — такое наименьшее число, что каждое ограниченное множество $S \subseteq \mathbb{R}^d$ можно разбить на $f(d)$ частей меньшего диаметра. Пример правильного симплекса показывает, что $f(d) \geq d+1$.

Гипотеза Борсука была доказана для случая, когда S — сфера (самим Борсуком), для гладких тел S (с использованием теоремы Борсука – Улама), для $d \leq 3$ и еще для нескольких случаев, но в общем случае гипотеза оставалась открытой[1]. Наилучшую известную верхнюю оценку для $f(d)$ получил Одед Шрамм [6]: он показал, что для всех достаточно больших d

$$f(d) \leq (1.23)^d.$$

Эта оценка выглядит очень слабой по сравнению с гипотезой «$f(d) = d+1$», но неожиданно она оказалась разумной, когда Джефф Кан и Гил Калаи в 1993 году [3] эффектно опровергли гипотезу Борсука. Через шестьдесят лет после статьи Борсука Кан и Калаи доказали, что для достаточно больших d справедливо неравенство $f(d) \geq (1.2)^{\sqrt{d}}$.

Достойную Книги версию доказательства Кана – Калаи получила А.Нилли [4]: короткое и полное, оно дает явный контрпример к гипотезе Борсука для размерности $d = 946$. Мы приведем здесь модификацию этого доказательства, принадлежащую Андрею Райгородскому [5]



Любой d-симплекс *можно* разбить на $d+1$ частей меньшего диаметра.

[1] Обзор работ, связанных с гипотезой Борсука и опубликованных до 1969 года включительно, можно найти в [9*], стр. 58–94. — *Прим. перев.*

и Бернульфу Вайсбаху [7], которые сократили размерность до $d = 561$ и даже до $d = 560$. Последний «рекорд», установленный в 2003 году Аике Хинричсом и Кристианом Рихтером [2], равен $d = 298$.

Теорема. *Пусть $q = p^m$ — степень простого числа, $n = 4q - 2$ и $d = \binom{n}{2} = (2q-1)(4q-3)$. Тогда в $\mathbb{R}^d$ существует множество $S \subseteq \{+1, -1\}^d$, содержащее 2^{n-2} точек и такое, что каждое разбиение S на части меньшего, чем у S, диаметра содержит не менее*

$$\frac{2^{n-2}}{\sum_{i=0}^{q-2} \binom{n-1}{i}}$$

частей. При $q = 9$ отсюда следует, что гипотеза Борсука неверна для размерности $d = 561$. Более того, для всех достаточно больших d справедливо неравенство $f(d) > (1.2)^{\sqrt{d}}$.

А. Нилли

■ **Доказательство.** Построение множества S проводится в четыре шага.

(1) Пусть q — степень простого числа; положим $n = 4q - 2$ и

$$Q \;:=\; \Big\{\boldsymbol{x} \in \{+1,-1\}^n : x_1 = 1,\ \#\{i : x_i = -1\} \text{ четно}\Big\}.$$

Таким образом, Q есть множество 2^{n-2} векторов в $\mathbb{R}^n$. Мы покажем, что для всех векторов $\boldsymbol{x}, \boldsymbol{y} \in Q$ выполняется соотношение $\langle \boldsymbol{x}, \boldsymbol{y} \rangle \equiv 2 \pmod 4$.

Будем называть векторы $\boldsymbol{x}, \boldsymbol{y}$ *почти ортогональными*, если $|\langle \boldsymbol{x}, \boldsymbol{y} \rangle| = 2$. Мы докажем, что любое подмножество $Q' \subseteq Q$, которое не содержит почти ортогональных векторов, должно быть «малым»: $|Q'| \le \sum_{i=0}^{q-2} \binom{n-1}{i}$.

(2) С помощью Q мы построим множество

$$R \;:=\; \{\boldsymbol{x}\boldsymbol{x}^T : \boldsymbol{x} \in Q\},$$

$$\boldsymbol{x} = \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \\ -1 \end{pmatrix} \quad \Longrightarrow$$

$$\boldsymbol{x}^T = \begin{pmatrix} 1 & -1 & -1 & 1 & -1 \end{pmatrix}$$

$$\boldsymbol{x}\boldsymbol{x}^T = \begin{pmatrix} 1 & -1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 & 1 \end{pmatrix}$$

Векторы, матрицы и скалярные произведения

Будем считать все векторы $\boldsymbol{x}, \boldsymbol{y}, \ldots$ векторами-столбцами. Тогда транспонированные векторы $\boldsymbol{x}^T, \boldsymbol{y}^T, \ldots$ — векторы-строки. Матричное произведение $\boldsymbol{x}\boldsymbol{x}^T$ есть матрица ранга 1 с элементами $(\boldsymbol{x}\boldsymbol{x}^T)_{ij} = x_i x_j$.

Если $\boldsymbol{x}, \boldsymbol{y}$ — векторы-столбцы, то их *скалярное произведение* есть

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle \;=\; \sum_i x_i y_i \;=\; \boldsymbol{x}^T \boldsymbol{y}.$$

Нам потребуется также скалярное произведение матриц $X, Y \in \mathbb{R}^{n \times n}$, которые можно интерпретировать как векторы длины n^2, так что их скалярное произведение есть

$$\langle X, Y \rangle \;:=\; \sum_{i,j} x_{ij} y_{ij}.$$

состоящее из 2^{n-2} симметричных $(n \times n)$-матриц ранга 1. Мы интерпретируем эти матрицы как векторы с n^2 компонентами: $R \subseteq \mathbb{R}^{n^2}$. Мы покажем, что все углы между этими векторами острые: для любой пары векторов их скалярное произведение положительно и не меньше 4. Более того, если в $R' \subseteq R$ нет пары векторов со скалярным произведением 4, то $|R'|$ «мало́»: $|R'| \le \sum_{i=0}^{q-2} \binom{n-1}{i}$.

(3) Используя R, мы получим множество точек в пространстве $\mathbb{R}^{\binom{n}{2}}$, координатами которых являются расположенные под главной диагональю элементы соответствующих матриц:

$$S \;:=\; \{(\boldsymbol{x}\boldsymbol{x}^T)_{i>j} : \boldsymbol{x}\boldsymbol{x}^T \in R\}.$$

В множестве S, как и в R, содержится 2^{n-2} точек. Максимальное расстояние между этими точками достигается на почти ортогональных векторах $\boldsymbol{x}, \boldsymbol{y} \in Q$. Поэтому подмножество $S' \subseteq S$ с меньшим, чем у S, диаметром должно быть «малым»: $|S'| \le \sum_{i=0}^{q-2} \binom{n-1}{i}$.

(4) Оценки. Согласно шагу **(3)**, в каждом разбиении S на части меньшего диаметра должно быть не меньше

$$g(q) \;:=\; \frac{2^{4q-4}}{\sum_{i=0}^{q-2} \binom{4q-3}{i}}$$

частей. Следовательно,

$$f(d) \ge \max\{g(q), d+1\} \qquad \text{при} \;\; d \;=\; (2q-1)(4q-3).$$

Поэтому каждое неравенство $g(q) > (2q-1)(4q-3)+1$ дает контрпример к гипотезе Борсука для размерности $d = (2q-1)(4q-3)$. Ниже мы найдем, что $g(9) > 562$ (это дает контрпример для $d = 561$) и докажем неравенство

$$g(q) \;>\; \frac{e}{64\,q^2} \left(\frac{27}{16}\right)^q,$$

которое дает асимптотическую оценку $f(d) > (1.2)^{\sqrt{d}}$ для достаточно больших d.

Детализация шага (1). Начнем с нескольких простых соображений, связанных с делимостью.

Лемма. *Функция $P(z) := \binom{z-2}{q-2}$ является многочленом степени $q-2$. Она принимает целые значения для всех целых z. Целое число $P(z)$ делится на p тогда и только тогда, когда z не сравнимо с 0 или 1 по модулю q.*

■ **Доказательство.** Запишем биномиальный коэффициент в виде

$$P(z) \;=\; \binom{z-2}{q-2} \;=\; \frac{(z-2)(z-3)\cdot\ldots\cdot(z-q+1)}{(q-2)(q-3)\cdot\;\ldots\;\ldots\cdot 2\cdot 1} \qquad (*)$$

и сравним числа вхождений p как множителей в разложения знаменателя и числителя. Знаменатель имеет то же число множителей p, что и $(q-2)!$ (или что $(q-1)!$, так как $q-1$ не делится на p). Действительно, согласно утверждению на полях *все* произведение $q-1$ целых

Утверждение. *Если $a \equiv b \not\equiv 0 \pmod q$, то a и b делятся на одну и ту же степень p.*

■ **Доказательство.** По условию $a = b + sp^m$ и b не делится на $p^m = q$. Поэтому если p^k делит b, то $k < m$ и, следовательно, p^k делит также a. Утверждение симметрично по a и b. □

чисел, по одному из каждого ненулевого класса вычетов по модулю q, делятся на одну и ту же степень p.

Далее, если z сравнимо с 0 или 1 по модулю q, то числитель имеет такой же тип: все множители в произведении принадлежат различным классам вычетов, среди которых не встречаются лишь нулевой класс (числа, кратные q) и либо класс -1, либо класс $+1$. Но ни элементы класса $+1$, ни элементы класса -1 не делятся на p. Следовательно, числитель и знаменатель дроби (*) делятся на одну и ту же степень p, вследствие чего их отношение (*) не делится на p.

С другой стороны, если $z \not\equiv 0, 1 \pmod q$, то произведение в числителе дроби $(*)$ содержит один множитель, который делится на $q = p^m$, и не содержит множителей из двух соседних ненулевых классов вычетов: один из них представляет числа, которые не делятся на p, а другой — числа, которые делятся на степень p, меньшую, чем $q = p^m$. Поэтому в числителе количество множителей p больше, чем в знаменателе, и дробь (*) делится на p. □

Теперь рассмотрим произвольное подмножество $Q' \subseteq Q$, не содержащее почти ортогональных векторов. Мы хотим показать, что Q' должно быть «малым».

Утверждение 1. *Если $\boldsymbol{x}, \boldsymbol{y}$ — различные векторы из Q, то $\frac{1}{4}(\langle \boldsymbol{x}, \boldsymbol{y}\rangle + 2)$ — целое число, удовлетворяющее неравенствам*

$$-(q-2) \;\le\; \tfrac{1}{4}(\langle \boldsymbol{x}, \boldsymbol{y}\rangle + 2) \;\le\; q-1.$$

Как $\boldsymbol{x}$, так и $\boldsymbol{y}$ имеют четное число компонент, равных -1, поэтому число компонент, по которым $\boldsymbol{x}$ и $\boldsymbol{y}$ различаются, тоже четно. Следовательно, для всех $\boldsymbol{x}, \boldsymbol{y} \in Q$

$$\langle \boldsymbol{x}, \boldsymbol{y}\rangle \;=\; (4q-2) \;-\; 2\#\{i : x_i \ne y_i\} \;\equiv\; -2 \pmod 4,$$

т. е. число $\frac{1}{4}(\langle \boldsymbol{x}, \boldsymbol{y}\rangle + 2)$ целое.

Так как $\boldsymbol{x}, \boldsymbol{y} \in \{+1, -1\}^{4q-2}$, то $-(4q-2) \le \langle \boldsymbol{x}, \boldsymbol{y}\rangle \le 4q-2$, или $-(q-1) \le \frac{1}{4}(\langle \boldsymbol{x}, \boldsymbol{y}\rangle + 2) \le q$. Нижняя оценка в этих неравенствах никогда не достигается, поскольку из $x_1 = y_1 = 1$ следует $\boldsymbol{x} \ne -\boldsymbol{y}$. Верхняя оценка обращается в равенство лишь при $\boldsymbol{x} = \boldsymbol{y}$.

Утверждение 2. *Если многочлен $F_{\boldsymbol{y}}(\boldsymbol{x})$ степени $q-2$ от переменных $x_1, \ldots, x_n$ определяется равенством*

$$F_{\boldsymbol{y}}(\boldsymbol{x}) \;:=\; P\big(\tfrac{1}{4}(\langle \boldsymbol{x}, \boldsymbol{y}\rangle + 2)\big) \;=\; \binom{\frac{1}{4}(\langle \boldsymbol{x}, \boldsymbol{y}\rangle + 2) - 2}{q-2},$$

то при любом $\boldsymbol{y} \in Q'$ значение $F_{\boldsymbol{y}}(\boldsymbol{x})$ делится на p, если $\boldsymbol{x} \in Q' \backslash \{\boldsymbol{y}\}$, и не делится на p, если $\boldsymbol{x} = \boldsymbol{y}$.

Представление в виде биномиального коэффициента показывает, что многочлен $F_{\boldsymbol{y}}(\boldsymbol{x})$ принимает целые значения. Если $\boldsymbol{x} = \boldsymbol{y}$, то мы получаем значение $F_{\boldsymbol{y}}(\boldsymbol{y}) = 1$. Если же $\boldsymbol{x} \ne \boldsymbol{y}$, то из леммы следует, что $F_{\boldsymbol{y}}(\boldsymbol{x})$ не делится на p тогда и только тогда, когда число $\frac{1}{4}(\langle \boldsymbol{x}, \boldsymbol{y}\rangle + 2)$ сравнимо по модулю q с 0 или с 1. Согласно утверждению 1 это происходит лишь тогда, когда $\frac{1}{4}(\langle \boldsymbol{x}, \boldsymbol{y}\rangle + 2)$ есть либо 0, либо 1, т. е. когда $\langle \boldsymbol{x}, \boldsymbol{y}\rangle \in \{-2, +2\}$. Но для этого $\boldsymbol{x}$ и $\boldsymbol{y}$ должны быть почти ортогональны, что противоречит определению множества Q'.

Утверждение 3. *То же самое справедливо для многочленов $\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$ от $n-1$ переменных $x_2,\dots,x_n$, которые получаются при разложении $F_{\boldsymbol{y}}(\boldsymbol{x})$ в сумму одночленов, удалении из них переменной x_1 и понижении степени других переменных, т. е. при заменах $x_1=1$ и $x_i^2=1$ для $i>1$. Степени многочленов $\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$ не выше $q-2$.*

Все векторы $\boldsymbol{x}\in Q\subseteq\{+1,-1\}^n$ удовлетворяют условиям $x_1=1$ и $x_i^2=1$. Следовательно, замены не изменяют значения многочленов на множестве Q. Они также не увеличивают степень, и поэтому степени многочленов $\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$ не превосходят $q-2$.

Утверждение 4. *Не существует линейных соотношений (с рациональными коэффициентами), которые связывают многочлены $\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$, т. е. многочлены $\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$, $\boldsymbol{y}\in Q'$, линейно независимы над полем $\mathbb{Q}$. В частности, они различны.*

Допустим, что существует соотношение вида $\sum_{\boldsymbol{y}\in Q'}\alpha_{\boldsymbol{y}}\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})=0$, в котором коэффициенты $\alpha_{\boldsymbol{y}}$ рациональны и не все равны нулю. Умножая это равенство на подходящий скаляр, можно сделать все коэффициенты целыми числами, не все из которых делятся на p. Но тогда для каждого $\boldsymbol{y}\in Q'$, полагая $\boldsymbol{x}:=\boldsymbol{y}$ и учитывая утверждение 2, находим что $\alpha_{\boldsymbol{y}}\overline{F}_{\boldsymbol{y}}(\boldsymbol{y})$ делится на p, и поэтому $\alpha_{\boldsymbol{y}}$ делится на p (так как $\overline{F}_{\boldsymbol{y}}(\boldsymbol{y})$ на p не делится).

Утверждение 5. *Величина $|Q'|$ ограничена сверху числом не содержащих квадратов одночленов степени не выше $q-2$ от $n-1$ переменных, а их число равно $\sum_{i=0}^{q-2}\binom{n-1}{i}$.*

По построению многочлены $\overline{F}_{\boldsymbol{y}}$ свободны от квадратов: ни один из составляющих их одночленов не содержит переменных в степени выше 1. Поэтому каждый из многочленов $\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$ есть линейная комбинация свободных от квадратов одночленов степени не выше $q-2$ от $n-1$ переменных $x_2,\dots,x_n$. Так как многочлены $\overline{F}_{\boldsymbol{y}}(\boldsymbol{x})$ линейно независимы, то их число (равное $|Q'|$) не может быть больше числа таких одночленов.

Детализация шага (2). Первый столбец матрицы $\boldsymbol{x}\boldsymbol{x}^T$ есть $\boldsymbol{x}$. Поэтому для различных $\boldsymbol{x}\in Q$ мы получаем различные матрицы $M(\boldsymbol{x}):=\boldsymbol{x}\boldsymbol{x}^T$. Интерпретируем эти матрицы как векторы размерности n^2 с компонентами x_ix_j. Простое вычисление

$$\begin{aligned}\big\langle M(\boldsymbol{x}),M(\boldsymbol{y})\big\rangle &= \sum_{i=1}^{n}\sum_{j=1}^{n}(x_ix_j)(y_iy_j)\\ &= \Big(\sum_{i=1}^{n}x_iy_i\Big)\Big(\sum_{j=1}^{n}x_jy_j\Big) \;=\; \langle\boldsymbol{x},\boldsymbol{y}\rangle^2 \;\geq\; 4\end{aligned}$$

показывает, что скалярное произведение векторов $M(\boldsymbol{x})$ и $M(\boldsymbol{y})$ минимально тогда и только тогда, когда $\boldsymbol{x},\boldsymbol{y}\in Q$ почти ортогональны.

Детализация шага (3). Пусть $U(\boldsymbol{x})\in\{+1,-1\}^d$ — вектор, составленный из всех элементов матрицы $M(\boldsymbol{x})$, которые лежат ниже ее главной диагонали. Учитывая симметричность матрицы $M(\boldsymbol{x})=\boldsymbol{x}\boldsymbol{x}^T$ и то, что

$$M(\boldsymbol{x}) \;=\; \begin{pmatrix} 1 & & & U(\boldsymbol{x}) \\ & 1 & & \\ & & \ddots & \\ U(\boldsymbol{x}) & & & 1 \end{pmatrix}$$

ее элементы на главной диагонали равны $+1$, мы видим,что из условия $M(\boldsymbol{x}) \neq M(\boldsymbol{y})$ следует $U(\boldsymbol{x}) \neq U(\boldsymbol{y})$. Более того,

$$4 \;\le\; \langle M(\boldsymbol{x}), M(\boldsymbol{y})\rangle \;=\; 2\langle U(\boldsymbol{x}), U(\boldsymbol{y})\rangle + n,$$

т. е.

$$\langle U(\boldsymbol{x}), U(\boldsymbol{y})\rangle \;\ge\; -\frac{n}{2} + 2,$$

и равенство достигается тогда и только тогда, когда $\boldsymbol{x}$ и $\boldsymbol{y}$ почти ортогональны. В силу того, что все векторы $U(\boldsymbol{x}) \in S$ имеют одну и ту же длину $\sqrt{\langle U(\boldsymbol{x}), U(\boldsymbol{x})\rangle} = \sqrt{\binom{n}{2}}$, это означает, что максимальное расстояние между точками $U(\boldsymbol{x}), U(\boldsymbol{y}) \in S$ достигается как раз тогда, когда $\boldsymbol{x}$ и $\boldsymbol{y}$ почти ортогональны.

Детализация шага (4). Если $q = 9$, то $g(9) \approx 758.31$, что больше $d + 1 = \binom{34}{2} + 1 = 562$.

Чтобы вывести общую оценку для больших d, воспользуемся монотонностью и унимодальностью биномиальных коэффициентов, а также оценками $n! > e(\frac{n}{e})^n$ и $n! < en(\frac{n}{e})^n$ (см. приложение к гл. 2):

$$\sum_{i=0}^{q-2}\binom{4q-3}{i} < q\binom{4q}{q} = q\,\frac{(4q)!}{q!(3q)!} < q\,\frac{e\,4q\left(\frac{4q}{e}\right)^{4q}}{e\left(\frac{q}{e}\right)^{q} e\left(\frac{3q}{e}\right)^{3q}} = \frac{4q^2}{e}\Big(\frac{256}{27}\Big)^q.$$

Таким образом,

$$f(d) \;\ge\; g(q) \;=\; \frac{2^{4q-4}}{\sum\limits_{i=0}^{q-2}\binom{4q-3}{i}} \;>\; \frac{e}{64q^2}\Big(\frac{27}{16}\Big)^q.$$

Отсюда, учитывая неравенства

$$d \;=\; (2q-1)(4q-3) \;=\; 5q^2 + (q-3)(3q-1) \;\ge\; 5q^2 \quad \text{при } q \ge 3,$$

$$q = \tfrac{5}{8} + \sqrt{\tfrac{d}{8} + \tfrac{1}{64}} > \sqrt{\tfrac{d}{8}} \qquad \text{и} \qquad \big(\tfrac{27}{16}\big)^{\sqrt{\frac{1}{8}}} > 1.2032,$$

получаем, что для всех достаточно больших d

$$f(d) \;>\; \frac{e}{13d}(1.2032)^{\sqrt{d}} \;>\; (1.2)^{\sqrt{d}}. \qquad \square$$

Контрпример для размерности 560 получается, если заметить, что при $q = 9$ отношение $g(q) \approx 758$ *значительно* больше размерности $d(q) = 561$. Поэтому контрпример для $d = 560$ можно построить, используя лишь «три четверти» точек в S, удовлетворяющих условию $x_{21} + x_{31} + x_{32} = -1$.

Известно, что гипотеза Борсука верна для $d \le 3$, но она не была подтверждена ни для одного большего измерения. С другой стороны, она верна для $d \le 8$, если ограничиваться рассмотренными выше подмножествами $S \subseteq \{1, -1\}^d$ (см. [8]). Во всяком случае, вполне вероятно, что можно найти контрпримеры и для довольно малых размерностей.

Литература

[1] Borsuk K. *Drei Sätze über die n-dimensionale euklidische Sphäre.* Fundamenta Math., **20** (1933), 177–190.

[2] Hinrichs A., Richter C. *New sets with large Borsuk numbers.* Discrete Math., **270** (2003), 136–146.

[3] Kahn J., Kalai G. *A counterexample to Borsuk's conjecture.* Bulletin Amer. Math. Soc., **29** (1993), 60–62.

[4] Nilli A. *On Borsuk's problem.* В сб. «Jerusalem Combinatorics '93» (Barcelo H., Kalai G., eds.), Contemporary Mathematics, **178**, Amer. Math. Soc. 1994, 209–210.

[5] Райгородский А. М. *О размерности в проблеме Борсука.* Успехи матем. наук, **52** (1997), вып. 6, с. 181–182.

[6] Schramm O. *Illuminating sets of constant width.* Mathematika, **35** (1988), 180–199.

[7] Weissbach B. *Sets with large Borsuk number.* Beiträge zur Algebra und Geometrie/Contributions to Algebra and Geometry, **41** (2000), 417–423.

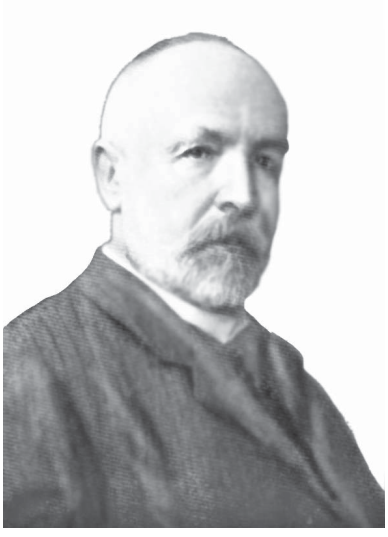
[8] Ziegler G. M. *Coloring Hamming graphs, optimal binary codes, and the 0/1-Borsuk problem in low dimensions.* Lecture Notes in Computer Science, **2122**, Springer-Verlag 2001, 164–175.

[9*] Грюнбаум Б. *Этюды по комбинаторной геометрии и теории выпуклых тел.* — М.: Наука, 1971.

Математический анализ

«Приморский курортный отель Гильберта»

Глава 17 Множества, функции и гипотеза континуума



Георг Кантор

Теория множеств, основанная во второй половине XIX столетия Георгом Кантором, полностью преобразовала математику. Математика в современную эпоху немыслима без понятия множества; по этому поводу Давид Гильберт сказал: «Никто не выгонит нас из рая (теории множеств), который создал для нас Кантор».

Одной из основных идей Кантора было понятие *объема* или *мощности* $|M|$ множества M. Для конечных множеств его определение очевидно: мы просто подсчитываем число элементов и говорим, что M является n-множеством (или имеет объем n), если M содержит ровно n элементов. Таким образом, два конечных множества M и N имеют равный объем, если они содержат одинаковое число элементов.

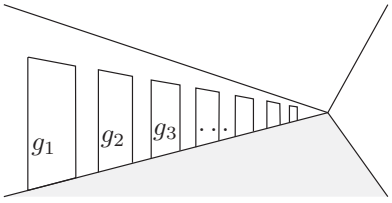
Чтобы перенести понятие равного объема на бесконечные множества, воспользуемся поясняющим экспериментом для конечных множеств. Предположим, что толпа людей садится в автобус. Как проверить, что число пассажиров *равно* числу посадочных мест? Очень просто: позволим пассажирам занять их места. Два множества (пассажиров и мест) имеют одинаковые объемы тогда и только тогда, когда каждый пассажир найдет место и ни одно посадочное место не окажется пустым. Другими словами, объемы двух множеств одинаковы, если существует *биекция* одного множества в другое.

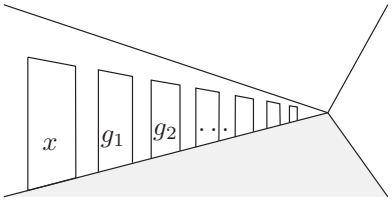
Теперь дадим общее определение: два произвольных множества M и N (конечных или бесконечных) имеют *равный объем* или *равную мощность* тогда и только тогда, когда существует биекция из M в N. Ясно, что понятие равного объема есть отношение эквивалентности, и поэтому можно сопоставить каждому классу множеств равного объема «число», называемое *кардинальным числом* (или *кардиналом*). Например, конечным множествам сопоставляются кардинальные числа $0, 1, 2, \ldots, n, \ldots$: n соответствует классу n-множеств, в частности, 0 — *пустому множеству* $\varnothing$. Отметим очевидный факт: объем собственного подмножества конечного множества M всегда меньше объема множества M.

Теория становится очень интересной (и противоречащей интуиции) при переходе к бесконечным множествам. Пусть $\mathbb{N} = \{1, 2, 3, \ldots\}$ — множество натуральных чисел. Назовем множество M *счетным*, если существует взаимно однозначное соответствие между M и $\mathbb{N}$. Иначе говоря, M счетно, если можно составить список элементов M в виде $m_1, m_2, m_3, \ldots$ Однако имеет место странное явление. Если добавить к $\mathbb{N}$ новый элемент x, то $\mathbb{N} \cup \{x\}$ тоже будет счетным и, следовательно, будет иметь равный с $\mathbb{N}$ объем!

Красивой иллюстрацией этого эффекта является «отель Гильберта». Предположим, что отель имеет счетное множество комнат с номерами $1, 2, 3, \ldots$ и что все они заселены. В комнате i живет постоялец g_i. Прибывает новый гость x и просит устроить его, на что управляющий говорит: «Извините, все комнаты заняты». «Нет проблем, — возража-

ет вновь прибывший, — переселите постояльца g_1 в комнату 2, g_2 — в комнату 3, g_3 — в комнату 4, и т. д., а я тогда смогу занять комнату 1». К удивлению управляющего (он не математик) эти действия дают результат: он может оставить всех постояльцев отеля и еще дополнительно разместить вновь прибывшего гостя x!





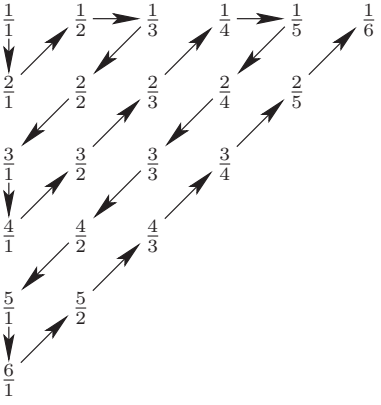
Теперь ясно, что он может также принять другого гостя y, и еще одного постояльца z, и т. д. В частности, заметим, что (в отличие от конечных множеств) собственное подмножество *бесконечного* множества M может иметь тот же самый объем, что и M. В действительности это свойство — характеризация бесконечности: множество бесконечно тогда и только тогда, когда оно имеет тот же объем, что некоторое его собственное подмножество.

Покинем отель Гильберта и вернемся к множествам чисел. Множество $\mathbb{Z}$ целых чисел счетно, так как его можно представить в виде $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$. Удивительно, что все рациональные числа тоже можно включить в одну последовательность.

Теорема 1. *Множество $\mathbb{Q}$ рациональных чисел счетно.*

■ **Доказательство.** Множество $\mathbb{Q}^+$ положительных рациональных чисел счетно, так как его можно перечислить указанным на полях способом (пропуская уже встретившиеся числа). Поэтому $\mathbb{Q}$ счетно (достаточно записать 0 в начале строки и после $\frac{p}{q}$ добавлять $-\frac{p}{q}$). Таким образом,

$$\mathbb{Q} \;=\; \{0, 1, -1, 2, -2, \tfrac{1}{2}, -\tfrac{1}{2}, \tfrac{1}{3}, -\tfrac{1}{3}, 3, -3, 4, -4, \tfrac{3}{2}, -\tfrac{3}{2}, \ldots\}.$$



Указанная на полях схема приводит также к следующему утверждению.

Объединение счетного множества счетных множеств M_n счетно.

В самом деле, по множествам $M_n = \{a_{n1}, a_{n2}, a_{n3}, \ldots\}$, $n = 1, 2, \ldots$, точно так же, как и выше, можно составить строку

$$\bigcup_{n=1}^{\infty} M_n \;=\; \{a_{11}, a_{21}, a_{12}, a_{13}, a_{22}, a_{31}, a_{41}, a_{32}, a_{23}, a_{14}, \ldots\}.$$

Поразмышляем еще немного о канторовской нумерации положительных рациональных чисел. Рисунку на полях соответствует строка

$$\tfrac{1}{1},\ \tfrac{2}{1},\ \tfrac{1}{2},\ \tfrac{1}{3},\ \tfrac{2}{2},\ \tfrac{3}{1},\ \tfrac{4}{1},\ \tfrac{3}{2},\ \tfrac{2}{3},\ \tfrac{1}{4},\ \tfrac{1}{5},\ \tfrac{2}{4},\ \tfrac{3}{3},\ \tfrac{4}{2},\ \tfrac{5}{1},\ \ldots,$$

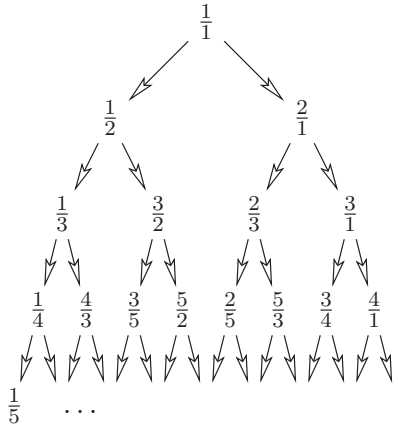
и из нее нужно лишь удалить повторения типа $\frac{2}{2} = \frac{1}{1}$ или $\frac{2}{4} = \frac{1}{2}$.

Однако недавно Нейл Калкин и Герберт Вилф [2] нашли более изящный и регулярный способ построения списка положительных рациональных чисел без повторений, начинающийся так:

$$\tfrac{1}{1},\ \tfrac{1}{2},\ \tfrac{2}{1},\ \tfrac{1}{3},\ \tfrac{3}{2},\ \tfrac{2}{3},\ \tfrac{3}{1},\ \tfrac{1}{4},\ \tfrac{4}{3},\ \tfrac{3}{5},\ \tfrac{5}{2},\ \tfrac{2}{5},\ \tfrac{5}{3},\ \tfrac{3}{4},\ \tfrac{4}{1},\ \ldots$$

Здесь знаменатель n-го рационального числа при любом n равен числителю $(n+1)$-го числа. Иначе говоря, n-я дробь равна $b(n)/b(n+1)$, где $\big(b(n)\big)_{n\ge 0}$ — последовательность, начинающаяся так:

$$(1,\ 1,\ 2,\ 1,\ 3,\ 2,\ 3,\ 1,\ 4,\ 3,\ 5,\ 2,\ 5,\ 3,\ 4,\ 1,\ 5,\ \ldots).$$



Впервые ее изучал немецкий математик Морис Абрахам Штерн в статье 1858 года [7], и ее называют *двухатомным рядом Штерна*. Как построить ее и тем самым список Калкина – Вилфа положительных дробей? Рассмотрим изображенное на полях бесконечное двоичное дерево, в вершинах которого стоят рациональные числа. Оно строится по рекурсивному правилу:

- $\frac{1}{1}$ находится в верхушке дерева,
- каждая вершина $\frac{i}{j}$ имеет двух потомков: левого $\frac{i}{i+j}$ и правого $\frac{i+j}{j}$.

Несложно проверить следующие четыре свойства:

(1) Все дроби в дереве несократимы, т. е. если в нем появляется дробь $\frac{r}{s}$, то r и s взаимно просты.

Это верно для верхушки $\frac{1}{1}$, а далее мы используем индукцию. Если r и s взаимно просты, то взаимно просты r и $r+s$, а также s и $r+s$.

(2) Каждая несократимая дробь $\frac{r}{s} > 0$ появляется в дереве.

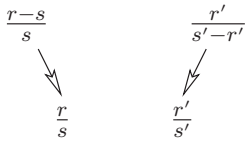
Используем индукцию по величине суммы $r+s$. Наименьшее ее значение $r+s=2$ имеет дробь $\frac{r}{s}=\frac{1}{1}$ в верхушке дерева. Если $r>s$, то по предположению индукции в дереве есть дробь $\frac{r-s}{s}$, и $\frac{r}{s}$ — ее правый потомок. Аналогично, если $r<s$, то в дереве есть дробь $\frac{r}{s-r}$, и $\frac{r}{s}$ — ее левый потомок.

(3) Каждая несократимая дробь появляется ровно один раз.

Рассуждаем аналогично. Если дробь $\frac{r}{s}$ появляется больше одного раза, то $r \neq s$, поскольку в каждой вершине дерева, кроме его верхушки, стоит либо $\frac{i}{i+j}<1$, либо $\frac{i+j}{j}>1$. В каждом из случаев $r>s$ или $r<s$ можно, как и ранее, воспользоваться индукцией.

Таким образом, каждое положительное рациональное число появляется в дереве ровно один раз, и все их можно выписывать, проходя по каждому слою слева направо. При этом получится приведенный ранее начальный фрагмент.

(4) Знаменатель n-й дроби в списке равен числителю $(n+1)$-й дроби.



Это верно при $n=0$ и в случае, когда n-я дробь — левый потомок. Пусть n-я дробь $\frac{r}{s}$ — правый потомок. Если $\frac{r}{s}$ лежит на правой границе, то $s=1$, а следующая дробь лежит на левой границе и имеет числитель 1. Наконец, если $\frac{r}{s}$ лежит внутри дерева и $\frac{r'}{s'}$ — следующая дробь, то $\frac{r}{s}$ — правый потомок $\frac{r-s}{s}$, а $\frac{r'}{s'}$ — левый потомок $\frac{r'}{s'-r'}$. По индукции знаменатель $\frac{r-s}{s}$ есть числитель дроби $\frac{r'}{s'-r'}$, так что $s=r'$.

Все это хорошо, но нас ждет нечто большее. Возникают два вопроса:

– Есть ли «смысл» у последовательности $\big(b(n)\big)_{n\geq 0}$? Иначе говоря, описывает ли она что-нибудь простое?

– Существует ли простой способ по заданной дроби $\frac{r}{s}$ найти следующую за ней в списке?

Чтобы ответить на первый вопрос, заметим, что у вершины $b(n)/b(n+1)$ есть два потомка $b(2n+1)/b(2n+2)$ и $b(2n+2)/b(2n+3)$. Из правил построения дерева следуют рекуррентные формулы

$$b(2n+1) = b(n) \quad \text{и} \quad b(2n+2) = b(n) + b(n+1). \tag{1}$$

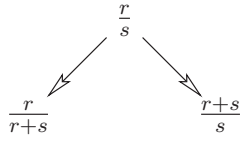
Начальное условие $b(0) = 1$ и равенства (1) полностью определяют последовательность $(b(n))_{n\geq 0}$.

А есть ли «красивая» «известная» последовательность, удовлетворяющая этим формулам? Да, есть. Каждое число n единственным образом записывается в виде суммы разных степеней 2 — это обычное двоичное представление n. *Гипердвоичное* представление n — это представление n в виде суммы степеней 2, в котором каждая степень 2^k появляется *не более двух раз*. Пусть $h(n)$ — число таких представлений n. Проверьте, что последовательность $h(n)$ удовлетворяет соотношениям (1), и поэтому $b(n) = h(n)$ для всех n.

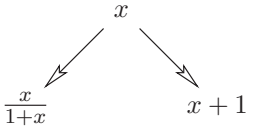
Например, $h(6) = 3$ и есть три гипердвоичных представления
$6 = 4 + 2$
$6 = 4 + 1 + 1$
$6 = 2 + 2 + 1 + 1$.

Заодно доказан удивительный факт: если дробь $\frac{r}{s}$ несократима, то существует ровно одно такое целое число n, что $r = h(n)$ и $s = h(n+1)$.

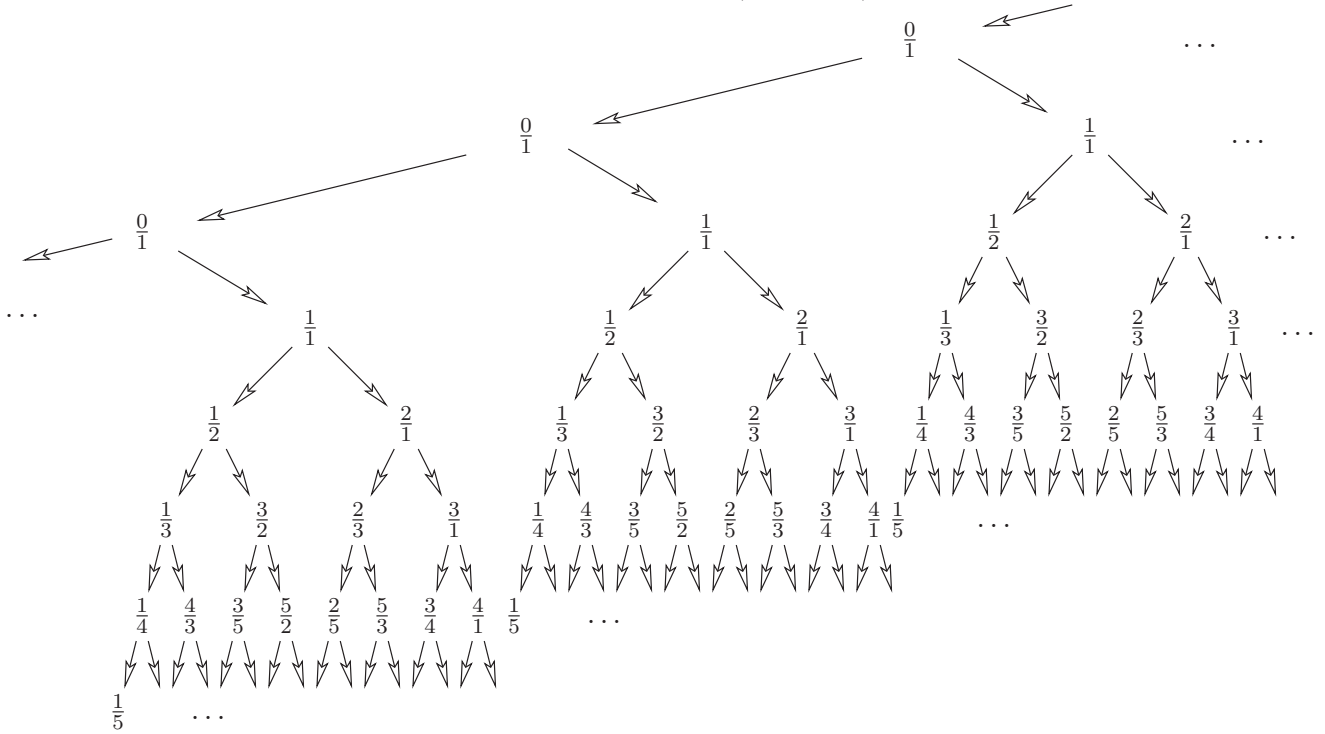
Займемся теперь вторым вопросом. Ветвление в дереве имеет вид



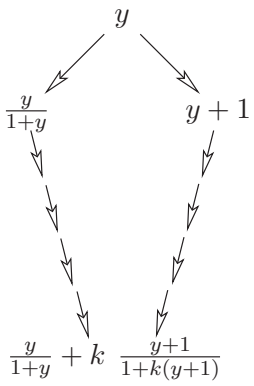
или, при $x := \frac{r}{s}$,



Используя его, построим бесконечное двоичное дерево (без корня):



В этом дереве все строки одинаковы, и каждая представляет собой список Калкина – Вилфа положительных дробей (начинающийся с дополнительной дроби $\frac{0}{1}$).



И как же переходить от одного рационального числа к следующему? Чтобы найти ответ, заметим прежде всего, что для любого рационального x его правым потомком является $x+1$, правым внуком $x+2$, и поэтому $x+k$ — самый правый потомок в k-м поколении. Аналогично, левым потомком x является $\frac{x}{1+x}$, его левым потомком — дробь $\frac{x}{1+2x}$, и т. д.: самый левый потомок x в k-м поколении — это $\frac{x}{1+kx}$.

Теперь, чтобы найти правило перехода от $\frac{r}{s}=x$ к «следующему» рациональному числу $f(x)$ в списке, рассмотрим изображенную на полях ситуацию. В бесконечном двоичном дереве для чисел x и $f(x)$ (соседей в одной строке) существует их «ближайший общий предок» y, так что x является (при некотором $k\ge 0$) самым правым потомком в k-м поколении левого потомка $y\ge 0$, а $f(x)$ — самым левым потомком в k-м поколении правого потомка y. Используя формулы для самого правого и самого левого потомков в k-м поколении, получаем

$$x \;=\; \frac{y}{1+y}+k,$$

как показано на рисунке на полях. Здесь $k=\lfloor x\rfloor$ — целая часть x, а $\frac{y}{1+y}=\{x\}$ — его дробная часть. Отсюда следует, что

$$f(x)=\frac{y+1}{1+k(y+1)}=\frac{1}{\frac{1}{y+1}+k}=\frac{1}{k+1-\frac{y}{y+1}}=\frac{1}{\lfloor x\rfloor+1-\{x\}}\,.$$

Тем самым мы получили замечательную формулу для числа $f(x)$, следующего за x, найденную недавно Моше Ньюманом:

Функция

$$x \;\longmapsto\; f(x) \;=\; \frac{1}{\lfloor x\rfloor+1-\{x\}}$$

порождает последовательность Калкина – Вилфа

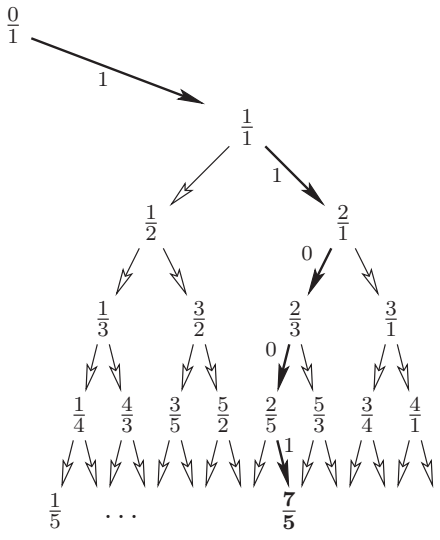
$$\tfrac{1}{1}\;\mapsto\;\tfrac{1}{2}\;\mapsto\;\tfrac{2}{1}\;\mapsto\;\tfrac{1}{3}\;\mapsto\;\tfrac{3}{2}\;\mapsto\;\tfrac{2}{3}\;\mapsto\;\tfrac{3}{1}\;\mapsto\;\tfrac{1}{4}\;\mapsto\;\tfrac{4}{3}\;\mapsto\;\ldots,$$

содержащую каждое положительное рациональное число ровно один раз.

Способ Калкина – Вилфа – Ньюмана нумерации положительных рациональных чисел имеет еще много других замечательных свойств. Например, можно спросить, существует ли быстрый способ нахождения n-й дроби в этом списке, скажем, для $n=10^6$. Такой способ есть:

Чтобы найти n-ю дробь в последовательности Калкина – Вилфа, нужно записать n в двоичной системе счисления: $n=(b_kb_{k-1}\ldots b_1b_0)_2$, и затем пройти в дереве Калкина – Вилфа по пути, заданному его разрядами, начиная с $\frac{s}{t}=\frac{0}{1}$. При $b_i=1$ нужно «переходить к правому потомку» (прибавлять знаменатель к числителю), а при $b_i=0$ «переходить к левому потомку» (прибавлять числитель к знаменателю).

Рисунок на полях показывает получающийся путь для $n = 25 = (11001)_2$: в последовательности Калкина – Вилфа 25-е число равно $\frac{7}{5}$. Читатель может легко построить схему вычисления по заданной дроби $\frac{s}{t}$ (двоичного представления) ее номера n в последовательности Калкина – Вилфа.



Теперь рассмотрим множество действительных чисел $\mathbb{R}$. Оно тоже счетно? Нет, это не так, и способ доказательства — *диагональный метод* Кантора — не только имеет фундаментальное значение для всей теории множеств, но, несомненно, принадлежит Книге как редкое проявление гениальности.

Теорема 2. *Множество $\mathbb{R}$ действительных чисел несчетно.*

■ **Доказательство.** Любое подмножество N счетного множества $M = \{m_1, m_2, m_3, \ldots\}$ *не более чем счетно* (т. е. конечно или счетно), потому что элементы подмножества N можно выписать в порядке их появления в M. Поэтому если существует несчетное подмножество $\mathbb{R}$, то $\mathbb{R}$ не может быть счетным. В качестве подмножества M множества $\mathbb{R}$ рассмотрим интервал $(0, 1]$ всех таких положительных действительных чисел r, что $0 < r \leq 1$. Предположим противное: M счетно; пусть $M = \{r_1, r_2, r_3, \ldots\}$ — строка, перечисляющая элементы множества M. Запишем каждое число r_n в виде его единственного *бесконечного* десятичного разложения без бесконечной последовательности нулей в конце:

$$r_n = 0, a_{n1}a_{n2}a_{n3}...,$$

где $a_{ni} \in \{0, 1, \ldots, 9\}$ для всех n и i. Например, $0.7 = 0.6999...$

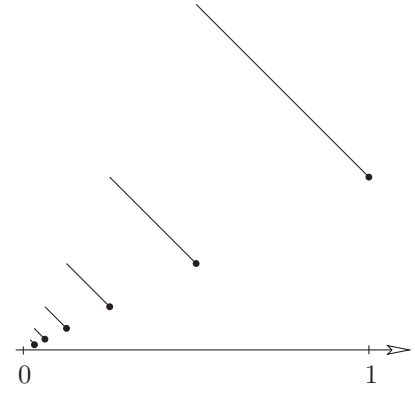
Рассмотрим теперь двойную бесконечную таблицу

$$\begin{array}{rcl} r_1 & = & 0, a_{11}a_{12}a_{13}... \\ r_2 & = & 0, a_{21}a_{22}a_{23}... \\ \vdots & & \vdots \\ r_n & = & 0, a_{n1}a_{n2}a_{n3}... \\ \vdots & & \vdots \end{array}$$

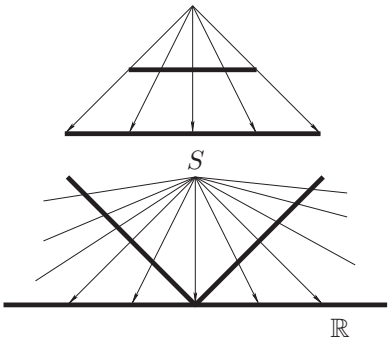
Для каждого n выберем число $b_n \in \{1, 2\}$, отличное от a_{nn}. Тогда $b = 0, b_1b_2b_3...b_n...$ — действительное число из нашего множества M и, следовательно, должно совпадать с одним из его элементов, скажем $b = r_k$. Но это невозможно, так как b_k отлично от a_{kk}. Вот и все доказательство! □

Поговорим еще немного о действительных числах. Заметим, что все четыре типа интервалов — $(0, 1), (0, 1], [0, 1)$ и $[0, 1]$ — имеют один и тот же объем. Проверим, например, что $(0, 1]$ и $(0, 1)$ имеют одинаковую мощность. Достаточно рассмотреть отображение $f : (0, 1] \longrightarrow (0, 1)$, определяемое равенствами

$$f(x) := \begin{cases} \frac{3}{2} - x & \text{при} \quad \frac{1}{2} < x \leq 1, \\ \frac{3}{4} - x & \text{при} \quad \frac{1}{4} < x \leq \frac{1}{2}, \\ \frac{3}{8} - x & \text{при} \quad \frac{1}{8} < x \leq \frac{1}{4}, \\ \quad \vdots & \end{cases}$$



$f : (0, 1] \longrightarrow (0, 1)$



Действительно, оно биективно, так как область изменения y в первой строке есть полуинтервал $\left[\frac{1}{2}, 1\right)$, во второй строке — $\left[\frac{1}{4}, \frac{1}{2}\right)$, в третьей строке — $\left[\frac{1}{8}, \frac{1}{4}\right)$, и т. д.

Далее, рассматривая указанную на полях центральную проекцию, мы находим, что *любые* два интервала (конечной положительной длины) имеют одинаковый объем. Верно даже более сильное утверждение: каждый интервал положительной длины имеет тот же объем, что и вся действительная прямая $\mathbb{R}$. Чтобы убедиться в этом, рассмотрим изломанный открытый интервал $(0, 1)$ и проекцию его на $\mathbb{R}$ из центра S (см.чертеж на полях).

Подведем итог: все открытые, полуоткрытые (конечные или бесконечные) интервалы положительной длины имеют один и тот же объем; обозначим этот объем буквой c, где c — обозначение *континуума*[1] (иногда так называют множество точек интервала [0,1]).

То, что конечные и бесконечные интервалы имеют один и тот же объем, можно было предвидеть, но следующее утверждение явно противоречит интуиции[2].

Теорема 3. *Множество $\mathbb{R}^2$ всех упорядоченных пар действительных чисел (вещественная плоскость) имеет такой же объем, что и $\mathbb{R}$.*

Эту теорему доказал Кантор в 1878 году [3]; ему же принадлежит идея объединения десятичных разложений двух действительных чисел в одно. Вариант метода Кантора, который мы собираемся изложить, тоже достоин Книги. Абрахам Френкель приписывает трюк, непосредственно порождающий биекцию, Юлиусу Кёнигу.

■ **Доказательство.** Достаточно доказать, что множество всех пар (x, y), $0 < x, y \leq 1$, можно биективно отобразить на $(0, 1]$. Рассмотрим пару (x, y) и запишем x и y в виде их единственных десятичных разложений, не заканчивающихся бесконечной последовательностью нулей, как в следующем примере:

$$\begin{array}{rcrrrrrl} x & = & 0,3 & 01 & 2 & 007 & 08 & \ldots \\ y & = & 0,009 & 2 & 05 & 1 & 0008 & \ldots \end{array}$$

Заметим, что мы разделили цифры разложений x и y на группы, которые всегда оканчиваются первым ненулевым знаком. Далее, поставим в соответствие паре (x, y) число $z \in (0, 1]$, записав первую x-группу, потом первую y-группу, затем вторую x-группу, и т. д. В нашем примере мы получим

$$z = 0,3\ 009\ 01\ 2\ 2\ 05\ 007\ 1\ 08\ 0008\ \ldots$$

Так как разложения x и y не заканчиваются бесконечными последовательностями нулей, то выражение для z является десятичным разложением такого же вида.

Обратно, из выражения для z можно немедленно получить его прообраз (x, y), так что отображение биективно. Доказательство закончено. □

[1] «c» — первая буква латинского слова continuum (непрерывный). — *Прим. перев.*

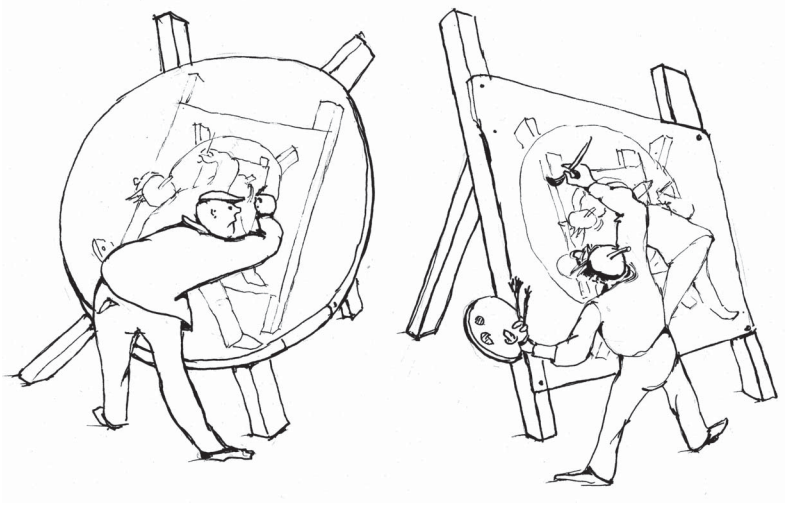
[2] Хотя оно и похоже на теорему о том, что $\mathbb{Q}^2$ (содержащееся в $\mathbb{R}^2$) счетно! — *Прим. ред.*

Учитывая, что $(x, y) \longmapsto x + iy$ есть биекция из $\mathbb{R}^2$ в множество комплексных чисел $\mathbb{C}$, мы заключаем, что $|\mathbb{C}| = |\mathbb{R}| = c$. Почему равенство $|\mathbb{R}^2| = |\mathbb{R}|$ является таким неожиданным? Да потому, что оно противоречит нашим представлениям о *размерности*. Равенство означает, что 2-мерную плоскость $\mathbb{R}^2$ (и, вообще, в силу индукции, n-мерное пространство $\mathbb{R}^n$) можно биективно отобразить в 1-мерную прямую $\mathbb{R}$. Следовательно, в общем случае размерность при биективных отображениях не сохраняется. Если, однако, потребовать, чтобы отображение и его обращение были непрерывными, то размерность будет сохраняться; это впервые доказал Лёйтзен Брауэр [1].

Пойдем немного дальше. Пока что мы определили понятие равного объема. Когда можно сказать, что объем множества M не больше объема множества N? Ключ к ответу снова дают отображения. Будем говорить, что кардинальное число $\mathfrak{m}$ *меньше или равно* $\mathfrak{n}$, если для множеств M и N с $|M| = \mathfrak{m}$, $|N| = \mathfrak{n}$ существует *инъекция* из M в N. Ясно, что соотношение $\mathfrak{m} \leq \mathfrak{n}$ не зависит от выбора представлений множеств M и N. Для конечных множеств это снова соответствует нашему интуитивному понятию: объем m-множества не больше объема n-множества тогда и только тогда, когда $m \leq n$.

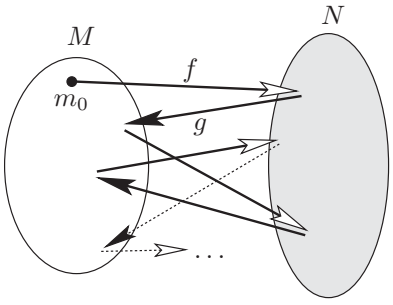
Теперь перед нами встает основная проблема. Конечно, хотелось бы, чтобы обычные правила, относящиеся к неравенствам, были справедливы для кардинальных чисел. Но верны ли они для бесконечных кардиналов? В частности, верно ли что из $\mathfrak{m} \leq \mathfrak{n}$, $\mathfrak{n} \leq \mathfrak{m}$ следует $\mathfrak{m} = \mathfrak{n}$?

Утвердительный ответ дается известной теоремой Кантора – Бернштейна. Кантор сформулировал ее в 1883 году, а первое полное доказательство привел Феликс Бернштейн на семинаре Кантора в 1897 году. Позднее доказательства предлагали Рихард Дедекинд, Эрнст Цермело и другие. Наше доказательство принадлежит Юлиусу Кёнигу (1906).



«Рисование Кантора и Бернштейна»

Теорема 4. *Если каждое из двух множеств M и N можно инъективно отобразить в другое, то существует биекция из M в N, т. е. $|M| = |N|$.*



■ **Доказательство.** Не ограничивая общности, мы можем предполагать, что M и N не пересекаются: в противном случае можно заменить множество N его копией.

Отображения f и g переводят элементы множества M в элементы множества N и обратно. Один из способов сделать эту потенциально запутанную ситуацию совершенно ясной и упорядоченной состоит в построении цепочек элементов множества $M \cup N$. Выберем произвольный элемент $m_0 \in M$ и, начиная с него, построим цепочку элементов, применяя f, затем g, затем снова f, затем g и т. д. Цепочка может либо замкнуться (это случай 1), если этот процесс приведет нас обратно в m_0, либо продолжаться без повторений бесконечно. (Первый «повторяющийся» элемент цепи не может отличаться от m_0 в силу инъективности.)

Если цепочка продолжается бесконечно, то мы можем попытаться пойти в обратном направлении: от m_0 к $g^{-1}(m_0)$, если m_0 лежит в образе g, затем к $f^{-1}(g^{-1}(m_0))$, если $g^{-1}(m_0)$ лежит в образе f, и т. д. При этом могут возникнуть три случая. Процесс движения по цепочке в обратном направлении может продолжаться бесконечно (случай 2), он может остановиться на элементе M, не лежащем в образе g (случай 3) или на элементе N, не лежащем в образе f (случай 4).

Тогда $M \cup N$ расщепляется на цепочки четырех типов, элементы которых мы можем обозначить так, что биекция будет задаваться соотношением $F : m_i \longmapsto n_i$. Проверим это для каждого случая отдельно:

Случай 1. Конечные циклы из $2k+2$ различных элементов ($k \geq 0$):

$$m_0 \xrightarrow{f} n_0 \xrightarrow{g} m_1 \xrightarrow{f} \cdots \xrightarrow{f} m_k \xrightarrow{f} n_k \xrightarrow{g} m_0$$

Случай 2. Бесконечные в обе стороны цепочки различных элементов:

$$\cdots \longrightarrow m_0 \xrightarrow{f} n_0 \xrightarrow{g} m_1 \xrightarrow{f} n_1 \xrightarrow{g} m_2 \xrightarrow{f} \cdots$$

Случай 3. Бесконечные в одну сторону цепочки различных элементов, начинающиеся с элементов $m_0 \in M \backslash g(N)$:

$$m_0 \xrightarrow{f} n_0 \xrightarrow{g} m_1 \xrightarrow{f} n_1 \xrightarrow{g} m_2 \xrightarrow{f} \cdots$$

Случай 4. Бесконечные в одну сторону цепочки различных элементов, начинающиеся с элементов $n_0 \in N \backslash f(M)$:

$$n_0 \xrightarrow{g} m_0 \xrightarrow{f} n_1 \xrightarrow{g} m_1 \xrightarrow{f} \cdots \qquad \square$$

Что можно сказать о других свойствах отношения порядка, описываемых неравенствами? Как обычно, мы полагаем $\mathfrak{m} < \mathfrak{n}$, если $\mathfrak{m} \leq \mathfrak{n}$, но $\mathfrak{m} \neq \mathfrak{n}$. Мы только что установили, что для любых кардиналов $\mathfrak{m}$ и $\mathfrak{n}$ справедлива не более чем одна из трех возможностей:

$$\mathfrak{m} < \mathfrak{n},\ \mathfrak{m} = \mathfrak{n},\ \mathfrak{m} > \mathfrak{n},$$

а из теории кардинальных чисел следует, что всегда имеет место ровно одно из этих соотношений (см. приложение к настоящей главе, Предложение 2). Более того, теорема Кантора – Бернштейна показывает, что отношение $<$ транзитивно, т. е. из $\mathfrak{m} < \mathfrak{n}$ и $\mathfrak{n} < \mathfrak{p}$ следует $\mathfrak{m} < \mathfrak{p}$. Поэтому кардиналы располагаются в линейном порядке, начиная с конечных кардиналов $0, 1, 2, 3, \ldots$

Используя обычную систему аксиом Цермело – Френкеля, легко показать, что любое бесконечное множество M содержит счетное подмножество. В самом деле, M содержит некоторый элемент m_1. Множество $M \setminus \{m_1\}$ не пусто (так как оно бесконечно) и, следовательно, содержит некоторый элемент m_2. Рассматривая $M \setminus \{m_1, m_2\}$, мы делаем вывод о существовании в нем элемента m_3, и т. д. Итак, объем счетного множества есть *наименьший бесконечный* кардинал, который обычно обозначается $\aleph_0$ (произносится «алеф нуль»).

«Наименьший бесконечный кардинал»

В качестве простого следствия неравенства $\aleph_0 \leqslant \mathfrak{m}$ для любого бесконечного кардинала $\mathfrak{m}$ мы можем доказать утверждение об «отеле Гильберта» для любого бесконечного кардинального числа $\mathfrak{m}$, т. е. что $|M \cup \{x\}| = |M|$ для произвольного бесконечного множества M. Действительно, M содержит подмножество $N = \{m_1, m_2, m_3, \ldots\}$. Мы получим искомую биекцию, отобразив x в m_1, m_1 в m_2 и т. д., а элементы из $M \setminus N$ отобразив в себя.

Тем самым мы заодно доказали сформулированное выше утверждение: *Каждое бесконечное множество имеет тот же объем, что и некоторое его собственное подмножество.*

В качестве другого следствия теоремы Кантора – Бернштейна мы можем доказать, что множество $\mathcal{P}(\mathbb{N})$ всех подмножеств $\mathbb{N}$ имеет мощность c. Как уже отмечалось, достаточно показать, что $|\mathcal{P}(\mathbb{N}) \setminus \{\varnothing\}| = |(0, 1]|$. Примером инъективного отображения является

$$f : \mathcal{P}(\mathbb{N}) \setminus \{\varnothing\} \longrightarrow (0, 1], \qquad A \longmapsto \sum_{i \in A} 10^{-i},$$

а

$$g : (0, 1] \longrightarrow \mathcal{P}(\mathbb{N}) \setminus \{\varnothing\}, \qquad 0, b_1 b_2 b_3 \ldots \longmapsto \{b_i 10^i : i \in \mathbb{N}\}$$

определяет инъекцию в обратном направлении.

Пока что мы ввели кардинальные числа $0, 1, 2, \ldots, \aleph_0$ и, кроме того, знаем, что мощность c множества $\mathbb{R}$ больше $\aleph_0$. Переход от $\mathbb{Q}$, где $|\mathbb{Q}| = \aleph_0$, к $\mathbb{R}$, для которого $|\mathbb{R}| = c$, немедленно вызывает следующий вопрос:

> *Является ли $c = |\mathbb{R}|$ следующим за $\aleph_0$ бесконечным кардинальным числом?*

Возникает и другой вопрос: существует ли следующее за $\aleph_0$ большее кардинальное число[3], т. е. можно ли приписать естественный смысл символу $\aleph_1$? Ответ на него положителен; доказательство намечено в приложении к этой главе.

Равенство $c = \aleph_1$ было названо *континуум-гипотезой*. Вопрос о том, верна ли континуум-гипотеза, в течение многих десятилетий считался

[3] Например, при естественном упорядочении $\mathbb{R}$ не существует действительного числа, следующего за 0. — *Прим. ред.*

одной из самых сложных проблем во всей математике. Ответ, который нашли Курт Гёдель и Поль Коэн, привел к границам логического мышления. Они показали, что утверждение $c = \aleph_1$ *не зависит* от системы аксиом Цермело – Френкеля таким же образом, как аксиома о параллельных прямых не зависит от других аксиом евклидовой геометрии. Существуют модели теории множеств, в которых равенство $c = \aleph_1$ выполняется, но имеются другие модели, в которых $c \neq \aleph_1$.

В свете этого факта становится интересным такой вопрос: есть ли другие условия (например, в анализе), эквивалентные континуум-гипотезе? Мы приведем один подобный пример и его чрезвычайно изящное и простое решение, полученное Паулем Эрдёшем. В 1962 году Ветцель задал следующий вопрос:

> *Пусть $\{f_\alpha\}$ — семейство попарно различных аналитических функций, определенных на множестве комплексных чисел и таких, что для каждого $z \in \mathbb{C}$ множество значений $\{f_\alpha(z)\}$ не более чем счетно (т. е. либо конечно, либо счетно); назовем это свойством (P_0).*
> *Следует ли из (P_0), что семейство само не более чем счетно?*

Немного позже Эрдёш показал [5], что ответ, неожиданно, зависит от континуум-гипотезы.

Теорема 5. *Если $c > \aleph_1$, то каждое семейство $\{f_\alpha\}$, удовлетворяющее (P_0), счетно. С другой стороны, если $c = \aleph_1$, то существует обладающее свойством (P_0) семейство $\{f_\alpha\}$, объем которого равен c.*

Для доказательства нам будут нужны некоторые основные факты о кардинальных и порядковых[4] числах. Читатели, которые не знакомы с этими понятиями, могут найти все необходимые результаты в приложении к настоящей главе.

■ **Доказательство теоремы 5.** Предположим вначале, что $c > \aleph_1$. Покажем, что для любого семейства аналитических функций $\{f_\alpha\}$ объема $\aleph_1$ существует такое комплексное число z_0, что *все* $\aleph_1$ значений $f_\alpha(z_0)$ различны. Следовательно, если семейство функций удовлетворяет условию (P_0), то оно должно быть счетным.

Чтобы доказать это, нужно воспользоваться свойствами порядковых чисел. Сначала вполне упорядочим семейство $\{f_\alpha\}$ в соответствии с начальным порядковым числом ω_1 кардинала $\aleph_1$. Согласно предложению 1 приложения это означает, что индекс пробегает все порядковые числа α, которые меньше ω_1. Теперь покажем, что множество пар (α, β), $\alpha < \beta < \omega_1$, имеет объем $\aleph_1$. Так как любое $\beta < \omega_1$ есть счетное порядковое число, то множество пар (α, β), $\alpha < \beta$, для каждого фиксированного β счетно. Беря объединение по всему множеству порядковых чисел β, имеющему объем $\aleph_1$, мы находим с помощью предложения 6 из приложения, что множество всех пар (α, β), $\alpha < \beta$, имеет объем $\aleph_1$.

Рассмотрим теперь для любой пары $\alpha < \beta$ множество

$$S(\alpha, \beta) \;=\; \{z \in \mathbb{C} : f_\alpha(z) = f_\beta(z)\}.$$

[4] Или трансфинитных. — *Прим. перев.*

Мы утверждаем, что каждое множество $S(\alpha,\beta)$ счетно. Чтобы проверить это, рассмотрим круги C_k радиусов $k = 1, 2, 3, \ldots$ с центром в начале координат комплексной плоскости. Если f_α и f_β совпадают в бесконечном множестве точек e_k некоторого круга C_k, то f_α и f_β тождественно равны в силу известной теоремы об аналитических функциях. Следовательно, f_α и f_β совпадают лишь в конечном числе точек каждого C_k и поэтому в целом — не более чем в счетном множестве точек. Теперь положим $S = \bigcup_{\alpha<\beta} S(\alpha,\beta)$. Снова используя предложение 6, мы находим, что S имеет объем $\aleph_1$, так как каждое из множеств $S(\alpha,\beta)$ счетно. И вот изюминка доказательства: так как $\mathbb{C}$ имеет объем c и по предположению c больше $\aleph_1$, то существует комплексное число $z_0 \notin S$, и для этого z_0 все $\aleph_1$ значений $f_\alpha(z_0)$ различны.

Далее предположим, что $c = \aleph_1$. Рассмотрим множество $D \subseteq \mathbb{C}$ комплексных чисел $p + iq$ с рациональными действительной и мнимой частями. Поскольку для каждого p множество $\{p + iq : q \in \mathbb{Q}\}$ счетно, мы находим, что и D счетно. Более того, множество D *плотно* в $\mathbb{C}$: каждый открытый круг в комплексной плоскости содержит некоторую точку из D. Пусть $\{z_\alpha : 0 \le \alpha < \omega_1\}$ — вполне упорядоченное множество $\mathbb{C}$. Построим семейство $\{f_\beta : 0 \le \beta < \omega_1\}$, состоящее из $|\aleph_1|$ различных аналитических функций, для которых

$$f_\beta(z_\alpha) \in D \quad \text{всякий раз, когда } \alpha < \beta. \tag{1}$$

Любое такое семейство удовлетворяет условию (P_0). В самом деле, каждая точка $z \in \mathbb{C}$ имеет некоторый индекс, скажем, $z = z_\alpha$. Для всех $\beta > \alpha$ значения $\{f_\beta(z_\alpha)\}$ принадлежат *счетному* множеству D. Так как α — счетное порядковое число, функции f_β, где $\beta \le \alpha$ добавляют не более чем счетное множество других значений $f_\beta(z_\alpha)$, и поэтому множество всех значений $\{f_\beta(z_\alpha)\}$ также не более чем счетно. Следовательно, если мы построим семейство $\{f_\beta\}$, удовлетворяющее условию (1), то вторая часть теоремы будет доказана.

Построение семейства $\{f_\beta\}$ производится с помощью трансфинитной индукции[5]. В качестве f_0 мы можем взять произвольную аналитическую функцию, например, $f_0 = \text{const}$. Предположим, что функции f_β уже построены для всех $\beta < \gamma$. Учитывая, что γ — счетное порядковое число, мы можем переупорядочить $\{f_\beta : 0 \le \beta < \gamma\}$ и получить последовательность $g_1, g_2, g_3, \ldots$ То же самое переупорядочение множества $\{z_\alpha : 0 \le \alpha < \gamma\}$ дает последовательность $w_1, w_2, w_3, \ldots$ Нашей целью будет построить функцию f_γ, которая для каждого n удовлетворяет условиям

$$f_\gamma(w_n) \in D \qquad \text{и} \qquad f_\gamma(w_n) \ne g_n(w_n). \tag{2}$$

Второе из условий (2) обеспечит различие всех функций f_γ $(0 \le \gamma < \omega_1)$, а первое условие — выполнение (1), откуда согласно нашему предыдущему рассуждению следует (P_0). Заметим, что возможность выполнения условия $f_\gamma(w_n) \ne g_n(w_n)$ обосновывается с помощью диагонального метода.

Чтобы построить f_γ, положим

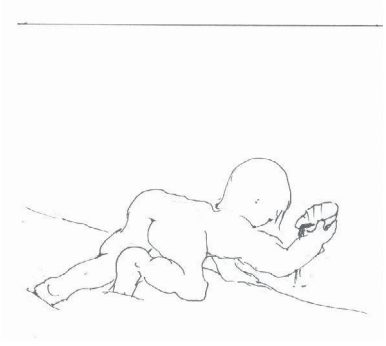
$$\begin{aligned} f_\gamma(z) \quad := \quad & \varepsilon_0 + \varepsilon_1(z - w_1) + \varepsilon_2(z - w_1)(z - w_2) + \\ & + \varepsilon_3(z - w_1)(z - w_2)(z - w_3) + \ldots \end{aligned}$$

[5] См., например, [8*], с.28. — *Прим. перев.*

Если γ — конечное порядковое число, то f_γ является многочленом и, следовательно, аналитической функцией, и мы можем, конечно, выбрать числа ε_i так, чтобы выполнялись условия (2). Теперь предположим, что γ — счетное порядковое число. Тогда

$$f_\gamma(z) \;=\; \sum_{n=0}^{\infty} \varepsilon_n (z-w_1)\cdots(z-w_n). \qquad (3)$$

Заметим, что значения ε_m $(m \geq n)$ не влияют на значение $f_\gamma(w_n)$, так что мы можем последовательно шаг за шагом задавать коэффициенты ε_n. Если последовательность $\{\varepsilon_n\}$ сходится к 0 достаточно быстро, то (3) определяет аналитическую функцию. Наконец, поскольку D — плотное множество, мы можем выбирать последовательность (ε_n) так, чтобы f_γ удовлетворяла условиям (2), и доказательство закончено. □



В легенде о святом Августине говорится, что, прогуливаясь по берегу моря и размышляя о бесконечности, он увидел ребенка, который пытался осушить океан с помощью маленькой раковины....

Приложение: о кардинальных и порядковых числах

В первую очередь обсудим вопрос: для каждого ли кардинального числа существует следующее большее кардинальное число. Сначала покажем, что для каждого кардинального числа $\mathfrak{m}$ всегда имеется кардинальное число $\mathfrak{n}$, которое больше $\mathfrak{m}$. Для этого снова воспользуемся вариантом диагонального метода Кантора.

Пусть M — множество; докажем, что объем множества $\mathcal{P}(M)$ *всех подмножеств* M больше, чем объем M. Сопоставляя каждому элементу $m \in M$ подмножество $\{m\} \in \mathcal{P}(M)$, мы находим, что M можно биективно отобразить в подмножество $\mathcal{P}(M)$, откуда по определению следует, что $|M| \leq |\mathcal{P}(M)|$. Остается показать, что $\mathcal{P}(M)$ *нельзя* биективно отобразить в подмножество M. Предположим противное: пусть $\varphi : N \longrightarrow \mathcal{P}(M)$ — биекция из $N \subseteq M$ на $\mathcal{P}(M)$. Рассмотрим подмножество $U \subseteq N$ всех элементов N, *не* содержащихся в своих образах при действии φ, т. е. $U = \{m \in N : m \notin \varphi(m)\}$. Так как φ — биекция, то существует такой элемент $u \in N$, что $\varphi(u) = U$. Тогда либо $u \in U$, либо $u \notin U$, но оба эти случая невозможны! Действительно, если $u \in U$, то $u \notin \varphi(u) = U$ согласно определению U; если же $u \notin U = \varphi(u)$, то $u \in U$, и в обоих случаях мы приходим к противоречию.

Скорее всего, читатель уже встречался с таким рассуждением. Давно известен парадокс брадобрея: «Брадобрей — это мужчина, бреющий всех мужчин, которые не бреются сами. Бреется ли сам брадобрей?»

Чтобы углубиться в теорию, введем другую важную концепцию Кантора — упорядоченные множества и порядковые числа. Множество M *упорядочено* с помощью отношения $<$, если отношение $<$ транзитивно и для любых двух различных элементов a и b из M либо $a < b$, либо $b < a$. Например, можно упорядочить множество $\mathbb{N}$ обычным способом в соответствии с величиной его элементов: $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$, но, конечно, можно также упорядочить $\mathbb{N}$ в обратном направлении: $\mathbb{N} = \{\ldots, 4, 3, 2, 1\}$, или положить $\mathbb{N} = \{1, 3, 5, \ldots, 2, 4, 6, \ldots\}$, перечисляя сначала нечетные, а затем четные числа.

Введем теперь важное понятие. Упорядоченное множество M называется *вполне упорядоченным*, если каждое непустое подмножество M

имеет первый элемент. Как легко проверить, указанные выше первое и третье упорядочения $\mathbb{N}$ являются вполне упорядоченными, а второе упорядочение — нет. Фундаментальная *теорема о полном упорядочении множества*, вытекающая из аксиом (включая аксиому выбора), утверждает, что *каждое* множество M можно вполне упорядочить. В дальнейшем мы будем рассматривать лишь вполне упорядоченные множества.

Будем говорить, что два вполне упорядоченных множества M и N (с отношениями порядка $<_M$ и $<_N$) *подобны* (или имеют *один и тот же порядковый тип*), если существует биекция φ из M в N, которая не нарушает порядок, т. е. если из $m <_M n$ следует, что $\varphi(m) <_N \varphi(n)$. Заметим, что произвольное упорядоченное множество, подобное вполне упорядоченному множеству, само вполне упорядочено.

Множества $\mathbb{N} = \{1, 2, 3, \ldots\}$ и $\mathbb{N} = \{1, 3, 5, \ldots, 2, 4, 6, \ldots\}$ вполне упорядочены, но *не* подобны: первое упорядочение имеет лишь один элемент без непосредственного предшественника, в то время как второе имеет два таких элемента.

Понятно, что подобие является отношением эквивалентности, и поэтому мы можем говорить о *порядковом числе* α, связанном с классом подобных множеств. Любые два конечные вполне упорядоченные множества одинаковой мощности подобны, и мы снова используем порядковое число n для обозначения порядкового типа n-множеств. Отметим, что два подобных множества по определению имеют одинаковую мощность. Значит, есть смысл говорить о *мощности* $|\alpha|$. Заметим еще, что любое подмножество вполне упорядоченного множества тоже вполне упорядочено в соответствии с индуцированным порядком.

Сравним теперь порядковые числа, как мы делали это для кардинальных чисел. Пусть M — вполне упорядоченное множество и $m \in M$. Множество $M_m = \{x \in M : x < m\}$ назовем (*начальным*) *сегментом*, определяемым элементом m; множество N — сегмент множества M, если $N = M_m$ для некоторого $m \in M$. В частности, множество M_m — пустое, если m — первый элемент множества M. Пусть теперь μ и ν — порядковые числа вполне упорядоченных множеств M и N. Будем говорить, что μ *меньше* ν, $\mu < \nu$, если M подобно некоторому сегменту множества N. Снова выполняется закон транзитивности: из $\mu < \nu$, $\nu < \pi$ следует, что $\mu < \pi$, так как при отображении подобия сегмент отображается в сегмент.

Порядковое число множества $\{1, 2, 3, \ldots\}$ меньше порядкового числа множества $\{1, 3, 5, \ldots, 2, 4, 6, \ldots\}$.

Ясно, что для конечных множеств неравенство $m < n$ имеет обычный смысл. Обозначим через ω порядковое число множества $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$, упорядоченного согласно величине элементов. Рассматривая сегмент $\mathbb{N}_{n+1}$, мы находим, что $n < \omega$ для любого конечного n. Далее, соотношение $\omega \leq \alpha$ справедливо для любого бесконечного порядкового числа α. В самом деле, если бесконечное вполне упорядоченное множество M имеет порядковое число α, то M имеет первый элемент m_1, множество $M\backslash\{m_1\}$ имеет первый элемент m_2, множество $M\backslash\{m_1, m_2\}$ имеет первый элемент m_3. Продолжая таким образом, получаем в M последовательность $m_1 < m_2 < m_3 < \ldots$ Если $M = \{m_1, m_2, m_3, \ldots\}$, то M подобно $\mathbb{N}$, и поэтому $\alpha = \omega$. С другой стороны, если $M\backslash\{m_1, m_2, \ldots\}$ не пусто, то в нем есть первый элемент m, и мы приходим к выводу, что $\mathbb{N}$ подобно сегменту M_m, т. е. $\omega < \alpha$ по определению.

Теперь сформулируем (без доказательств, которые не трудны) три основных утверждения о порядковых числах. Согласно первому из них любое порядковое число μ имеет «стандартное» представляющее его вполне упорядоченное множество W_μ.

Предложение 1. *Пусть μ — порядковое число и W_μ обозначает множество порядковых чисел, меньших μ. Тогда:*

(i) *элементы множеств W_μ попарно сравнимы;*

(ii) *если упорядочить W_μ согласно величинам элементов, то W_μ будет вполне упорядоченным и ему будет соответствовать порядковое число μ.*

Предложение 2. *Любые два порядковых числа μ и ν удовлетворяют ровно одному из соотношений $\mu < \nu$, $\mu = \nu$, $\mu > \nu$.*

Предложение 3. *Каждое множество порядковых чисел (упорядоченных в соответствии с величиной) вполне упорядочено.*

После этой экскурсии по порядковым числам вернемся к кардинальным числам. Пусть $\mathfrak{m}$ — кардинальное число и $O_\mathfrak{m}$ обозначает множество всех порядковых чисел μ, для которых $|\mu| = \mathfrak{m}$. Согласно Предложению 3 в $O_\mathfrak{m}$ существует *наименьшее* порядковое число $\omega_\mathfrak{m}$, которое мы назовем *начальным порядковым числом* множества $O_\mathfrak{m}$. Например, ω является начальным порядковым числом для $\aleph_0$.

Теперь мы можем доказать основной результат этой главы.

Предложение 4. *Для каждого кардинального числа $\mathfrak{m}$ существует однозначно определенное соседнее большее кардинальное число.*

■ **Доказательство.** Мы уже знаем, что существует некоторое большее кардинальное число $\mathfrak{n}$. Рассмотрим теперь множество $\mathcal{K}$ всех кардинальных чисел, которые больше $\mathfrak{m}$ и не превосходят $\mathfrak{n}$. Поставим в соответствие каждому $\mathfrak{p} \in \mathcal{K}$ его начальное порядковое число $\omega_\mathfrak{p}$. Среди этих начальных чисел имеется наименьшее (см. Предложение 3); соответствующее ему кардинальное число является наименьшим и, следовательно, искомым кардинальным числом, соседним с $\mathfrak{m}$ и бóльшим $\mathfrak{m}$. □

Предложение 5. *Пусть бесконечное множество M имеет мощность $\mathfrak{m}$, и вполне упорядочено в соответствии с начальным порядковым числом $\omega_\mathfrak{m}$. Тогда M не имеет последнего элемента.*

■ **Доказательство.** В самом деле, если M имеет последний элемент m, то сегмент M_m будет иметь порядковое число $\mu < \omega_\mathfrak{m}$, где $|\mu| = \mathfrak{m}$, что противоречит определению $\omega_\mathfrak{m}$. □

Наконец, нам требуется значительное усиление утверждения о том, что объединение счетного множества счетных множеств снова счетно. В следующем предложении мы рассматриваем *произвольные* семейства счетных множеств.

Предложение 6. *Пусть M — такое множество, что $|M| = \mathfrak{m}$ — бесконечный кардинал, и пусть $\{A_\alpha\}_{\alpha\in M}$ — семейство счетных множеств A_α. Тогда объем объединения $\bigcup\limits_\alpha A_\alpha$ не больше $\mathfrak{m}$.*

■ **Доказательство.** Можно предполагать, что множества A_α попарно не пересекаются, так как это не уменьшает объем объединения. Пусть

индексное множество M вполне упорядочено согласно начальному порядковому числу $\omega_{\mathfrak{m}}$. Заменим теперь каждое $\alpha \in M$ счетным множеством $B_\alpha = \{b_{\alpha 1} = \alpha, b_{\alpha 2}, b_{\alpha 3}, \ldots\}$, упорядоченным в соответствии с ω, и обозначим новое множество $\widetilde{M}$. Тогда, полагая $b_{\alpha i} < b_{\beta j}$, если $\alpha < \beta$, и $b_{\alpha i} < b_{\alpha j}$, если $i < j$, получим, что $\widetilde{M}$ тоже вполне упорядочено. Пусть $\widetilde{\mu}$ — порядковое число множества $\widetilde{M}$. Учитывая, что M — подмножество $\widetilde{M}$, в силу предыдущих соображений имеем $\mu \leq \widetilde{\mu}$. Если $\mu = \widetilde{\mu}$, то M подобно $\widetilde{M}$; если же $\mu < \widetilde{\mu}$, то M подобно сегменту $\widetilde{M}$. Далее, так как упорядочение $\omega_{\mathfrak{m}}$ множества M не имеет последнего элемента (см. Предложение 5), мы находим, что в обоих случаях M подобно объединению счетных множеств B_β и поэтому имеет ту же самую мощность.

Остальное просто. Пусть $\varphi : \bigcup B_\beta \longrightarrow M$ — биекция; предположим, что $\varphi(B_\beta) = \{\alpha_1, \alpha_2, \alpha_3, \ldots\}$. Заменим каждый элемент α_i на A_{α_i} и рассмотрим объединение $\bigcup A_{\alpha_i}$. Учитывая, что $\bigcup A_{\alpha_i}$ — объединение *счетного* множества счетных множеств (и, следовательно, счетно), мы видим, что B_β имеет объем, одинаковый с объемом $\bigcup A_{\alpha_i}$. Другими словами, для каждого β существует биекция из B_β в $\bigcup A_{\alpha_i}$ и тем самым биекция ψ из $\bigcup B_\beta$ в $\bigcup A_\alpha$. Но тогда отображение $\psi\varphi^{-1}$ дает желаемую биекцию из M в $\bigcup A_\alpha$, так что $|\bigcup A_\alpha| = \mathfrak{m}$. □

Литература

[1] Brouwer L. E. J. *Beweis der Invarianz der Dimensionszahl.* Math. Annalen, **70** (1911), 161–165.

[2] Calkin N., Wilf H. *Recounting the rationals.* Amer. Math. Monthly, **107** (2000), 360–363.

[3] Cantor G. *Ein Beitrag zur Mannigfaltigkeitslehre.* Journal für die reine und angewandte Mathematik, **84** (1878), 242–258.

[4] Cohen P. *Set Theory and the Continuum Hypothesis.* W. A. Benjamin, New York, 1966.

[5] Erdős P. *An interpolation problem associated with the continuum hypothesis.* Michigan Math. J., **11** (1964), 9–10.

[6] Kamke E. *Theory of Sets,* Dover Books, 1950.

[7] Stern M. A. *Ueber eine zahlentheoretische Funktion.* Journal für die reine und angewandte Mathematik, **55** (1858), 193–220.

[8*] Серпинский В. *О теории множеств.* М.: Просвещение, 1966.

«Бесконечное множество кардиналов»

Во славу неравенств

Глава 18

Математический анализ изобилует неравенствами, о чем свидетельствует, например, знаменитая книга «Неравенства» Харди, Литтлвуда и Пойа [4]. Учитывая мнение Дьердя Пойа (одного из чемпионов Книги Доказательств) о том, какие доказательства являются самыми подходящими, рассмотрим два наиболее важных неравенства и два применения каждого из них.

Наше первое неравенство разные авторы приписывают Коши, Шварцу и (или) Буняковскому[1].

Теорема I (неравенство Коши – Буняковского – Шварца). *Пусть $\langle \boldsymbol{a}, \boldsymbol{b}\rangle$ — скалярное произведение в вещественном векторном пространстве V (с нормой $|\boldsymbol{a}|^2 := \langle \boldsymbol{a}, \boldsymbol{a}\rangle$). Тогда для любых векторов $\boldsymbol{a}, \boldsymbol{b} \in V$ справедливо неравенство*

$$\langle \boldsymbol{a}, \boldsymbol{b}\rangle^2 \;\le\; |\boldsymbol{a}|^2|\boldsymbol{b}|^2,$$

и равенство имеет место тогда и только тогда, когда $\boldsymbol{a}$ и $\boldsymbol{b}$ линейно зависимы.

■ **Доказательство.** Следующее (фольклорное) доказательство является, видимо, самым коротким. Рассмотрим квадратичный многочлен

$$|x\boldsymbol{a} + \boldsymbol{b}|^2 \;=\; x^2|\boldsymbol{a}|^2 + 2x\langle \boldsymbol{a}, \boldsymbol{b}\rangle + |\boldsymbol{b}|^2$$

от переменной x. Достаточно рассмотреть случай, когда $\boldsymbol{a} \ne \boldsymbol{0}$. Если $\boldsymbol{b} = \lambda\boldsymbol{a}$, то, очевидно, $\langle \boldsymbol{a}, \boldsymbol{b}\rangle^2 = |\boldsymbol{a}|^2|\boldsymbol{b}|^2$. Если, с другой стороны, $\boldsymbol{a}$ и $\boldsymbol{b}$ линейно независимы, то $|x\boldsymbol{a} + \boldsymbol{b}|^2 > 0$ для всех x и, следовательно, дискриминант $\langle \boldsymbol{a}, \boldsymbol{b}\rangle^2 - |\boldsymbol{a}|^2|\boldsymbol{b}|^2$ меньше нуля. □

Наш второй пример — неравенство для *гармонического, геометрического и арифметического средних.*

Теорема II (гармоническое, геометрическое и арифметическое средние). *Пусть $a_1, \ldots, a_n$ — положительные действительные числа. Тогда*

$$\frac{n}{\frac{1}{a_1} + \ldots + \frac{1}{a_n}} \;\le\; \sqrt[n]{a_1 a_2 \ldots a_n} \;\le\; \frac{a_1 + \ldots + a_n}{n},$$

и равенство в обоих случаях выполняется тогда и только тогда, когда все числа $a_1, \ldots, a_n$ равны.

[1] Неравенство для сумм произведений и сумм квадратов получил О. Коши в 1821 г., а аналогичные неравенства для интегралов — В. Я. Буняковский в 1859 г. и Г. А. Шварц в 1884 г. — *Прим. ред.*

■ **Доказательство.** Следующее красивое нестандартное индуктивное доказательство приписывают Коши (см. [7]). Пусть $P(n)$ — утверждение о справедливости второго неравенства, записанного в виде

$$a_1 a_2 \dots a_n \ \le \ \Big(\frac{a_1 + \dots + a_n}{n}\Big)^n.$$

Для $n = 2$ имеем $a_1 a_2 \le \big(\frac{a_1+a_2}{2}\big)^2 \Longleftrightarrow (a_1 - a_2)^2 \ge 0$, так что $P(2)$ верно. Если показать, что при любом натуральном $n \ge 3$

(A) $P(n) \Longrightarrow P(n-1)$,

(B) $P(n)$ и $P(2) \Longrightarrow P(2n)$,

то, очевидно, справедливость $P(n)$ для всех n будет доказана.

Чтобы доказать **(A)**, положим

$$A := \sum_{k=1}^{n-1} \frac{a_k}{n-1}.$$

Тогда

$$\Big(\prod_{k=1}^{n-1} a_k\Big) A \ \overset{P(n)}{\le} \ \left(\frac{\sum\limits_{k=1}^{n-1} a_k \ + \ A}{n}\right)^n \ = \ \Big(\frac{(n-1)A + A}{n}\Big)^n \ = \ A^n$$

и поэтому верно $P(n-1)$:

$$\prod_{k=1}^{n-1} a_k \ \le \ A^{n-1} \ = \ \left(\frac{\sum\limits_{k=1}^{n-1} a_k}{n-1}\right)^{n-1}.$$

Теперь докажем **(B)**:

$$\prod_{k=1}^{2n} a_k = \Big(\prod_{k=1}^{n} a_k\Big)\Big(\prod_{k=n+1}^{2n} a_k\Big) \ \overset{P(n)}{\le} \ \Big(\sum_{k=1}^{n} \frac{a_k}{n}\Big)^n \Big(\sum_{k=n+1}^{2n} \frac{a_k}{n}\Big)^n$$

$$\overset{P(2)}{\le} \ \left(\frac{\sum\limits_{k=1}^{2n} \frac{a_k}{n}}{2}\right)^{2n} \ = \ \left(\frac{\sum\limits_{k=1}^{2n} a_k}{2n}\right)^{2n},$$

что и требовалось.

Условие равенства проверяется совсем легко.

Левое неравенство между гармоническим и геометрическим средними теперь следует из правого, примененного к величинам $\frac{1}{a_1}, \dots, \frac{1}{a_n}$. □

■ **Другое доказательство.** Из многих других доказательств неравенства для арифметического и геометрического средних (в монографии [2] их приведено более 50) выберем особенно поразительное недавнее доказательство Альзера. Фактически это доказательство приводит к более сильному неравенству

$$a_1^{p_1} a_2^{p_2} \dots a_n^{p_n} \ \ \le \ \ p_1 a_1 + p_2 a_2 + \dots + p_n a_n$$

для любых положительных чисел $a_1, \ldots, a_n, p_1, \ldots, p_n$, удовлетворяющих условию $\sum_{i=1}^n p_i = 1$. Обозначим выражение в левой части неравенства через G, а выражение в правой части через A. Можно считать, что $a_1 \le \ldots \le a_n$. Ясно, что $a_1 \le G \le a_n$, и, следовательно, должно существовать такое k, что $a_k \le G \le a_{k+1}$. Отсюда вытекает, что

$$\sum_{i=1}^{k} p_i \int_{a_i}^{G} \Big(\frac{1}{t} - \frac{1}{G}\Big)\, dt \;+\; \sum_{i=k+1}^{n} p_i \int_{G}^{a_i} \Big(\frac{1}{G} - \frac{1}{t}\Big)\, dt \;\ge\; 0 \qquad (1)$$

так как все подынтегральные выражения неотрицательны. Преобразовывая (1), получаем неравенство

$$\sum_{i=1}^{n} p_i \int_{G}^{a_i} \frac{1}{G}\, dt \;\ge\; \sum_{i=1}^{n} p_i \int_{G}^{a_i} \frac{1}{t}\, dt,$$

левая часть которого равна

$$\sum_{i=1}^{n} p_i \frac{a_i - G}{G} \;=\; \frac{A}{G} - 1,$$

в то время как правая часть есть

$$\sum_{i=1}^{n} p_i (\log a_i - \log G) = \log \prod_{i=1}^{n} a_i^{p_i} - \log G = 0.$$

Таким образом, $\frac{A}{G} - 1 \ge 0$, в силу чего $A \ge G$. В случае равенства все интегралы в (1) должны быть равны нулю, а это возможно только при $a_1 = \ldots = a_n = G$. □

Наше первое применение — прекрасный результат Лагерра (см. [7]), касающийся локализации корней многочленов.

Теорема 1. *Если все корни многочлена $x^n + a_{n-1}x^{n-1} + \ldots + a_0$ — действительные числа, то они содержатся в интервале с концевыми точками*

$$-\frac{a_{n-1}}{n} \pm \frac{n-1}{n}\sqrt{a_{n-1}^2 - \frac{2n}{n-1}a_{n-2}}\ .$$

■ **Доказательство.** Пусть y — один из корней, а $y_1, \ldots, y_{n-1}$ — остальные корни. Тогда многочлен можно записать в виде произведения $(x-y)(x-y_1)\cdots(x-y_{n-1})$. Следовательно,

$$\begin{aligned} -a_{n-1} &= y + y_1 + \ldots + y_{n-1}, \\ a_{n-2} &= y(y_1 + \ldots + y_{n-1}) + \sum_{i<j} y_i y_j, \end{aligned}$$

и поэтому

$$a_{n-1}^2 - 2a_{n-2} - y^2 \;=\; \sum_{i=1}^{n-1} y_i^2.$$

Применяя неравенство Коши к $(y_1, \ldots, y_{n-1})$ и $(1, \ldots, 1)$, получаем

$$\begin{aligned} (a_{n-1} + y)^2 &= (y_1 + y_2 + \ldots + y_{n-1})^2 \le \\ &\le (n-1)\sum_{i=1}^{n-1} y_i^2 \;=\; (n-1)(a_{n-1}^2 - 2a_{n-2} - y^2), \end{aligned}$$

$a_1 = a_1^{p_1} \ldots a_1^{p_n} \le a_1^{p_1} \ldots a_n^{p_n} = G \le a_n^{p_1} \ldots a_n^{p_n} = a_n$.
— *Прим. перев.*

Используются равенства

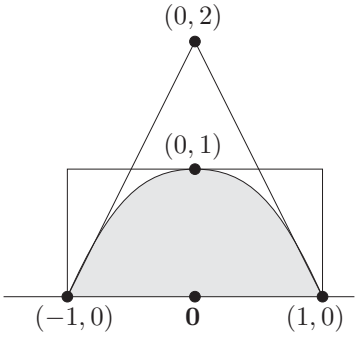
$$\int_{a_i}^{G} \Big(\frac{1}{t} - \frac{1}{G}\Big)\, dt = \int_{G}^{a_i} \Big(\frac{1}{G} - \frac{1}{t}\Big)\, dt,$$

$i = 1, \ldots, k$. — *Прим. перев.*

или

$$y^2 + \frac{2a_{n-1}}{n}\, y + \frac{2(n-1)}{n}\, a_{n-2} - \frac{n-2}{n}\, a_{n-1}^2 \le 0.$$

Таким образом, y (как и все y_i) расположен между корнями квадратного уравнения, а они совпадают с указанными в теореме границами. □



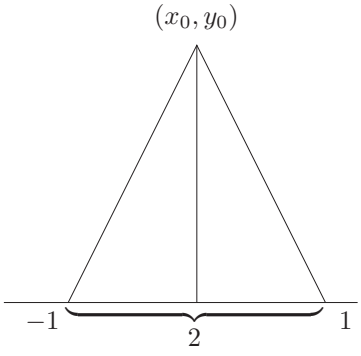
Наше второе применение мы начнем с известного элементарного свойства параболы. Рассмотрим параболу, описываемую функцией $f(x) = 1 - x^2$ в промежутке между точками $x = -1$ и $x = 1$. Поставим в соответствие $f(x)$ *тангенциальный треугольник*[2] и *тангенциальный прямоугольник*, как на рисунке на полях.

Мы находим, что заштрихованная площадь $A = \int_{-1}^{1}(1 - x^2)dx$ равна $\frac{4}{3}$, а площади T и R треугольника и прямоугольника равны 2. Следовательно, $\frac{T}{A} = \frac{3}{2}$ и $\frac{R}{A} = \frac{3}{2}$.

В своей замечательной статье Пауль Эрдёш и Тибор Галлаи [3] поставили вопрос: что произойдет, если $f(x)$ — такой вещественный многочлен n-й степени, что $f(-1) = f(1) = 0$ и $f(x) > 0$ при $-1 < x < 1$. Тогда площадь A равна $\int_{-1}^{1} f(x)dx$. Предположим, что $f(x)$ принимает в интервале $(-1, 1)$ максимальное значение в точке b, так что $R = 2f(b)$. Вычисляя тангенсы углов наклона касательных в точках -1 и 1, легко увидеть (см. вставку), что

$$T \;=\; \frac{2f'(1)f'(-1)}{f'(1) - f'(-1)}\,, \tag{2}$$

соответственно, $T = 0$, если $f'(1) = f'(-1) = 0$.



Тангенциальный треугольник

Площадь T тангенциального треугольника равна y_0, где (x_0, y_0) — точка пересечения двух касательных. Уравнения этих касательных суть $y = f'(-1)(x + 1)$ и $y = f'(1)(x - 1)$. Поэтому

$$x_0 \;=\; \frac{f'(1) + f'(-1)}{f'(1) - f'(-1)},$$

и, следовательно,

$$y_0 \;=\; f'(1)\left(\frac{f'(1) + f'(-1)}{f'(1) - f'(-1)} - 1\right) \;=\; 2\frac{f'(1)f'(-1)}{f'(1) - f'(-1)}.$$

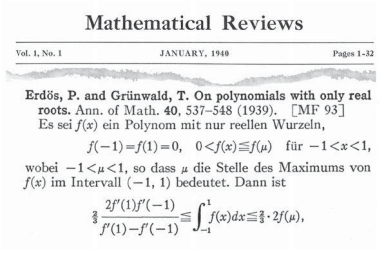
В общем случае нетривиальных оценок для $\frac{T}{A}$ и $\frac{R}{A}$ не существует. Чтобы убедиться в этом, положим $f(x) = 1 - x^{2n}$. Тогда $T = 2n$, $A = \frac{4n}{2n+1}$ и поэтому $\frac{T}{A} > n$. Аналогично, $R = 2$ и $\frac{R}{A} = \frac{2n+1}{2n}$, что стремится к 1, когда $n \to \infty$. Но, как показали Эрдёш и Галлаи, для многочленов, все корни которых вещественны, существуют нетривиальные неравенства, связывающие $\frac{T}{A}$ и $\frac{R}{A}$.

[2] Т.е. со сторонами, касающимися параболы. — *Прим. перев.*

Теорема 2. *Пусть $f(x)$ — вещественный многочлен степени $n \geq 2$, имеющий лишь действительные корни, причем $f(-1) = f(1) = 0$ и $f(x) > 0$ при $-1 < x < 1$. Тогда*

$$\frac{2}{3}T \;\leq\; A \;\leq\; \frac{2}{3}R,$$

и равенство в обоих случаях имеет место лишь для $n = 2$.


Mathematical Reviews

Vol. 1, No. 1 JANUARY, 1940 Pages 1-32

Erdös, P. and Grünwald, T. On polynomials with only real roots. Ann. of Math. **40**, 537–548 (1939). [MF 93]
Es sei $f(x)$ ein Polynom mit nur reellen Wurzeln,

$$f(-1)=f(1)=0, \quad 0<f(x)\leqq f(\mu) \quad \text{für } -1<x<1,$$

wobei $-1<\mu<1$, so dass μ die Stelle des Maximums von $f(x)$ im Intervall $(-1, 1)$ bedeutet. Dann ist

$$\tfrac{2}{3}\frac{2f'(1)f'(-1)}{f'(1)-f'(-1)} \leqq \int_{-1}^{1} f(x)dx \leqq \tfrac{2}{3}\cdot 2f(\mu),$$

Эрдёш и Галлаи установили этот результат, используя сложное доказательство по индукции. В рецензии [6] на эту статью, которая была опубликована в 1940-м году на первой странице первого выпуска Mathematical Reviews, Дьердь Пойа показал, что первое неравенство теоремы 2 можно просто доказать с помощью неравенства для арифметического и геометрического средних — прекрасный пример добросовестной рецензии и Доказательства из Книги одновременно.

■ **Доказательство неравенства $\frac{2}{3}T \leq A$.** Так как многочлен $f(x)$ имеет лишь действительные корни и не имеет их в открытом интервале $(-1, 1)$, его можно представить (с точностью до постоянного множителя, который в конце сократится) в виде

$$f(x) \;=\; (1-x^2)\prod_i(\alpha_i - x)\prod_j(\beta_j + x), \tag{3}$$

где все $\alpha_i \geq 1$, $\beta_j \geq 1$. Следовательно,

$$A \;=\; \int_{-1}^{1}(1-x^2)\prod_i(\alpha_i - x)\prod_j(\beta_j + x)dx.$$

С помощью подстановки $x \longmapsto -x$ мы получаем также, что

$$A \;=\; \int_{-1}^{1}(1-x^2)\prod_i(\alpha_i + x)\prod_j(\beta_j - x)dx,$$

и поэтому по неравенству для арифметического и геометрического средних (все множители под знаком интеграла неотрицательны)

$$\begin{aligned}
A \;&=\; \int_{-1}^{1}\frac{1}{2}\Big[\;(1-x^2)\prod_i(\alpha_i - x)\prod_j(\beta_j + x) \;+ \\
&\qquad + (1-x^2)\prod_i(\alpha_i + x)\prod_j(\beta_j - x)\;\Big]dx \\
&\geq\; \int_{-1}^{1}(1-x^2)\Big(\prod_i(\alpha_i^2 - x^2)\prod_j(\beta_j^2 - x^2)\Big)^{1/2}dx \geq \\
&\geq\; \int_{-1}^{1}(1-x^2)\Big(\prod_i(\alpha_i^2 - 1)\prod_j(\beta_j^2 - 1)\Big)^{1/2}dx = \\
&=\; \frac{4}{3}\Big(\prod_i(\alpha_i^2 - 1)\prod_j(\beta_j^2 - 1)\Big)^{1/2}.
\end{aligned}$$

Вычислим $f'(1)$ и $f'(-1)$. (Можно считать, что $f'(-1), f'(1) \neq 0$, так как в противном случае $T = 0$ и неравенство $\frac{2}{3}T \leq A$ становится тривиальным.) В силу (3)

$$f'(1) \;=\; -2\prod_i(\alpha_i - 1)\prod_j(\beta_j + 1)$$

и аналогично

$$f'(-1) \;=\; 2\prod_i(\alpha_i + 1)\prod_j(\beta_j - 1)\,.$$

Отсюда следует, что

$$A \;\geq\; \frac{2}{3}\,(-f'(1)f'(-1))^{1/2}.$$

Применяя теперь неравенство для гармонического и геометрического средних к $-f'(1)$ и $f'(-1)$ и учитывая (2), находим:

$$A \;\geq\; \frac{2}{3}\,\frac{2}{\frac{1}{-f'(1)} + \frac{1}{f'(-1)}} \;=\; \frac{4}{3}\,\frac{f'(1)f'(-1)}{f'(1) - f'(-1)} \;=\; \frac{2}{3}\,T,$$

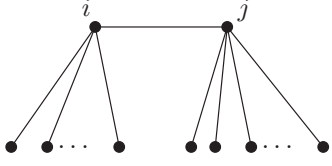
что и требовалось доказать. Анализируя условия, при которых все приведенные выше неравенства становятся равенствами, легко получить последнее утверждение для левого неравенства теоремы. □

Предлагаем читателю найти такое же вдохновляющее доказательство второго неравенства теоремы 2.

Неравенства составляют значительную часть математического анализа; мы же приведем пример из теории графов, в которой использование неравенств приводит к совершенно неожиданному результату. В главе 36 мы рассмотрим теорему Турана. В простейшем случае она принимает следующий вид.

Теорема 3. *Пусть G — граф с n вершинами, не имеющий треугольников. Тогда G имеет не более $\frac{n^2}{4}$ ребер, и равенство достигается лишь тогда, когда n четно и G является полным двудольным графом $K_{n/2,n/2}$.*

■ **Первое доказательство.** Это доказательство, использующее неравенство Коши, принадлежит Мантелю [5]. Пусть $V = \{1, \ldots, n\}$ — множество вершин и E — множество ребер графа G. Обозначим через d_i степень вершины i, так что $\sum_{i\in V} d_i = 2|E|$ (см. формулу (4) в главе 25). Пусть ij — ребро. Так как G не имеет треугольников, мы находим, что $d_i + d_j \leq n$, поскольку нет вершин, смежных и i, и j.



Отсюда следует, что

$$\sum_{ij\in E}(d_i + d_j) \;\leq\; n|E|.$$

Заметим, что d_i появляется в написанной сумме ровно d_i раз, так что

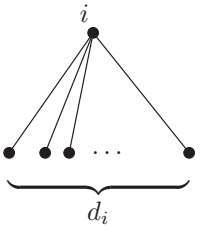
$$n|E| \;\geq\; \sum_{ij\in E}(d_i + d_j) \;=\; \sum_{i\in V} d_i^2,$$

и поэтому применение неравенства Коши к векторам $(d_1, \ldots, d_n)^T$ и $(1, \ldots, 1)^T$ дает оценку

$$n|E| \;\geq\; \sum_{i\in V} d_i^2 \;\geq\; \frac{(\sum d_i)^2}{n} \;=\; \frac{4|E|^2}{n},$$

из которой вытекает утверждение теоремы. В случае равенства должно быть $d_i = d_j$ для всех i, j; кроме того, $d_i = \frac{n}{2}$, так как $d_i + d_j = n$. Учитывая, что G свободен от треугольников, отсюда немедленно заключаем, что $G = K_{n/2,n/2}$. □

■ **Второе доказательство.** Следующее доказательство теоремы 3, в котором используется неравенство для арифметического и геометрического средних, является фольклором Книги Доказательств. Пусть α — объем наибольшего независимого множества A графа G и $\beta = n - \alpha$. Так как G не имеет треугольников, то соседи любой вершины образуют независимое множество, поэтому $d_i \leq \alpha$ для всех i.



Множество вершин $B = V\backslash A$ объема β пересекается с каждым ребром графа G. (Ребро графа G, не пересекающееся с B, должно соединять вершины $E\backslash B = A$, что противоречит выбору A. — *Прим. перев.*) Считая ребра графа G согласно их концевым вершинам в B, мы получаем $|E| \leq \sum_{i\in B} d_i$. Неравенство для арифметического и геометрического средних теперь дает

$$|E| \;\leq\; \sum_{i\in B} d_i \;\leq\; \alpha\beta \;\leq\; \Big(\frac{\alpha+\beta}{2}\Big)^2 \;=\; \frac{n^2}{4}\,.$$

Как и ранее, случай равенства рассматривается без труда. □

Литература

[1] Alzer H. *A proof of the arithmetic mean-geometric mean inequality.* Amer. Math. Monthly, **103** (1996), 585.

[2] Bullen P. S., Mitrinovics D. S., Vasić P. M. *Means and their Inequalities.* Reidel, Dordrecht, 1988.

[3] Erdős P., Grünwald T. *On polynomials with only real roots.* Annals Math., **40** (1939), 537–548.

[4] Hardy G. H., Littlewood J. E., Pólya G. *Inequalities.* Cambridge University Press, Cambridge, 1952. [Русский перевод английского издания 1934 г.: Харди Г. Г., Литтльвуд Дж. Е., Полиа Г. *Неравенства.* М.: Гос. изд-во иностранной литературы, 1948.]

[5] Mantel W. *Problem 28.* Wiskundige Opgaven, **10** (1906), 60–61.

[6] Pólya G. *Review of* [3]. Mathematical Reviews, **1** (1940), 1.

[7] Pólya G., Szegő G. *Problems and Theorems in Analysis, Vol. I.* Springer-Verlag, Berlin, Heidelberg, New York, 1972/78; Reprint 1998. [Русские переводы см., например: Полиа Г., Сеге Г. *Задачи и теоремы из анализа*, т. 1. М., ГИТТЛ, 1956, 1978].

Глава 19 Основная теорема алгебры

Высказывались мнения, что «Основная теорема алгебры» не является действительно основной, что она не совсем теорема, так как в некоторых случаях используется как определение, и что в ее классическом виде она относится не столько к алгебре, сколько к математическому анализу.

Жан Лерон Д'Аламбер

> *Каждый отличный от константы многочлен с комплексными коэффициентами имеет хотя бы один корень в поле комплексных чисел.*

Гаусс назвал эту теорему, для которой он предложил семь доказательств, «основной теоремой алгебраических уравнений». Она, несомненно, является одной из вех в истории математики. Как отметил Рейнгольд Реммерт в своем обзоре [5], «именно возможность доказательства этой теоремы в комплексной области больше всего остального подготовила почву для полного признания комплексных чисел».

Многие величайшие математики от Гаусса и Коши до Лиувилля и Лапласа внесли вклад в рассматриваемую тему. В статье Нетто и Ле Вавассера [3] перечислено около сотни доказательств. Приводимое здесь доказательство — одно из наиболее элегантных и, безусловно, самое короткое. Оно повторяет рассуждения Даламбера [1] и Арганда [2] и использует лишь некоторые элементарные свойства многочленов и комплексных чисел. Мы признательны Франс Дакар за изысканный вариант доказательства. По существу те же самые рассуждения использовались также в статьях Редхеффера [4], Вольфенштайна [6] и, несомненно, некоторых других авторов.

Нам потребуются три утверждения из начального курса анализа.

(A) Многочлены — это непрерывные функции.

(B) Любое комплексное число с абсолютной величиной, равной 1, имеет корень m-й степени при любом $m \geq 1$.

(C) Принцип минимума Коши: непрерывная функция f, определенная на компактном множестве S и принимающая действительные значения, достигает минимума в S.

Пусть теперь $p(z) = \sum_{k=0}^{n} c_k z^k$ — комплексный многочлен степени $n \geq 1$. В качестве первого и решающего шага мы докажем утверждение, которое называют по-разному — леммой Даламбера или неравенством Арганда.

Лемма. *Если $p(a) \neq 0$, то в каждом круге D с центром в точке a есть такая внутренняя точка $b \neq a$, что $|p(b)| < |p(a)|$.*

■ **Доказательство.** Пусть круг D имеет радиус R. Тогда внутренние точки D имеют вид $a+w$, где $|w| < R$. Вначале покажем, что с помощью простых алгебраических преобразований можно получить формулу

$$p(a + w) = p(a) + cw^m(1 + r(w)), \tag{1}$$

где c — ненулевое комплексное число, $1 \le m \le n$ и $r(w)$ — многочлен степени $n-m$, причем $r(0)=0$. В самом деле,

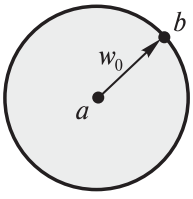
$$\begin{aligned} p(a+w) &= \sum_{k=0}^{n} c_k (a+w)^k \\ &= \sum_{k=0}^{n} c_k \sum_{i=0}^{k} \binom{k}{i} a^{k-i} w^i = \sum_{i=0}^{n} \Big(\sum_{k=i}^{n} \binom{k}{i} c_k a^{k-i} \Big) w^i \\ &= p(a) + \sum_{i=1}^{n} \Big(\sum_{k=i}^{n} \binom{k}{i} c_k a^{k-i} \Big) w^i = p(a) + \sum_{i=1}^{n} d_i w^i. \end{aligned}$$

Пусть теперь $m \ge 1$ — минимальное значение i, при котором d_i отлично от 0. Положим $c = d_m$ и вынесем множитель cw^m. Получим

$$p(a+w) = p(a) + cw^m (1 + r(w)).$$

Теперь оценим сверху $|cw^m|$ и $|r(w)|$. Если $|w|$ меньше $\rho_1 := \sqrt[m]{|p(a)/c|}$, то $cw^m < p(a)$. Далее, поскольку функция $r(w)$ непрерывна и $r(0)=0$, при некотором $\rho_2 > 0$ для всех w с $|w| < \rho_2$ выполняется неравенство $|r(w)| < 1$. Следовательно, для значений $|w|$, меньших $\rho = \min(\rho_1, \rho_2)$, имеем

$$|cw^m| < |p(a)| \qquad \text{и} \qquad |r(w)| < 1. \tag{2}$$



Воспользуемся утверждением (B) о корнях m-й степени из единицы. Пусть ζ — корень m-й степени из $-\frac{p(a)/c}{|p(a)/c|}$; это комплексное число, модуль которого равен 1. Пусть ε — такое действительное число, что $0 < \varepsilon < \min(\rho, R)$; положим $w_0 = \varepsilon\zeta$. Покажем, что $b = a + w_0$ и есть искомая точка в круге D, для которой $|p(b)| < |p(a)|$. Во-первых, b содержится в D, так как $|w_0| = \varepsilon < R$; кроме того, согласно (1)

$$|p(b)| = |p(a+w_0)| = |p(a) + cw_0^m (1 + r(w_0))|. \tag{3}$$

Далее определим множитель δ равенством

$$cw_0^m = c\varepsilon^m \zeta^m = -\frac{\varepsilon^m}{|p(a)|/c}\, p(a) = -\delta p(a);$$

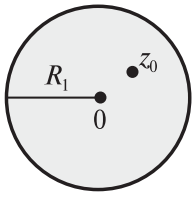
в силу (2)

$$0 < \delta = \varepsilon^m \frac{|c|}{|p(a)|} < 1.$$

Используя неравенство треугольника, получаем для выражения в правой части (3) оценку

$$\begin{aligned} |p(a) + cw_0(1 + r(w_0))| &= |p(a) - \delta p(a)(1 + r(w_0))| \\ &= |(1-\delta)p(a) - \delta p(a) r(w_0)| \\ &\le (1-\delta)|p(a)| + \delta |p(a)||r(w_0)| \\ &< (1-\delta)|p(a)| + \delta |p(a)| = p(a), \end{aligned}$$

и лемма доказана. □



Окончание доказательства «основной теоремы алгебраических уравнений» просто. Ясно, что $p(z)z^{-n}$ при $|z| \to \infty$ стремится к коэффициенту c_n при старшем члене $p(z)$. Поэтому $|p(z)|$ стремится к бесконечности вместе с $|z| \to \infty$. Следовательно, существует такое $R_1 > 0$, что $|p(z)| > |p(0)|$ для всех точек z на окружности $z : |z| = R_1$. Более того, согласно утверждению (C) минимальное значение непрерывной действительнозначной функции $|p(z)|$ в компактном множестве $D_1 = \{z : |z| \le R_1\}$ достигается в некоторой точке z_0. Так как $|p(z)| > |p(0)|$ на границе D_1, то эта точка z_0 должна находиться внутри D_1. Но согласно лемме Даламбера минимальное значение $|p(z_0)|$ не может быть больше 0, и тем самым доказательство завершено.

Литература

[1] D'Alembert J. R. *Recherches sur le calcul intégral.* Histoire de l'Academie Royale des Sciences et Belles, (1746), 182–224.

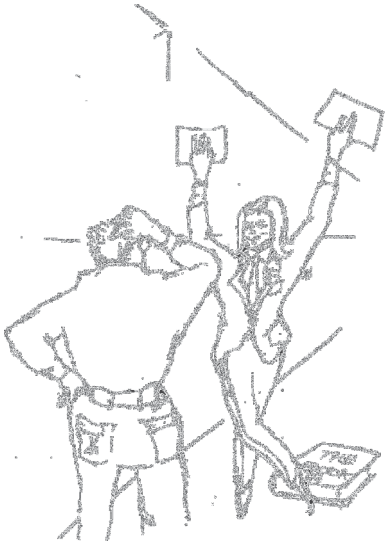
[2] Argand R. *Réflexions sur la nouvelle théorie d'analyse.* Annales de Mathematiques, **5** (1814), 197–209.

[3] Netto E., Le Vavasseur R. *Les fonctions rationelles.* Enc. Sciences Math. Pures Appl., **2** (1907), 1–232.

[4] Redheffer R. M. *What! Another note just on the fundamental theorem of algebra?* Amer. Math. Monthly, **71** (1964), 180–185.

[5] Remmert R. *The fundamental theorem of algebra.* In: Numbers, Graduate Texts in Mathematics, **123**, Springer, New York, 1991.

[6] Wolfenstein S. *Proof of the fundamental theorem of algebra.* Amer. Math. Monthly, **74** (1967), 853–854.



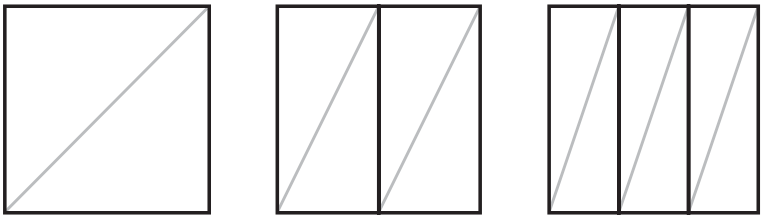
— Доказательства из Книги: одно для Основной Теоремы, одно для Взаимности Квадратичных Вычетов!

— Как дела на этот раз?
— Хорошо. Я несу 100 доказательств Основной Теоремы Алгебры.

Один квадрат и нечетное число треугольников

Глава 20

Предположим, что мы хотим разбить квадрат на n треугольников равной площади. Если n четно, то это сделать несложно: например, можно разделить квадрат вертикальными линиями на $\frac{n}{2}$ одинаковых прямоугольников и в каждом из них провести диагональ.

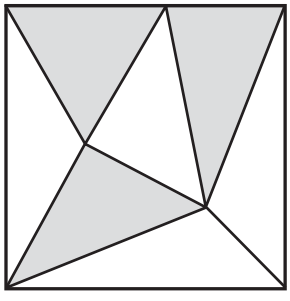


Пусть теперь n нечетно. Даже для $n = 3$ не ясно, как это сделать, и после нескольких попыток возникает мысль о том, что такое разбиение, скорее всего, построить невозможно. Поэтому сформулируем задачу в общем виде.

> *Можно ли разбить квадрат на нечетное число n треугольников одинаковой площади?*

Вопрос выглядит как классическая задача из евклидовой геометрии. Казалось бы, что ответ должен быть давно известен (возможно, даже грекам). Но когда Фред Ричмэн и Джон Томас [3] в 1960 году заинтересовались этой задачей, они к своему удивлению обнаружили, что никто не знает ни ответа, ни статей, в которых она обсуждается.

Так вот: ответ отрицательный не только для $n = 3$, но и для любого нечетного n. Но как доказывать подобное утверждение? Изменяя масштаб, мы можем, конечно, ограничиться единичным квадратом с вершинами $(0,0), (1,0), (0,1), (1,1)$. Следовательно, любое рассуждение должно так или иначе использовать то обстоятельство, что площадь треугольников в разложении квадрата равна $\frac{1}{n}$, где n нечетно. Приведенное ниже гениальное и совершенно неожиданное доказательство нашел Пауль Монски [2] с помощью соображений Джона Томаса [5]. В доказательстве используются алгебраический аппарат и нормирования для построения удивительной раскраски плоскости вместе с некоторыми элегантными и потрясающе простыми комбинаторными рассуждениями. Более того, пока что не предложено никаких других доказательств!



Существуют разбиения квадратов на нечетное число треугольников, площади которых *почти* равны.

Прежде чем формулировать теорему мы приведем краткие сведения о нормах. Всем известна функция абсолютной величины $|x|$, определен-

ная на множестве рациональных чисел $\mathbb{Q}$ (или на множестве действительных чисел $\mathbb{R}$). Она отображает $\mathbb{Q}$ в множество неотрицательных действительных чисел так, что для всех x и y

(i) $|x| = 0$ тогда и только тогда, когда $x = 0$,

(ii) $|xy| = |x||y|$ и

(iii) $|x + y| \le |x| + |y|$ (неравенство треугольника).

Неравенство треугольника превращает $\mathbb{R}$ в метрическое пространство и приводит к известным понятиям сходимости. Около 1900 года было сделано великое открытие: оказалось, что кроме абсолютной величины существуют другие естественные функции на $\mathbb{Q}$, которые удовлетворяют условиям (i)–(iii).

Пусть p — простое число. Любое рациональное число $r \ne 0$ можно единственным образом представить в виде

$$r = p^k \frac{a}{b}, \qquad k \in \mathbb{Z}, \tag{1}$$

где целые a и b положительны и взаимно просты с p. Определим для числа r его *p-адическую величину* (или *p-адическую норму*):

$$|r|_p := p^{-k}, \qquad |0|_p = 0. \tag{2}$$

Условия (i) и (ii) для этой функции очевидно выполняются, а вместо (iii) мы получаем более сильное неравенство

(iii′) $|x + y|_p \le \max\{|x|_p, |y|_p\}$ (неархимедово свойство).

Пример: $\left|\frac{3}{4}\right|_2 = 4$, $\left|\frac{6}{7}\right|_2 = |2|_2 = \frac{1}{2}$ и $\left|\frac{3}{4} + \frac{6}{7}\right|_2 = \left|\frac{45}{28}\right|_2 = \left|\frac{1}{4} \cdot \frac{45}{7}\right|_2 = 4 = \max\left\{\left|\frac{3}{4}\right|_2, \left|\frac{6}{7}\right|_2\right\}$.

Действительно, пусть $r = p^k \frac{a}{b}$ и $s = p^\ell \frac{c}{d}$, причем мы можем предположить, что $k \ge \ell$, т. е. $|r|_p = p^{-k} \le p^{-\ell} = |s|_p$. Тогда

$$|r + s|_p = \left|p^k \frac{a}{b} + p^\ell \frac{c}{d}\right|_p = \left|p^\ell \left(p^{k-\ell}\frac{a}{b} + \frac{c}{d}\right)\right|_p$$
$$= p^{-\ell}\left|\frac{p^{k-\ell}ad + bc}{bd}\right|_p \le p^{-\ell} = \max\{|r|_p, |s|_p\},$$

так как знаменатель bd взаимно прост с p. Отсюда следует также, что

(iv) $|x + y|_p = \max\{|x|_p, |y|_p\}$, если $|x|_p \ne |y|_p$;

далее мы докажем, что это свойство на самом деле вытекает из (iii′).

Любая функция $v : K \to \mathbb{R}_{\ge 0}$, определенная на поле K, для которой при любых $x, y \in K$ выполняются условия

(i) $v(x) = 0$ тогда и только тогда, когда $x = 0$,

(ii) $v(xy) = v(x)v(y)$ и

(iii′) $v(x + y) \le \max\{v(x), v(y)\}$ (неархимедово свойство),

называется *неархимедовой действительной нормой* поля K.

Для каждой такой нормы v мы имеем $v(1) = v(1)v(1)$, так что $v(1) = 1$ и $1 = v(1) = v((-1)(-1)) = [v(-1)]^2$, в силу чего $v(-1) = 1$. Поэтому из (ii) мы получаем, что $v(-x) = v(x)$ для всех x и $v(x^{-1}) = [v(x)]^{-1}$ для $x \geq 0$.

Каждое поле имеет тривиальную норму, которая отображает любой ненулевой элемент поля в 1, и если v — действительная неархимедова норма, то для любого положительного действительного числа t действительной неархимедовой нормой является и v^t. Таким образом, для $\mathbb{Q}$ существуют p-адические нормы и их степени, и известная теорема Островского утверждает, что все нетривиальные действительные неархимедовы нормы поля $\mathbb{Q}$ принадлежат этому классу[1]. Покажем теперь, что важное свойство

(iv) $v(x+y) = \max\{v(x), v(y)\}$, если $v(x) \neq v(y)$,

имеет место для любой неархимедовой нормы. В самом деле, пусть $v(x) < v(y)$. Тогда

$$v(y) = v((x+y)-x) \leq \max\{v(x+y), v(x)\} = v(x+y) \leq \max\{v(x), v(y)\} = v(y),$$

где неравенства вытекают из (iii′) , первое равенство очевидно, а остальные следуют из предположения $v(x) < v(y)$ и первого неравенства. Таким образом, $v(x+y) = v(y) = \max\{v(x), v(y)\}$.

Из свойства (iv) и равенства $v(-x) = v(x)$ также вытекает, что $v(a \pm b_1 \pm b_2 \pm \ldots \pm b_\ell) = v(a)$, если $v(a) > v(b_i)$ для всех i.

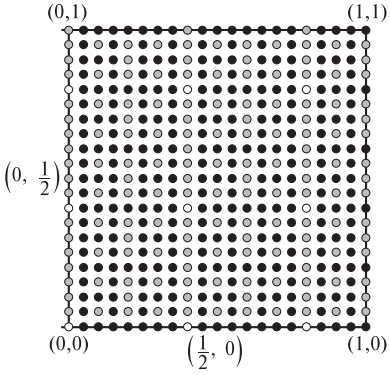
Замечательный подход Монски к решению задачи разбиения квадрата основан на использовании продолжения 2-адичной нормы $|x|_2$ до нормы v поля $\mathbb{R}$, где «продолжение» означает, что равенство $v(x) = |x|_2$ должно выполняться для всех $x \in \mathbb{Q}$. Доказательство существования такого действительного неархимедова продолжения выходит за рамки стандартной алгебры. Далее мы приводим рассуждения Монски в версии Хендрика Ленстры, которая использует лишь норму v, принимающую значения в произвольной «упорядоченной группе» (не обязательно в $(\mathbb{R}_{>0}, \cdot, <)$) и такую, что $v(\frac{1}{2}) > 1$. Определение и доказательство существования такой нормы можно найти в приложении к этой главе.

Здесь мы заметим лишь, что для любой нормы v, для которой $v(\frac{1}{2}) > 1$, имеют место равенства $v(\frac{1}{n}) = 1$ при всех целых нечетных n. Действительно, неравенство $v(\frac{1}{2}) > 1$ означает, что $v(2) < 1$, откуда с помощью (iii′) и индукции по k получаем $v(2k) < 1$. Отсюда и из (iv) следует, что $v(2k+1) = 1$, и поэтому $v(\frac{1}{2k+1}) = 1$ согласно (ii).

Теорема Монски. *Разбить квадрат на нечетное число треугольников равной площади невозможно.*

■ **Доказательство.** Мы построим необычную раскраску точек плоскости тремя красками, имеющую удивительные свойства. Одно из них состоит в том, что площадь любого треугольника, вершины которого раскрашены в три различных цвета (в дальнейшем такие треугольники называются *разноцветными*), имеет v-норму, большую 1, значит, эта площадь не может равняться $\frac{1}{n}$, если n нечетно. Затем мы проверим, что любое разбиение единичного квадрата должно содержать разноцветный треугольник, что завершит доказательство.

[1] Формулировку и доказательство теоремы Островского можно найти в книге В. Л. Ван дер Варден. Алгебра, М.: Наука, 1978, с. 546–548. — *Прим. перев.*



Раскраска точек (x, y) действительной плоскости определяется по элементам тройки $(x, y, 1)$, имеющим максимальное значение нормы v. Максимум может достигаться на одном, двух или даже трех элементах тройки. Цвет точки (x, y) (черный, серый, белый) зависит от первого элемента тройки $(x, y, 1)$, на котором впервые достигается максимальное значение v:

$$\text{цвет точки } (x,y): \begin{cases} \text{черный, если} & v(x) \geq v(y),\ v(x) \geq v(1), \\ \text{серый, если} & v(x) < v(y),\ v(y) \geq v(1), \\ \text{белый, если} & v(x) < v(1),\ v(y) < v(1). \end{cases}$$

Таким образом каждой точке на плоскости приписывается единственный цвет. На полях показаны цвета точек единичного квадрата, координаты которых являются дробями вида $\frac{k}{20}$.

Следующее предложение — первый шаг в доказательстве теоремы Монски.

Лемма 1. *Если $p_b = (x_b, y_b)$ — черная точка, $p_g = (x_g, y_g)$ — серая точка и $p_r = (x_r, y_r)$ — белая точка, то v-норма определителя*

$$\det \begin{pmatrix} x_b & y_b & 1 \\ x_g & y_g & 1 \\ x_r & y_r & 1 \end{pmatrix}$$

не может быть меньше 1.

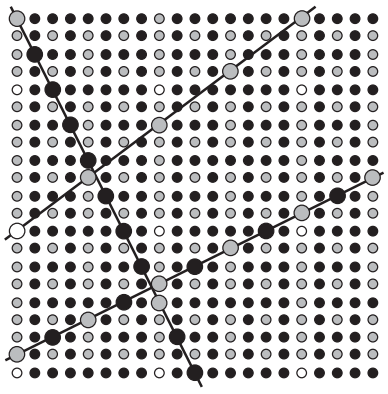
■ **Доказательство.** Определитель равен сумме шести слагаемых. Одно из них есть произведение диагональных элементов $x_b y_g 1$. По построению раскраски значение v-нормы каждого диагонального элемента не меньше v-норм других элементов в этой строке. Поэтому, заменяя v-нормы сомножителей v-нормами последних элементов строк (которые равны 1), мы получаем неравенство

$$v(x_b y_g 1) = v(x_b)v(y_g)v(1) \geq v(1)v(1)v(1) = 1.$$

Каждое из остальных 5 слагаемых определителя — это произведение трех элементов матрицы (взятых по одному из каждой строки) со знаком, который, как мы знаем, не влияет на v-норму. Хотя бы один из этих элементов расположен ниже главной диагонали, и поэтому его v-норма строго меньше v-нормы диагонального элемента той же строки. Кроме того, хотя бы один из этих элементов расположен выше главной диагонали, и поэтому его v-норма не превосходит v-норму диагонального элемента той же строки. Значит, v-нормы всех этих пяти слагаемых строго меньше v-нормы слагаемого, соответствующего главной диагонали. Поэтому, учитывая свойство (iv) неархимедовых норм, мы находим, что v-норма определителя равна v-норме слагаемого, соответствующего главной диагонали:

$$v\left(\det \begin{pmatrix} x_b & y_b & 1 \\ x_g & y_g & 1 \\ x_r & y_r & 1 \end{pmatrix}\right) = v(x_b y_g 1) \geq 1. \qquad \square$$

Следствие. *Любая прямая на плоскости имеет точки не более чем двух цветов. Площадь разноцветного треугольника не может равняться ни нулю, ни $\frac{1}{n}$ при нечетном n.*



■ **Доказательство.** Площадь треугольника с вершинами в черной точке p_b, серой точке p_g и белой точке p_r равна абсолютной величине выражения

$$\tfrac{1}{2}((x_b - x_r)(y_g - y_r) - (x_g - x_r)(y_b - y_r)),$$

которое с точностью до знака есть половина определителя из леммы 1.

Эти три точки не могут лежать на одной прямой, так как если бы определитель был равен нулю, то его норма была бы равна 0. Площадь треугольника не может быть равна $\frac{1}{n}$ при нечетном n, поскольку в этом случае определитель был бы равен $\pm\frac{2}{n}$, и из соотношений $v(\frac{1}{2}) > 1$ и $v(\frac{1}{n}) < 1$ следовало бы неравенство

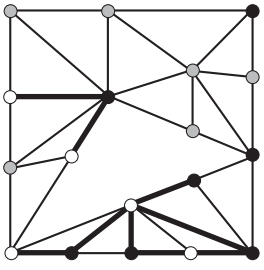
$$v(\pm\tfrac{2}{n}) = [v(\tfrac{1}{2})]^{-1} v(\tfrac{1}{n}) < 1,$$

противоречащее лемме 1. □

Зачем мы построили эту раскраску? Теперь, используя ее, мы покажем, что любое разбиение единичного квадрата $S = [0,1]^2$ на n треугольников (равновеликих или нет!) обязательно содержит разноцветный треугольник, который (согласно следствию) не может иметь площадь $\frac{1}{n}$, если n нечетно. Таким образом, следующая лемма завершает доказательство теоремы Монски.

Лемма 2. *Каждое разбиение единичного квадрата $S = [0,1]^2$ на конечное число треугольников содержит нечетное количество разноцветных треугольников и, следовательно, не менее одного такого треугольника.*

■ **Доказательство.** Следующее перечислительное доказательство в полном смысле этого слова вдохновлено идеей, принадлежащей Эмануэлю Шпернеру (она будет использована еще раз в лемме Шпернера в гл. 25).



Рассмотрим отрезки между соседними вершинами разбиения квадрата на треугольники. Назовем отрезок *черно-белым*, если один конец у него черный, а другой белый. Например, на приведенном выше рисунке черно-белые отрезки выделены жирными линиями.

Сделаем два замечания, используя утверждение из следствия о том, что на каждой прямой точки могут быть окрашены не более чем двумя цветами.

(A) На нижней стороне квадрата имеется *нечетное* число черно-белых отрезков, поскольку точка $(0,0)$ является белой, точка $(1,0)$ — черной, а все вершины между ними либо белые, либо черные. Поэтому при переходе по нижней стороне из белого конца в черный происходит

нечетное число изменений цвета вершин. На других сторонах квадрата черно-белых отрезков нет.

(B) Если вершины треугольника T имеют не более двух цветов, то число черно-белых отрезков на его сторонах *четно*. С другой стороны, на сторонах каждого разноцветного треугольника находится нечетное число черно-белых отрезков. Действительно, между черной и белой вершинами имеется нечетное число черно-белых отрезков, а между вершинами с другими комбинациями цветов — четное число таких отрезков (если они есть). Поэтому разноцветный треугольник имеет нечетное число черно-белых отрезков на своей границе, тогда как любой другой треугольник имеет четное число (2 или 0) пар вершин, одна из которых черная, а другая — белая.

Теперь найдем сумму чисел черно-белых отрезков на сторонах всех треугольников в разбиении квадрата. Так как каждый черно-белый отрезок внутри квадрата считается дважды, а их общее число на сторонах квадрата нечетно, то результат подсчета даст нечетное число. Поэтому, учитывая **(B)**, мы приходим к выводу, что разбиение квадрата должно содержать нечетное число разноцветных треугольников. □

Приложение: Продолжения норм

Совсем не очевидно, что всегда можно продолжить действительную неархимедову норму из одного поля в большее. Но это можно сделать, причем не только для продолжения из $\mathbb{Q}$ в $\mathbb{R}$, но вообще из произвольного поля K в поле L, содержащее K. Это утверждение известно как «теорема Шевалле» (см., например, книгу Джекобсона [1]).

Далее установим значительно более слабое утверждение, но достаточное для нашего применения к нечетным разбиениям квадрата. Действительно, в доказательстве теоремы Монски мы не использовали сложение в множестве значений $v : \mathbb{R} \to \mathbb{R}_{\geq \not\sim}$. Мы использовали лишь умножение и отношение порядка на $\mathbb{R}_{\geq 0}$. Поэтому для нашего доказательства достаточно, чтобы ненулевые значения v содержались в (мультипликативной) упорядоченной абелевой группе $(G, \cdot, <)$. Иными словами, множество элементов G линейно упорядочено и если $a < b$, то $ac < bc$ для всех $a, b, c \in G$. Ввиду предположения о том, что групповая операция — умножение, нейтральный элемент G обозначим 1. Для определения нормы мы введем специальный элемент 0 и будем считать, что для всех $a \in G$ имеют место соотношения $0 \notin G$, $0a = 0$ и $0 < a$. Конечно, простым примером такой упорядоченной абелевой группы является $(\mathbb{R}_{>0}, \cdot, <)$ с обычным линейным порядком, а простым примером для $\{0\} \cup G$ является $(\mathbb{R}_{\geq 0}, \cdot)$.

Определение. Пусть K — поле. *Неархимедова норма v со значениями в упорядоченной абелевой группе G* — это такое отображение $v : K \to \{0\} \cup G$, что для всех $x, y \in K$

(i) $v(x) = 0 \iff x = 0$,
(ii) $v(xy) = v(x)v(y)$,
(iii′) $v(x + y) \leq \max\{v(x), v(y)\}$,
(iv) $v(x + y) = \max\{v(x), v(y)\}$ всякий раз, когда $v(x) \neq v(y)$.

Четвертое условие в этом определении снова вытекает из первых трех. Среди простых следствий отметим такое:

$$\text{если } v(x) < 1,\ x \neq 0,\ \text{то } v(x^{-1}) = [v(x)]^{-1} > 1.$$

Мы докажем следующее утверждение.

Теорема. *В поле действительных чисел $\mathbb{R}$ можно ввести такую неархимедову норму со значениями в упорядоченной абелевой группе*

$$v : \mathbb{R} \to \{0\} \cup G,$$

что $v(\frac{1}{2}) > 1$.

■ **Доказательство.** Сначала установим связь любой нормы поля с подкольцом поля. (Все рассматриваемые нами подкольца содержат 1.) Предположим, что $v : K \to \{0\} \cup G$ — норма. Пусть

$$R := \{x \in K : v(x) \leq 1\},\quad U := \{x \in K : v(x) = 1\}.$$

Немедленно находим, что R — подкольцо K, которое назовем *кольцом нормирования*, соответствующим v.

Более того, из равенства $v(xx^{-1}) = v(1) = 1$ следует, что $v(x) = 1$ тогда и только тогда, когда $v(x^{-1}) = 1$. Следовательно, U — множество единиц (обратимых элементов) R. В частности, U является подгруппой K^*, где $K^* := K \setminus \{0\}$ — мультипликативная группа поля K. Наконец, если $R^{-1} := \{x^{-1} : x \in R \setminus \{0\}\}$, то $K = R \cup R^{-1}$. Действительно, если $x \notin R$, то $v(x) > 1$ и потому $v(x^{-1}) < 1$, так что $x^{-1} \in R$. Свойство $K = R \cup R^{-1}$ полностью характеризует все возможные кольца нормирования в заданном поле.

Лемма. *Собственное подкольцо $R \subseteq K$ является кольцом нормирования по отношению к некоторой норме v со значениями в упорядоченной группе G тогда и только тогда, когда $K = R \cup R^{-1}$.*

■ **Доказательство.** Выше мы показали справедливость леммы в одну сторону. Теперь предположим, что $K = R \cup R^{-1}$. Как нам построить группу G? Если $v : K \to \{0\} \cup G$ — норма, соответствующая R, то отношение $v(x) < v(y)$ имеет место тогда и только тогда, когда $v(xy^{-1}) < 1$, т. е. тогда и только тогда, когда $xy^{-1} \in R \setminus U$. К тому же $v(x) = v(y)$ тогда и только тогда, когда $xy^{-1} \in U$, т. е. $xU = yU$ как смежные классы в факторгруппе K^*/U.

Следовательно, естественный способ продолжить рассуждения состоит в следующем. Возьмем факторгруппу $G := K^*/U$ и определим на G отношение порядка, положив

$$xU < yU \quad :\Longleftrightarrow \quad xy^{-1} \in R \setminus U.$$

(Хорошим упражнением является проверка того, что такое определение действительно превращает G в упорядоченную группу.) Теперь отображение $v : K \to \{0\} \cup G$ определяется самым естественным способом:

$$v(0) = 0 \qquad \text{и} \qquad v(x) := xU \quad \text{при } x \neq 0.$$

Легко проверяются условия (i)–(iii′) для v и то, что R есть кольцо с нормированием, соответствующее v. □

Поэтому для доказательства теоремы достаточно найти такое кольцо нормирования $B \subset \mathbb{R}$, что $\frac{1}{2} \notin B$.

Утверждение. *Максимальное по включению подкольцо $B \subset \mathbb{R}$ есть кольцо нормирования, если $\frac{1}{2} \notin B$.*

$\mathbb{Z} \subset \mathbb{R}$ — подкольцо, и $\frac{1}{2} \notin \mathbb{Z}$, но оно не является максимальным.

Вначале, пожалуй, стоит отметить, что *максимальное* подкольцо $B \subset \mathbb{R}$, для которого $\frac{1}{2} \notin B$, существует.

Это не вполне очевидно, но доказывается с помощью стандартного применения леммы Цорна, приведенной во вставке.

Действительно, если мы имеем неубывающую цепь подколец $B_i \subset \mathbb{R}$, не содержащих $\frac{1}{2}$, то эта цепь имеет верхнюю грань — объединение всех подколец B_i. Оно снова является подкольцом и не содержит $\frac{1}{2}$.

Лемма Цорна

Лемма Цорна имеет фундаментальное значение в алгебре и других областях математики, когда хотят построить максимальную структуру. Она играет также решающую роль в логических основах математики.

Лемма. *Пусть $P_\leq$ — непустое частично упорядоченное множество, в котором каждая неубывающая цепь $(a_i)_\leq$ имеет верхнюю грань b, так что $a_i \leq b$ для всех i. Тогда $P_\leq$ содержит максимальный элемент M, т. е. такой, что не существует элементов $c \in P_\leq$, для которых $M < c$.*

Чтобы доказать Утверждение, предположим, что $B \subset \mathbb{R}$ — максимальное подкольцо, не содержащее $\frac{1}{2}$. Если B не является кольцом нормирования, то существует элемент $\alpha \in \mathbb{R} \setminus (B \cup B_{-1})$. Обозначим через $B[\alpha]$ подкольцо, порождаемое $B \cup \{\alpha\}$, т. е. множество всех действительных чисел, которые можно представить полиномами от α с коэффициентами из B. Пусть $2B \subseteq B$ — совокупность всех элементов вида $2b$, $b \in B$. Так как $2B$ — подмножество B, то $2B[\alpha] \subseteq B[\alpha]$ и $2B[\alpha^{-1}] \subseteq B[\alpha^{-1}]$. Если бы выполнялось хотя бы одно из соотношений $2B[\alpha] \neq B[\alpha]$ или $2B[\alpha^{-1}] \neq B[\alpha^{-1}]$, то ввиду условия $1 \in B$ отсюда следовало бы, что $\frac{1}{2} \notin B[\alpha]$ (соответственно, $\frac{1}{2} \notin B[\alpha^{-1}]$), но это противоречило бы максимальности $B \subset \mathbb{R}$ как подкольца, не содержащего $\frac{1}{2}$. Таким образом, мы получаем, что $2B[\alpha] = B[\alpha]$ и $2B[\alpha^{-1}] = B[\alpha^{-1}]$. Это означает, что условие $1 \in B$ можно записать в виде

$$1 = 2u_0 + 2u_1\alpha + \ldots + 2u_m\alpha^m, \quad \text{где} \ \ u_i \in B, \tag{3}$$

и аналогично

$$1 = 2v_0 + 2v_1\alpha^{-1} + \ldots + 2v_n\alpha^{-n}, \quad \text{где} \ \ v_i \in B. \tag{4}$$

После умножения равенства (4) на α^n и вычитания из обеих его частей $2v_0\alpha^n$ получаем

$$(1 - 2v_0)\alpha^n = 2v_1\alpha^{n-1} + \ldots + 2v_{n-1}\alpha + 2v_n. \tag{5}$$

Допустим, что представления (3) и (4) выбраны так, чтобы m и n были минимально возможными. Предположим также, что $m \geq n$, так как в противном случае мы можем поменять местами α с α^{-1} и (3) с (4).

Теперь умножим (3) на $1 - 2v_0$ и прибавим $2v_0$ к обеим частям полученного равенства:

$$1 = 2(u_0(1 - 2v_0) + v_0) + 2u_1(1 - 2v_0)\alpha + \ldots + 2u_m(1 - 2v_0)\alpha^m.$$

Если в этой формуле заменить $(1-2v_0)\alpha^m$ умноженной на α^{m-n} правой частью (5), то получим выражение элемента $1 \in B$ в виде многочлена из $2B[\alpha]$ степени не более $m - 1$. Это противоречит предположению о минимальности m и доказывает Утверждение. □

Литература

[1] Jacobson N. *Lectures in Abstract Algebra, Part III: Theory of Field and Galois Theory.* Graduate Texts in Mathematics, **32**, Springer, New York, 1975.

[2] Monsky P. *On dividing a square into triangles.* Amer. Math. Monthly, **77** (1970), 161–164.

[3] Richman F., Thomas J. *Problem 5471.* Amer. Math. Monthly, **74** (1967), 329.

[4] Stein S. K., Szabó S. *Algebra and Tiling: Homomorphisms in the Service of Geometry.* Carus Math. Monographs, **25**, MAA, Washington DC, 1994.

[5] Thomas J. *A dissection problem.* Math. Magazine, **41** (1968), 187–190.

Глава 21 Теорема Пойа о многочленах

Дьердь Пойа

Среди многих достижений Пойа в анализе следующий результат восхищал Эрдёша своей необычностью и красотой доказательства. Пусть

$$f(z) \;=\; z^n + b_{n-1}z^{n-1} + \ldots + b_0$$

— многочлен от комплексной переменной z степени $n \geq 1$ со старшим коэффициентом 1. Поставим в соответствие $f(z)$ множество

$$\mathcal{C} \;:=\; \{z \in \mathbb{C} : |f(z)| \leq 2\},$$

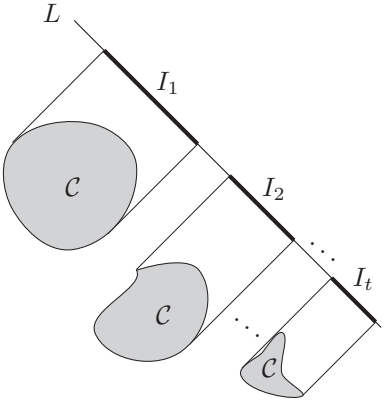
т. е. $\mathcal{C}$ — множество точек, которые f отображает в круг радиуса 2 с центром в нуле комплексной плоскости. Так, при $n = 1$ область $\mathcal{C}$ есть просто круг диаметра 4.

С помощью изумительно простого рассуждения Пойа установил следующее замечательное свойство множества $\mathcal{C}$:

> *Возьмем произвольную прямую L в комплексной плоскости и рассмотрим ортогональную проекцию $\mathcal{C}_L$ множества $\mathcal{C}$ на L. Тогда общая длина любой такой проекции никогда не превосходит* 4.

Что здесь понимается под общей длиной проекции $\mathcal{C}_L$? Мы увидим, что $\mathcal{C}_L$ — объединение конечного числа непересекающихся интервалов $I_1, \ldots, I_t$, и утверждение означает, что $\ell(I_1) + \ldots + \ell(I_t) \leq 4$, где $\ell(I_j)$ — обычная длина интервала I_i.

Вращение плоскости позволяет свести утверждение к случаю, когда L — вещественная ось в комплексной плоскости. Имея в виду эти замечания, сформулируем результат Пойа.



Теорема 1. *Пусть $f(z)$ — многочлен от комплексной переменной степени $n \geq 1$ со старшим коэффициентом 1 и $\mathcal{C} = \{z \in \mathbb{C} : |f(z)| \leq 2\}$. Пусть, далее, $\mathcal{R}$ — ортогональная проекция множества $\mathcal{C}$ на вещественную ось. Тогда существуют такие интервалы $I_1, \ldots, I_t$ на вещественной прямой, в совокупности покрывающие $\mathcal{R}$, что*

$$\ell(I_1) + \ldots + \ell(I_t) \;\leq\; 4.$$

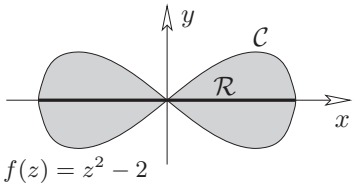
Ясно, что оценка 4 теоремы достигается для $n = 1$. Чтобы лучше почувствовать задачу, рассмотрим многочлен $f(z) = z^2 - 2$; для него оценка 4 достигается. Если $z = x + iy$ — комплексное число, то x — его ортогональная проекция на вещественную ось. Значит,

$$\mathcal{R} = \{x \in \mathbb{R} : x + iy \in \mathcal{C} \text{ для некоторого } y\}.$$

Читатель может легко доказать, что если $f(z) = z^2 - 2$, то $x + iy \in \mathcal{C}$ тогда и только тогда, когда

$$(x^2 + y^2)^2 \;\leq\; 4(x^2 - y^2).$$

Отсюда следует, что $x^4 \le (x^2+y^2)^2 \le 4x^2$, и поэтому $x^2 \le 4$, т. е. $|x| \le 2$. С другой стороны, если $z = x \in \mathbb{R}$ и $|x| \le 2$, то $|z^2-2| \le 2$, и мы находим, что $\mathcal{R}$ есть в точности интервал $[-2,2]$ длины 4.

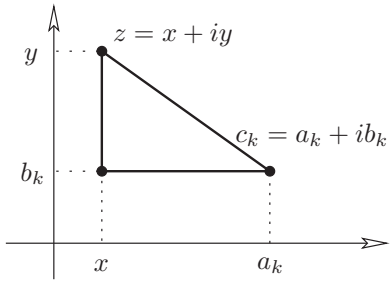


В качестве первого шага к доказательству используем равенство $f(z) = (z-c_1)\cdots(z-c_n)$, где $c_k = a_k + ib_k$ — корни $f(z)$, и рассмотрим многочлен от *вещественной* переменной $p(x) = (x-a_1)\cdots(x-a_n)$. Пусть $z = x+iy \in \mathcal{C}$. Тогда по теореме Пифагора

$$|x-a_k|^2 + |y-b_k|^2 = |z-c_k|^2,$$

так что $|x-a_k| \le |z-c_k|$ для всех k, т. е.

$$|p(x)| \;=\; |x-a_1|\cdots|x-a_n| \;\le\; |z-c_1|\cdots|z-c_n| \;=\; |f(z)| \le 2.$$



Таким образом, $\mathcal{R}$ содержится в множестве $\mathcal{P} = \{x \in \mathbb{R} : |p(x)| \le 2\}$, и задача будет решена, если показать, что множество $\mathcal{P}$ покрывается интервалами, суммарная длина которых не больше 4. Поэтому наша основная теорема 1 вытекает из следующего утверждения.

Теорема 2. *Пусть $p(x)$ — вещественный многочлен степени $n \ge 1$ со старшим коэффициентом, равным 1, и все его корни действительны. Тогда множество $\mathcal{P} = \{x \in \mathbb{R} : |p(x)| \le 2\}$ можно покрыть интервалами, общая длина которых не превосходит 4.*

В свою очередь, теорема 2, как показал Пойа в своей статье [2], есть следствие замечательного результата, принадлежащего Чебышёву. Чтобы сделать эту главу замкнутой, мы включим в качестве приложения доказательство теоремы Чебышёва, следуя при этом прекрасному изложению Пойа и Сеге.

Теорема Чебышёва. *Пусть $p(x)$ — вещественный многочлен степени $n \ge 1$ со старшим коэффициентом 1. Тогда*

$$\max_{-1\le x\le 1} |p(x)| \;\ge\; \frac{1}{2^{n-1}}\,.$$

Пафнутий Чебышёв на советской марке 1946 года

Отметим непосредственное следствие из теоремы Чебышёва.

Следствие. *Пусть $p(x)$ — вещественный многочлен степени $n \ge 1$ со старшим коэффициентом 1. Если $|p(x)| \le 2$ для всех x в интервале $[a,b]$, то $b-a \le 4$.*

■ **Доказательство.** Замена $y = \frac{2}{b-a}(x-a) - 1$ отображает x-интервал $[a,b]$ в y-интервал $[-1,1]$. Старший коэффициент многочлена

$$q(y) \;=\; p\left(\tfrac{b-a}{2}(y+1)+a\right)$$

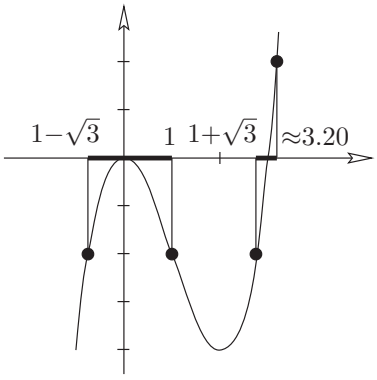
равен $(\frac{b-a}{2})^n$; кроме того,

$$\max_{-1\le y\le 1} |q(y)| \;=\; \max_{a\le x\le b} |p(x)|.$$

Согласно теореме Чебышёва

$$2 \ge \max_{a\le x\le b} |p(x)| \ge\; (\tfrac{b-a}{2})^n \tfrac{1}{2^{n-1}} \;=\; 2(\tfrac{b-a}{4})^n,$$

поэтому $b-a \le 4$, что и требовалось доказать. □



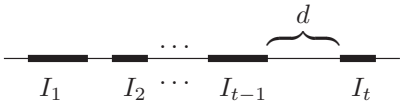
Если $p(x) = x^2(x-3)$, то $\mathcal{P} = [1-\sqrt{3}, 1] \cup [1+\sqrt{3}, \approx 3.2]$

Следствие подводит нас совсем близко к утверждению теоремы 2. Если множество $\mathcal{P} = \{x : |p(x)| \le 2\}$ — *интервал*, то длина $\mathcal{P}$ не больше 4. Однако множество $\mathcal{P}$ может не быть интервалом, как в указанном на полях примере, где $\mathcal{P}$ состоит из двух интервалов.

Что можно сказать о $\mathcal{P}$? Так как $p(x)$ — непрерывная функция, то $\mathcal{P}$ есть объединение непересекающихся замкнутых интервалов $I_1, I_2, \ldots$, и $p(x)$ принимает значения 2 или -2 в каждом из концов интервала I_j. Это означает, что число интервалов $I_1, \ldots, I_t$ конечно, поскольку $p(x)$ может принимать любое значение лишь конечное число раз.

Замечательная идея Пойа состояла в том, чтобы построить другой многочлен $\tilde{p}(x)$ степени n со старшим коэффициентом 1, для которого $\widetilde{\mathcal{P}} = \{x : |\tilde{p}(x)| \le 2\}$ есть *интервал* длины не меньше $\ell(I_1) + \ldots + \ell(I_t)$. Тогда в силу следствия $\ell(I_1) + \ldots + \ell(I_t) \le \ell(\widetilde{\mathcal{P}}) \le 4$, что и требуется.

■ **Доказательство теоремы 2.** Пусть $p(x) = (x-a_1)\cdots(x-a_n)$ — многочлен, для которого $\mathcal{P} = \{x \in \mathbb{R} : |p(x)| \le 2\} = I_1 \cup \ldots \cup I_t$, причем интервалы I_j расположены так, что I_1 — самый левый, а I_t — самый правый интервал. Прежде всего мы покажем, что любой интервал I_j содержит корень $p(x)$. Мы знаем, что $p(x)$ принимает значения 2 или -2 в концевых точках I_j. Если одно значение равно 2, а другое -2, то в I_j, несомненно, существует корень. Поэтому предположим, что $p(x) = 2$ в обеих концевых точках (случай $p(x) = -2$ рассматривается аналогично). Пусть $b \in I_j$ — точка, в которой достигается минимум $p(x)$ в I_j. Тогда $p'(b) = 0$ и $p''(b) \ge 0$. Если $p''(b) = 0$, то b является кратным корнем $p'(x)$ и, следовательно, корнем $p(x)$ ввиду факта 1 из вставки на стр. 153. Если, с другой стороны, $p''(b) > 0$, то согласно факту 2 из той же вставки, $p(b) \le 0$. Таким образом, либо $p(b) = 0$ и b — искомый корень, либо $p(b) < 0$ и существует корень в интервале между b и одной из двух концевых точек.



Мы подошли к завершающей идее доказательства. Пусть $I_1, \ldots, I_t$ — определенные выше интервалы. Предположим, что самый правый интервал I_t содержит (с учетом кратностей) m корней $p(x)$. Если $m = n$, то в силу только что доказанного нами I_t является единственным интервалом, и доказательство завершено. Поэтому предположим, что $m < n$; пусть d — длина промежутка между I_{t-1} и I_t (см. рис. на полях). Пусть, далее, $b_1, \ldots, b_m$ — корни $p(x)$, принадлежащие I_t, и $c_1, \ldots, c_{n-m}$ — оставшиеся корни. Тогда $p(x) = q(x)r(x)$, где $q(x) = (x-b_1)\cdots(x-b_m)$ и $r(x) = (x-c_1)\cdots(x-c_{n-m})$; положим $p_1(x) = q(x+d)r(x)$. Многочлен $p_1(x)$ тоже имеет степень n и старший коэффициент, равный единице. При $x \in I_1 \cup \ldots \cup I_{t-1}$ для всех $i = 1, \ldots, m$ имеем $|x+d-b_i| < |x-b_i|$ и, следовательно, $|q(x+d)| < |q(x)|$. Отсюда вытекает, что

$$|p_1(x)| \;\le\; |p(x)| \;\le\; 2 \qquad \text{при } \; x \in I_1 \cup \ldots \cup I_{t-1}.$$

С другой стороны, если $x \in I_t$, то $|r(x-d)| \le |r(x)|$, в силу чего

$$|p_1(x-d)| \;=\; |q(x)||r(x-d)| \;\le\; |p(x)| \;\le\; 2;$$

это означает, что $I_t - d \subseteq \mathcal{P}_1 = \{x : |p_1(x)| \le 2\}$.

Свойства многочленов с вещественными корнями

Пусть $p(x)$ — отличный от константы многочлен степени n, имеющий лишь вещественные корни.

Факт 1. *Если b — кратный корень $p'(x)$, то b тоже является корнем $p(x)$.*

■ **Доказательство.** Пусть $b_1 \le \ldots \le b_r$ — корни $p(x)$, имеющие кратности $s_1, \ldots, s_r$, так что $\sum_{j=1}^{r} s_j = n$. Если $s_j \ge 2$, то $p(x) = (x-b_j)^{s_j} h_j(x)$; поэтому b_j является корнем $p'(x)$ и кратность b_j как корня $p'(x)$ есть $s_j - 1$. Далее, $p'(x)$ имеет корень между b_1 и b_2, другой корень между b_2 и b_3,..., корень между b_{r-1} и b_r, и все они имеют *единичную* кратность, так как сумма $\sum_{j=1}^{r}(s_j - 1) + (r-1)$ равна $n-1$, т. е. степени $p'(x)$. Значит, *кратные* корни многочлена $p'(x)$ должны быть корнями $p(x)$. □

Факт 2. *Неравенство $p'(x)^2 \ge p(x)p''(x)$ выполняется для всех $x \in \mathbb{R}$.*

■ **Доказательство.** Если $x = a_i$ — некоторый корень $p(x)$, то неравенство верно. Предположим, что x — не корень $p(x)$. По правилу дифференцирования произведения

$$p'(x) \;=\; \sum_{k=1}^{n} \frac{p(x)}{x-a_k}, \quad \text{т. е.} \quad \frac{p'(x)}{p(x)} \;=\; \sum_{k=1}^{n} \frac{1}{x-a_k}.$$

Еще раз дифференцируя, получаем

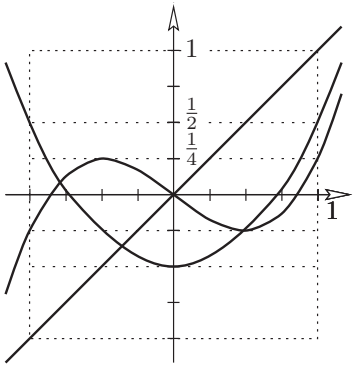
$$\frac{p''(x)p(x) - p'(x)^2}{p(x)^2} \;=\; -\sum_{k=1}^{n} \frac{1}{(x-a_k)^2} \;<\; 0. \qquad \square$$

Значит, множество $\mathcal{P}_1$ содержит $I_1 \cup \ldots \cup I_{t-1} \cup (I_t - d)$ и поэтому его суммарная длина не меньше, чем у $\mathcal{P}$. Заметим теперь, что при переходе от $p(x)$ к $p_1(x)$ интервалы I_{t-1} и $I_t - d$ сливаются в один. Поэтому составляющие $\mathcal{P}_1$ интервалы $J_1, \ldots, J_s$, в которых $|p_1(x)| \le 2$, имеют в сумме длину не менее $\ell(I_1) + \ldots + \ell(I_t)$, и самый правый интервал J_s содержит больше m корней $p_1(x)$. Повторяя эту процедуру не более $m-1$ раз, в конце концов получим многочлен $\tilde{p}(x)$, для которого $\widetilde{\mathcal{P}} = \{x : |\tilde{p}(x)| \le 2\}$ будет интервалом длины $\ell(\widetilde{\mathcal{P}}) \ge \ell(I_1) + \ldots \ell(I_t)$, и доказательство завершено. □

Приложение: теорема Чебышёва

Теорема. *Пусть $p(x)$ — вещественный многочлен степени $n \ge 1$ со старшим коэффициентом 1. Тогда*

$$\max_{-1 \le x \le 1} |p(x)| \;\ge\; \frac{1}{2^{n-1}}\,.$$



Многочлены $p_1(x) = x$, $p_2(x) = x^2 - \frac{1}{2}$ и $p_3(x) = x^3 - \frac{3}{4}x$, для которых достигается равенство в теореме Чебышёва.

Прежде чем приступить к доказательству, рассмотрим несколько примеров. На полях приведены графики многочленов степеней 1, 2 и 3, для каждого из которых в теореме Чебышёва выполняется равенство. Мы увидим, что на самом деле для каждой степени существует ровно один многочлен, для которого в оценке теоремы достигается равенство.

■ **Доказательство.** Пусть $p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ — вещественный многочлен со старшим коэффициентом 1. Так как мы интересуемся промежутком $-1 \le x \le 1$, сделаем замену $x = \cos\vartheta$ и обозначим через $g(\vartheta) := p(\cos\vartheta)$ получающийся многочлен от $\cos\vartheta$:

$$g(\vartheta) = (\cos\vartheta)^n + a_{n-1}(\cos\vartheta)^{n-1} + \ldots + a_0. \tag{1}$$

Доказательство проводится в два шага. Оба они являются классическими результатами и представляют самостоятельный интерес.

(A) Если представить $g(\vartheta)$ в виде *многочлена по косинусам*,

$$g(\vartheta) \;=\; b_n\cos n\vartheta + b_{n-1}\cos(n-1)\vartheta + \ldots + b_1\cos\vartheta + b_0, \tag{2}$$

где $b_k \in \mathbb{R}$, то его старший коэффициент $b_n = \frac{1}{2^{n-1}}$.

(B) Для произвольного многочлена по косинусам степени n

$$h(\vartheta) \;=\; \lambda_n\cos n\vartheta + \lambda_{n-1}\cos(n-1)\vartheta + \ldots + \lambda_0 \tag{3}$$

справедлива оценка $|\lambda_n| \le \max|h(\vartheta)|$.

Применение неравенства (3) к $g(\vartheta)$ дает утверждение теоремы.

Доказательство (A). Чтобы перейти от (1) к представлению (2), представим все степени $(\cos y)^k$ в виде многочленов по косинусам. Например, теорема сложения для косинусов дает

$$\cos 2\vartheta \;=\; \cos^2\vartheta - \sin^2\vartheta \;=\; 2\cos^2\vartheta - 1,$$

так что $\cos^2\vartheta = \frac{1}{2}\cos 2\vartheta + \frac{1}{2}$. В случае произвольной степени $(\cos\vartheta)^k$ перейдем к комплексным числам, используя соотношение $e^{ix} = \cos x + i\sin x$; величины e^{ix} являются комплексными числами, абсолютные значения которых равны 1 (см. вставку на с. 43 о комплексных корнях из единицы). В частности, отсюда получаем

$$e^{in\vartheta} \;=\; \cos n\vartheta + i\sin n\vartheta. \tag{4}$$

С другой стороны,

$$e^{in\vartheta} \;=\; (e^{i\vartheta})^n \;=\; (\cos\vartheta + i\sin\vartheta)^n. \tag{5}$$

Приравнивая вещественные части в (4) и (5) и учитывая, что $i^{4\ell+2} = -1$, $i^{4\ell} = 1$ и $\sin^2\theta = 1 - \cos^2\theta$, находим

$$\begin{aligned}\cos n\vartheta \;=\; &\sum_{\ell\ge 0}\binom{n}{4\ell}(\cos\vartheta)^{n-4\ell}(1-\cos^2\vartheta)^{2\ell} - \\ &-\sum_{\ell\ge 0}\binom{n}{4\ell+2}(\cos\vartheta)^{n-4\ell-2}(1-\cos^2\vartheta)^{2\ell+1}.\end{aligned} \tag{6}$$

Таким образом, $\cos n\vartheta$ — многочлен от $\cos\vartheta$ степени n:

$$\cos n\vartheta \;=\; c_n(\cos\vartheta)^n + c_{n-1}(\cos\vartheta)^{n-1} + \ldots + c_0, \qquad (7)$$

и из (6) легко найти его старший коэффициент:

$$c_n \;=\; \sum_{\ell\ge 0}\binom{n}{4\ell} + \sum_{\ell\ge 0}\binom{n}{4\ell+2} \;=\; 2^{n-1}.$$

$\sum_{k\ge 0}\binom{n}{2k} = 2^{n-1}$ при $n > 0$: Любому подмножеству множества $\{1,2,\ldots,n-1\}$ соответствует ровно одно подмножество множества $\{1,2,\ldots,n\}$ *четного* объема (элемент n добавляется, если необходимо).

Теперь обратим наше рассуждение. Предполагая по индукции, что при любом $k < n$ можно представить $(\cos\vartheta)^k$ в виде многочлена по косинусам степени k, выводим из формулы (7), что $(\cos\vartheta)^n$ можно представить в виде многочлена по косинусам степени n со старшим коэффициентом $b_n = \frac{1}{2^{n-1}}$.

Доказательство (B). Пусть $h(\vartheta)$ — многочлен по косинусам степени n из формулы (3); без ограничения общности будем считать, что $\lambda_n > 0$. Полагая $m(\vartheta) := \lambda_n \cos n\vartheta$, находим, что

$$m(\tfrac{k}{n}\pi) \;=\; (-1)^k\lambda_n \qquad \text{при} \quad k = 0,1,\ldots,n.$$

Допустим противное: $\max|h(\vartheta)| < \lambda_n$. Тогда разность

$$m(\tfrac{k}{n}\pi) - h(\tfrac{k}{n}\pi) \;=\; (-1)^k\lambda_n - h(\tfrac{k}{n}\pi)$$

положительна при четных k и отрицательна при нечетных k в отрезке $0 \le k \le n$. Следовательно, $m(\vartheta) - h(\vartheta)$ имеет не менее n корней в отрезке $[0,\pi]$. Но это невозможно, поскольку $m(\vartheta) - h(\vartheta)$ — многочлен по косинусам степени $n-1$, который поэтому имеет не более $n-1$ корней.

Доказательство п.(B) и теоремы Чебышёва завершено. □

Теперь читатель может легко дополнить анализ, показав, что $g_n(\vartheta) = \frac{1}{2^{n-1}}\cos n\vartheta$ является *единственным* многочленом по косинусам степени n со старшим коэффициентом 1, удовлетворяющим условию $\max|g(\vartheta)| = \frac{1}{2^{n-1}}$.

Многочлены $T_n(x) = \cos n\vartheta$, $x = \cos\vartheta$, называются *многочленами Чебышёва* (первого рода); таким образом $\frac{1}{2^{n-1}}T_n(x)$ — единственный нормированный многочлен[1] степени n, для которого справедливо равенство в теореме Чебышёва.

Литература

[1] Chebyshev P. L. *Œuvres,* Vol. I, Acad. Imperiale des Sciences, St. Petersburg, 1899, pp. 387–469. [Русский перевод: Чебышёв П. Л. *О функциях, наименее уклоняющихся от нуля.* Избр. труды, М., изд-во АН СССР, 1955, с. 579–608.]

[2] Pólya G. *Beitrag zur Verallgemeinerung des Verzerrungssatzes auf mehrfach zusammenhängenden Gebieten,* Sitzungsber. Preuss. Akad. Wiss. Berlin, 1928, 228–232; Collected Papers, Vol. I, MIT Press, 1974, 347–351.

[3] Pólya G., Szegő G. *Problems and Theorems in Analysis, Vol. II.* Springer-Verlag, Berlin–Heidelberg–New York, 1976; Reprint 1998. [Русский перевод: Полиа Г., Сеге Г. *Задачи и теоремы из анализа, т.2.* М., ГИТТЛ, 1956.]

[1] Нормированным называется многочлен, старший коэффициент которого равен 1. — *Прим. перев.*

Глава 22 О лемме Литтлвуда и Оффорда

Джон И. Литтлвуд

В своей работе [5] о распределении корней алгебраических уравнений Литтлвуд и Оффорд в 1943 году доказали следующее утверждение:

Пусть $a_1, a_2, \dots, a_n$ — комплексные числа и $|a_i| \geq 1$ для всех i. Рассмотрим 2^n линейных комбинаций $\sum_{i=1}^n \varepsilon_i a_i$, где $\varepsilon_i \in \{1, -1\}$. Тогда число сумм $\sum_{i=1}^n \varepsilon_i a_i$, лежащих в любом круге радиуса 1, не превосходит

$$c\,\frac{2^n}{\sqrt{n}}\log n \quad \textit{при некоторой константе } c > 0.$$

Несколько лет спустя Пауль Эрдёш [1] уточнил эту оценку, устранив множитель $\log n$, и, что более интересно, показал, что она по сути является простым следствием теоремы Шпернера (см. с. 189).

Чтобы упростить рассуждения Эрдёша, рассмотрим случай, когда все a_i действительны. Можно предполагать, что все a_i положительны (если $a_i < 0$, то можно заменить a_i на $-a_i$ и ε_i на $-\varepsilon_i$). Далее предположим, что какое-то множество сумм $\sum \varepsilon_i a_i$ находится внутри некоторого интервала длины 2. Пусть $N = \{1, 2, \dots, n\}$ — множество индексов. Для каждой суммы $\sum \varepsilon_i a_i$ положим $I := \{i \in N : \varepsilon_i = 1\}$. Если множество $I' = \{i \in N :\ \varepsilon'_i = 1\}$ соответствует сумме $\sum \varepsilon'_i a_i$ и $I \subset I'$, $I \neq I'$, то

$$\sum \varepsilon'_i a_i - \sum \varepsilon_i a_i \;=\; 2 \sum_{i \in I' \setminus I} a_i \;\geq\; 2,$$

т. е. суммы, соответствующие множествам I и I', $I \subset I'$, не могут находиться в одном интервале длины 2. Значит, множества I, для которых суммы $\sum \varepsilon_i a_i$ попадают в один и тот же интервал длины 2, образуют антицепь, и из теоремы Шпернера следует, что имеется не более $\binom{n}{\lfloor n/2 \rfloor}$ таких множеств. Согласно формуле Стирлинга (см. с. 19)

$$\binom{n}{\lfloor n/2 \rfloor} \;\leq\; c\,\frac{2^n}{\sqrt{n}} \quad \text{для некоторого } c > 0.$$

Если n четно и все $a_i = 1$, то существует $\binom{n}{n/2}$ комбинаций $\sum_{i=1}^n \varepsilon_i a_i$, равных нулю. Рассматривая интервал $(-1, 1)$, мы, таким образом, находим, что биномиальный коэффициент дает *точную* оценку сверху.

В той же статье Эрдёш предположил, что $\binom{n}{\lfloor n/2 \rfloor}$ — точная оценка и в случае комплексных чисел a_i (он смог получить в качестве оценки сверху лишь величину $c\,2^n n^{-1/2}$ при некотором $c > 0$) и что та же самая оценка справедлива для векторов $\boldsymbol{a}_1, \dots, \boldsymbol{a}_n$ с $|\boldsymbol{a}_i| \geq 1$ из вещественного гильбертова пространства, если круг радиуса 1 заменить открытым шаром радиуса 1.

Семейство подмножеств конечного множества — *антицепь*, если в нем нет двух таких подмножеств, что одно из них содержит другое.

Теорема Шпернера. *Любая антицепь подмножеств n-множества содержит не более $\binom{n}{\lfloor n/2 \rfloor}$ элементов.*

Эрдёш был прав, но только через 20 лет Дьюла Катона [2] и Даниэль Клейтман [3] независимо доказали его гипотезу для комплексных чисел (или, что то же самое, для плоскости $\mathbb{R}^2$). Их доказательства неявно использовали двумерность плоскости, и было не совсем ясно, допускают ли они обобщения на конечномерные вещественные векторные пространства.

Наконец, в 1970 году Клейтман [4] полностью доказал гипотезу Эрдёша о гильбертовых пространствах, использовав рассуждения ошеломляющей простоты. В действительности он доказал даже больше. Его доказательство — образец того, как важно найти правильное предположение индукции.

Чтобы успокоить читателей, не знакомых с понятием гильбертова пространства, заметим, что общее гильбертово пространство нам не потребуется. Так как мы имеем дело с конечными множествами векторов a_i, то достаточно рассматривать вещественное пространство $\mathbb{R}^d$ с обычным скалярным произведением.

Сформулируем результат Клейтмана.

Теорема. *Пусть $\boldsymbol{a}_1, \dots, \boldsymbol{a}_n$ — векторы в $\mathbb{R}^d$, длина каждого из которых не меньше 1, и $R_1, \dots, R_k$ — такие открытые области в $\mathbb{R}^d$, что $|\boldsymbol{x} - \boldsymbol{y}| < 2$ для любых $\boldsymbol{x}, \boldsymbol{y}$, принадлежащих одной и той же области R_i. Тогда число линейных комбинаций $\sum_{i=1}^n \varepsilon_i \boldsymbol{a}_i$, $\varepsilon_i \in \{1, -1\}$, которые принадлежат объединению областей $\bigcup_i R_i$, не превосходит суммы k наибольших биномиальных коэффициентов $\binom{n}{j}$.*
В частности, при $k = 1$ это число не превосходит $\binom{n}{\lfloor n/2 \rfloor}$.

Прежде чем перейти к доказательству, заметим, что оценка достигается для векторов

$$\boldsymbol{a}_1 = \dots = \boldsymbol{a}_n = \boldsymbol{a} = (1, 0, \dots, 0)^T.$$

В самом деле, для четного n существует $\binom{n}{n/2}$ сумм, равных 0, $\binom{n}{n/2-1}$ сумм, равных $(-2)\boldsymbol{a}$, $\binom{n}{n/2+1}$ сумм, равных $2\boldsymbol{a}$, и т. д. Выбрав шары радиуса 1 с центрами в точках

$$-2\lceil \tfrac{k-1}{2} \rceil \boldsymbol{a}, \quad \dots \quad (-2)\boldsymbol{a}, \quad \mathbf{0}, \quad 2\boldsymbol{a}, \quad \dots \quad 2\lfloor \tfrac{k-1}{2} \rfloor \boldsymbol{a},$$

мы получаем

$$\binom{n}{\lfloor \frac{n-k+1}{2} \rfloor} + \dots + \binom{n}{\frac{n-2}{2}} + \binom{n}{\frac{n}{2}} + \binom{n}{\frac{n+2}{2}} + \dots + \binom{n}{\lfloor \frac{n+k-1}{2} \rfloor}$$

сумм, лежащих в этих k шарах, что совпадает с указанным в теореме значением, так как наибольшие биномиальные коэффициенты сосредоточены около середины (см. с. 20).

Аналогичное рассуждение работает и для нечетных n.

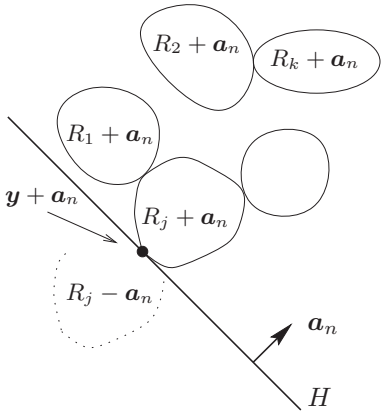
■ **Доказательство.** Без потери общности будем предполагать, что области R_i не пересекаются. Ключ к доказательству — рекуррентное соотношение для биномиальных коэффициентов, показывающее, как связаны наибольшие биномиальные коэффициенты для n и $n - 1$. Положим

$r = \lfloor \frac{n-k+1}{2} \rfloor, s = \lfloor \frac{n+k-1}{2} \rfloor$, тогда $\binom{n}{r}, \binom{n}{r+1}, \ldots, \binom{n}{s}$ суть k наибольших биномиальных коэффициентов для n. Из тождества $\binom{n}{i} = \binom{n-1}{i} + \binom{n-1}{i-1}$ следует, что

$$\begin{aligned} \sum_{i=r}^{s} \binom{n}{i} &= \sum_{i=r}^{s} \binom{n-1}{i} + \sum_{i=r}^{s} \binom{n-1}{i-1} \\ &= \sum_{i=r}^{s} \binom{n-1}{i} + \sum_{i=r-1}^{s-1} \binom{n-1}{i} \qquad (1) \\ &= \sum_{i=r-1}^{s} \binom{n-1}{i} + \sum_{i=r}^{s-1} \binom{n-1}{i}, \end{aligned}$$

и легко проверить, что первая и вторая суммы содержат $k+1$ и $k-1$ наибольших биномиальных коэффициентов соответственно.

В доказательстве Клейтмана используется индукция по n; случай $n = 1$ тривиален. В силу (1) для обоснования шага индукции достаточно показать, что множество линейных комбинаций векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$, попадающих в k непересекающихся областей, можно *взаимно однозначно* отобразить в множество комбинаций $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{n-1}$, попадающих в $k+1$ или в $k-1$ областей.



Утверждение. *По крайней мере для одного $j \in \{1, \ldots, k\}$ сдвиг $R_j - \boldsymbol{a}_n$ области R_j не пересекается ни с одним из сдвигов $R_1 + \boldsymbol{a}_n, \ldots, R_k + \boldsymbol{a}_n$.*

Чтобы доказать это утверждение, рассмотрим такую гиперплоскость $H = \{\boldsymbol{x} : \langle \boldsymbol{a}_n, \boldsymbol{x} \rangle = c\}$, ортогональную вектору $\boldsymbol{a}_n$, что все сдвиги $R_i + \boldsymbol{a}_n$ расположены по одну сторону от H (определяемую неравенством $\langle \boldsymbol{a}_n, \boldsymbol{x} \rangle \geq c$) и что H касается замыкания сдвига одной из областей, например, $R_j + \boldsymbol{a}_n$. Такая гиперплоскость существует, поскольку все области $R_1, \ldots, R_k$ ограничены. Далее, $|\boldsymbol{x} - \boldsymbol{y}| < 2$ для любых $\boldsymbol{x} \in R_j$ и $\boldsymbol{y}$ из замыкания области R_j (так как R_j открыто). Покажем, что $R_j - \boldsymbol{a}_n$ лежит по другую сторону от H.

Допустим противное: $\langle \boldsymbol{a}_n, \boldsymbol{x} - \boldsymbol{a}_n \rangle \geq c$ для некоторого $x \in R_j$, или, что то же, $\langle \boldsymbol{a}_n, \boldsymbol{x} \rangle \geq |\boldsymbol{a}_n|^2 + c$. Если $\boldsymbol{y} + \boldsymbol{a}_n$ — точка, в которой H касается $R_j + \boldsymbol{a}_n$, то $\boldsymbol{y}$ принадлежит замыканию области R_j и $\langle \boldsymbol{a}_n, \boldsymbol{y} + \boldsymbol{a}_n \rangle = c$, т. е. $\langle \boldsymbol{a}_n, -\boldsymbol{y} \rangle = |\boldsymbol{a}_n|^2 - c$. Поэтому в силу нашего предположения

$$\langle \boldsymbol{a}_n, \boldsymbol{x} - \boldsymbol{y} \rangle \;\geq\; 2|\boldsymbol{a}_n|^2,$$

а из неравенства Коши–Буняковского–Шварца вытекает, что

$$2|\boldsymbol{a}_n|^2 \;\leq\; \langle \boldsymbol{a}_n, \boldsymbol{x} - \boldsymbol{y} \rangle \;\leq\; |\boldsymbol{a}_n||\boldsymbol{x} - \boldsymbol{y}|;$$

так как $|\boldsymbol{a}_n| \geq 1$, то $2 \;\leq\; 2|\boldsymbol{a}_n| \;\leq\; |\boldsymbol{x} - \boldsymbol{y}|$, и полученное противоречие доказывает справедливость утверждения.

Остальное просто. Сгруппируем комбинации $\sum \varepsilon_i \boldsymbol{a}_i$, попавшие в $R_1 \cup \ldots \cup R_k$, следующим образом. В класс 1 включим все $\sum_{i=1}^{n} \varepsilon_i \boldsymbol{a}_i$ с $\varepsilon_n = -1$ и все попавшие в R_j комбинации $\sum_{i=1}^{n} \varepsilon_i \boldsymbol{a}_i$ с $\varepsilon_n = 1$. В класс 2 включим все оставшиеся комбинации с $\varepsilon_n = 1$, не попавшие в R_j.

Тогда все комбинации $\sum_{i=1}^{n} \varepsilon_i \boldsymbol{a}_i$ из класса 1 принадлежат $k+1$ непересекающимся областям $R_1 + \boldsymbol{a}_n, \ldots, R_k + \boldsymbol{a}_n$ и $R_j - \boldsymbol{a}_n$, а комбинации $\sum_{i=1}^{n-1} \varepsilon_i \boldsymbol{a}_i$ из класса 2 принадлежат $k-1$ непересекающимся областям $R_1 - \boldsymbol{a}_n, \ldots, R_k - \boldsymbol{a}_n$, отличным от $R_j - \boldsymbol{a}_n$. По предположению индукции класс 1 содержит не более $\sum_{i=r-1}^{s} \binom{n-1}{i}$ комбинаций, а класс 2 — не более $\sum_{i=r}^{s-1} \binom{n-1}{i}$ комбинаций. В силу (1) это завершает доказательство, несомненно, взятое прямо из Книги. □

Литература

[1] Erdős P. *On a lemma of Littlewood and Offord.* Bulletin Amer. Math. Soc., **51** (1945), 898–902.

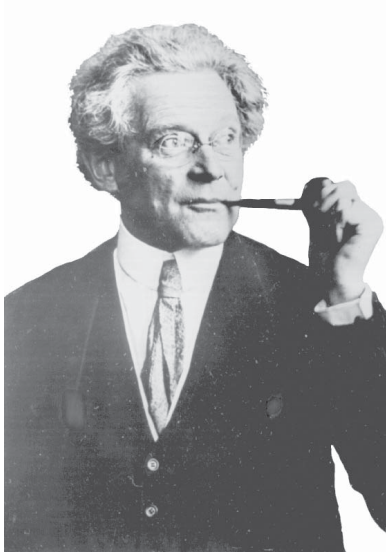
[2] Katona G. *On a conjecture of Erdős and a stronger form of Sperner's theorem.* Studia Sci. Math. Hungar., **1** (1966), 59–63.

[3] Kleitman D. *On a lemma of Littlewood and Offord on the distribution of certain sums.* Math. Zeitschrift, **90** (1965), 251–259.

[4] Kleitman D. *On a lemma of Littlewood and Offord on the distributions of linear combinations of vectors.* Advances Math., **5** (1970), 155–157.

[5] Littlewood J. E., Offord A. C. *On the number of real roots of a random algebraic equation. III.* Математический сборник, нов. сер., **12** (1943), № 3, 277–285.

Глава 23 Котангенс и прием Герглотца



Густав Герглотц

Какая формула, связанная с элементарными функциями, наиболее интересна? В своей прекрасной статье [2], изложению которой мы следуем, Юрген Элстродт выдвинул в качестве первого кандидата разложение функции котангенс на элементарные дроби:

$$\pi \operatorname{ctg} \pi x \;=\; \frac{1}{x} + \sum_{n=1}^{\infty} \left(\frac{1}{x+n} + \frac{1}{x-n} \right) \qquad (x \in \mathbb{R} \backslash \mathbb{Z}).$$

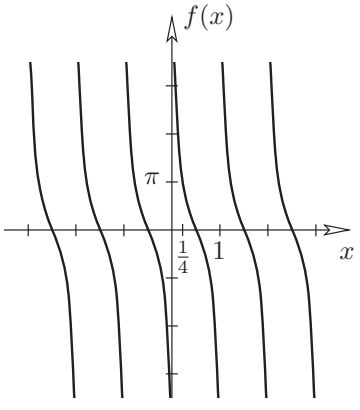
Эта элегантная формула была доказана Эйлером в §178 его *Introductio in Analysin Infinitorum* [3] и, несомненно, относится к числу его наиболее изящных достижений. Ее можно записать еще элегантнее:

$$\pi \operatorname{ctg} \pi x \;=\; \lim_{N \to \infty} \sum_{n=-N}^{N} \frac{1}{x+n}\,; \tag{1}$$

последняя запись (в отличие от первой) математически корректна, так как ряд $\sum_{n \in \mathbb{Z}} \frac{1}{x+n}$ сходится лишь условно.

Мы выведем (1) с помощью ошеломляюще простого рассуждения, которое приписывают Густаву Герглотцу: «приема Герглотца». Для начала положим

$$f(x) \;:=\; \pi \operatorname{ctg} \pi x, \qquad g(x) \;:=\; \lim_{N \to \infty} \sum_{n=-N}^{N} \frac{1}{x+n}\,,$$



Функция $f(x) = \pi \operatorname{ctg} \pi x$

а затем покажем, что эти функции имеют так много общих свойств, что они не могут не совпадать.

(A) Функции $f(x)$ и $g(x)$ определены и непрерывны для всех нецелых значений x.

Для функции $f(x) = \pi \operatorname{ctg} \pi x = \pi \frac{\cos \pi x}{\sin \pi x}$ это очевидно (см. рисунок на полях). Для $g(x)$ воспользуемся равенством $\frac{1}{x+n} + \frac{1}{x-n} = -\frac{2x}{n^2-x^2}$ и перепишем формулу Эйлера в виде

$$\pi \operatorname{ctg} \pi x \;=\; \frac{1}{x} - \sum_{n=1}^{\infty} \frac{2x}{n^2 - x^2}. \tag{2}$$

Для доказательства **(A)** достаточно показать, что ряд

$$\sum_{n=1}^{\infty} \frac{1}{n^2 - x^2}$$

для любого $x \notin \mathbb{Z}$ сходится равномерно в некоторой окрестности точки x. Первые члены ряда, для которых $2n-1 \le x^2$, не влияют на равномерность сходимости, так как их число конечно. С другой стороны, при $n \ge 2$ и $2n-1 > x^2$, т. е. при $n^2 - x^2 > (n-1)^2 > 0$, члены ряда можно оценить сверху:

$$0 \;<\; \frac{1}{n^2-x^2} \;<\; \frac{1}{(n-1)^2}\,,$$

и эта оценка справедлива не только в точке x, но и в ее окрестности. Наконец, из сходимости ряда $\sum \frac{1}{(n-1)^2}$ (к $\frac{\pi^2}{6}$, см. с. 53) следует равномерность сходимости ряда (2), что завершает доказательство утверждения **(A)**.

(B) Функции f и g — *периодические* с периодом 1, т. е. для всех $x \in \mathbb{R}\backslash\mathbb{Z}$ выполняются равенства $f(x+1) = f(x)$ и $g(x+1) = g(x)$.

Так как котангенс имеет период π, то f имеет период 1 (см. рисунок на предыдущей странице). В случае функции g положим

$$g_N(x) \;:=\; \sum_{n=-N}^{N} \frac{1}{x+n}\,.$$

Тогда

$$\begin{aligned} g_N(x+1) \;&=\; \sum_{n=-N}^{N} \frac{1}{x+1+n} \;=\; \sum_{n=-N+1}^{N+1} \frac{1}{x+n} \\ &=\; g_{N-1}(x) + \frac{1}{x+N} + \frac{1}{x+N+1}\,. \end{aligned}$$

Следовательно, $g(x+1) = \lim\limits_{N\to\infty} g_N(x+1) = \lim\limits_{N\to\infty} g_{N-1}(x) = g(x)$.

(C) Функции f и g — *нечетные*, т. е. $f(-x) = -f(x)$ и $g(-x) = -g(x)$ для всех $x \in \mathbb{R}\backslash\mathbb{Z}$.

Очевидно, что функция f обладает этим свойством, а в случае функции g достаточно заметить, что $g_N(-x) = -g_N(x)$.

Собственно прием Герглотца составляют два заключительные предложения. Во-первых, мы покажем, что f и g удовлетворяют одному и тому же функциональному уравнению; во-вторых — что функцию $h := f - g$ можно непрерывно продолжить на все множество действительных чисел $\mathbb{R}$.

(D) Функции f и g удовлетворяют одному и тому же функциональному уравнению: $f(\frac{x}{2}) + f(\frac{x+1}{2}) = 2f(x)$ и $g(\frac{x}{2}) + g(\frac{x+1}{2}) = 2g(x)$.

Для $f(x)$ это следует из теорем сложения для синуса и косинуса:

$$\begin{aligned} f(\tfrac{x}{2}) + f(\tfrac{x+1}{2}) \;&=\; \pi\left[\frac{\cos\frac{\pi x}{2}}{\sin\frac{\pi x}{2}} - \frac{\sin\frac{\pi x}{2}}{\cos\frac{\pi x}{2}}\right] \\ &=\; 2\pi\frac{\cos(\frac{\pi x}{2}+\frac{\pi x}{2})}{\sin(\frac{\pi x}{2}+\frac{\pi x}{2})} \;=\; 2\,f(x). \end{aligned}$$

Теоремы сложения:
$\sin(x+y) = \sin x\cos y + \cos x\sin y$,
$\cos(x+y) = \cos x\cos y - \sin x\sin y$,
$\Longrightarrow$ $\sin(x+\frac{\pi}{2}) = \cos x$,
$\cos(x+\frac{\pi}{2}) = -\sin x$,
$\sin x = 2\sin\frac{x}{2}\cos\frac{x}{2}$,
$\cos x = \cos^2\frac{x}{2} - \sin^2\frac{x}{2}$.

Функциональное уравнение для g следует из равенства

$$g_N(\tfrac{x}{2}) \;+\; g_N(\tfrac{x+1}{2}) = 2\,g_{2N}(x) \;+\; \frac{2}{x+2N+1}\,,$$

которое, в свою очередь, вытекает из соотношения

$$\frac{1}{\frac{x}{2}+n} + \frac{1}{\frac{x+1}{2}+n} = 2\Big(\frac{1}{x+2n} + \frac{1}{x+2n+1}\Big).$$

Теперь рассмотрим разность

$$h(x) \;=\; f(x) \;-\; g(x) \;=\; \pi\operatorname{ctg}\pi x - \Big(\frac{1}{x} - \sum_{n=1}^{\infty}\frac{2x}{n^2-x^2}\Big). \qquad (3)$$

$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} \pm \ldots$

$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} \pm \ldots$

Мы уже знаем, что h — непрерывная функция на $\mathbb{R}\backslash\mathbb{Z}$ и обладает свойствами **(B)**, **(C)** и **(D)**. Что происходит в целых точках? Используя разложения синуса и косинуса в ряды (или дважды применяя правило Лопиталя), находим

$$\lim_{x\to 0}\Big(\operatorname{ctg} x - \frac{1}{x}\Big) \;=\; \lim_{x\to 0}\frac{x\cos x - \sin x}{x\sin x} \;=\; 0,$$

и аналогично

$$\lim_{x\to 0}\Big(\pi\operatorname{ctg}\pi x - \frac{1}{x}\Big) \;=\; 0.$$

Но так как сумма $\sum_{n=1}^{\infty}\frac{2x}{n^2-x^2}$ в (3) при $x\to 0$ сходится к 0, то имеет место равенство $\lim\limits_{x\to 0} h(x) = 0$, и в силу периодичности

$$\lim_{x\to n} h(x) \;=\; 0 \qquad \text{для всех } n\in\mathbb{Z}.$$

Тем самым мы доказали следующее утверждение:

(E) Функция h, доопределенная условием $h(x) := 0$ при $x\in\mathbb{Z}$, непрерывна на $\mathbb{R}$ и обладает свойствами **(B)**, **(C)** и **(D)**.

Мы теперь готовы к последнему шагу доказательства. Так как h — периодическая непрерывная функция, то она принимает максимальное значение m. Пусть x_0 — такая точка отрезка $[0,1]$, что $h(x_0) = m$. Из **(D)** следует, что

$$h(\tfrac{x_0}{2}) + h(\tfrac{x_0+1}{2}) \;=\; 2m,$$

и поэтому $h(\frac{x_0}{2}) = h(\frac{x_0+1}{2}) = m$. С помощью итераций получаем, что $h(\frac{x_0}{2^n}) = m$ для всех n, и вследствие непрерывности $h(0) = m$. Но $h(0) = 0$, так что $m = 0$, т. е. $h(x) \le 0$ для всех $x\in\mathbb{R}$. Так как $h(x)$, кроме того, — *нечетная* функция, то неравенство $h(x) < 0$ невозможно. Таким образом, $h(x) = 0$ для всех $x\in\mathbb{R}$, и теорема Эйлера доказана. □

Из формулы (1) можно вывести очень много следствий, наиболее известное из которых относится к значениям дзета-функции Римана в четных положительных целых точках (см. приложение к гл. 8):

$$\zeta(2k) \;=\; \sum_{n=1}^{\infty}\frac{1}{n^{2k}} \qquad (k\in\mathbb{N}). \qquad (4)$$

В завершение этой главы рассмотрим рассуждения Эйлера о ряде (4), проведенные им в 1755 году [4], через несколько лет после вывода

формулы (1). Начнем с формулы (2). Умножая (2) на x и полагая $y = \pi x$ для $|y| < \pi$, получим:

$$\begin{aligned} y \operatorname{ctg} y &= 1 - 2\sum_{n=1}^{\infty} \frac{y^2}{\pi^2 n^2 - y^2} \\ &= 1 - 2\sum_{n=1}^{\infty} \frac{y^2}{\pi^2 n^2} \frac{1}{1 - \left(\frac{y}{\pi n}\right)^2}. \end{aligned}$$

Последняя дробь есть сумма бесконечной геометрической прогрессии, так что

$$\begin{aligned} y \operatorname{ctg} y &= 1 - 2\sum_{n=1}^{\infty} \sum_{k=1}^{\infty} \left(\frac{y}{\pi n}\right)^{2k} \\ &= 1 - 2\sum_{k=1}^{\infty} \Big(\frac{1}{\pi^{2k}} \sum_{n=1}^{\infty} \frac{1}{n^{2k}}\Big) y^{2k}, \end{aligned}$$

и мы доказали замечательное предложение:

Для всех $k \in \mathbb{N}$ коэффициент при y^{2k} в разложении функции $y \operatorname{ctg} y$ в степенной ряд удовлетворяет равенству

$$\big[y^{2k}\big]\, y \operatorname{ctg} y = -\frac{2}{\pi^{2k}} \sum_{n=1}^{\infty} \frac{1}{n^{2k}} = -\frac{2}{\pi^{2k}}\, \zeta(2k). \tag{5}$$

Есть и другой, возможно, значительно более «стандартный», способ разложения $y \operatorname{ctg} y$ в степенной ряд. Из анализа известно, что $e^{iy} = \cos y + i \sin y$; поэтому

$$\cos y = \frac{e^{iy} + e^{-iy}}{2}, \qquad \sin y = \frac{e^{iy} - e^{-iy}}{2i},$$

откуда находим

$$y \operatorname{ctg} y = iy \frac{e^{iy} + e^{-iy}}{e^{iy} - e^{-iy}} = iy \frac{e^{2iy} + 1}{e^{2iy} - 1}.$$

Сделав замену $z = 2iy$, получим:

$$y \operatorname{ctg} y = \frac{z}{2} \frac{e^z + 1}{e^z - 1} = \frac{z}{2} + \frac{z}{e^z - 1}. \tag{6}$$

Теперь нам нужно найти разложение функции $\frac{z}{e^z - 1}$ в степенной ряд. Заметим, что эта функция определена и непрерывна на всей прямой $\mathbb{R}$ (при $z = 0$ используем степенной ряд для экспоненциальной функции или правило Лопиталя, что приводит к значению, равному 1). Положим

$$\frac{z}{e^z - 1} := \sum_{n \geq 0} B_n \frac{z^n}{n!}. \tag{7}$$

Коэффициенты B_n называются *числами Бернулли* . Левая часть (6) — *четная* функция (т. е. $f(z) = f(-z)$), поэтому $B_n = 0$ для нечетных $n \geq 3$, но $B_1 = -\frac{1}{2}$, что соответствует члену $\frac{z}{2}$ в правой части (6).

Приравнивая коэффициенты при z^n в равенствах

$$\Big(\sum_{n\ge0} B_n\frac{z^n}{n!}\Big)(e^z-1) \;=\; \Big(\sum_{n\ge0} B_n\frac{z^n}{n!}\Big)\Big(\sum_{n\ge1}\frac{z^n}{n!}\Big) \;=\; z,$$

получаем соотношения

$$\sum_{k=0}^{n-1}\frac{B_k}{k!(n-k)!} \;=\; \begin{cases} 1 & \text{при } n=1,\\ 0 & \text{при } n\ne 1.\end{cases} \tag{8}$$

С помощью равенств (8) можно рекуррентно вычислять числа B_n. Если $n=1$, то $B_0=1$, если $n=2$, то $\frac{B_0}{2}+B_1=0$, т. е. $B_1=-\frac12$, и т. д.

Наконец, объединение равенств (6) и (7) дает

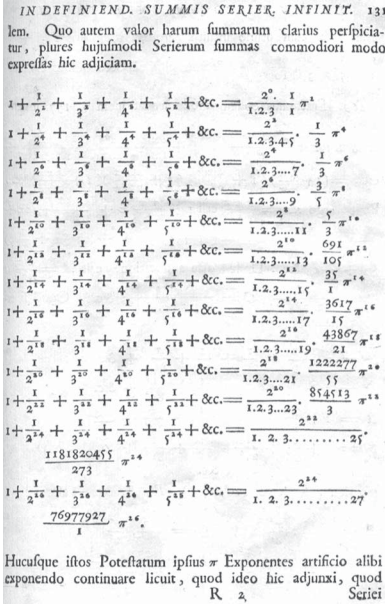
$$y\operatorname{ctg} y \;=\; \sum_{k=0}^{\infty} B_{2k}\frac{(2iy)^{2k}}{(2k)!} \;=\; \sum_{k=0}^{\infty}\frac{(-1)^k 2^{2k}B_{2k}}{(2k)!}y^{2k};$$

учитывая (5), приходим к формуле Эйлера для $\zeta(2k)$:

$$\sum_{n=1}^{\infty}\frac{1}{n^{2k}} \;=\; \frac{(-1)^{k-1}2^{2k-1}B_{2k}}{(2k)!}\,\pi^{2k} \qquad (k\in\mathbb{N}). \tag{9}$$

n	0	1	2	3	4	5	6	7	8
B_n	1	$-\frac12$	$\frac16$	0	$-\frac{1}{30}$	0	$\frac{1}{42}$	0	$-\frac{1}{30}$

Несколько первых чисел Бернулли. (Числа Бернулли, включая B_{34}, можно найти в [5*, с.272]. — *Прим. перев.*)



IN DEFINIEND. SUMMIS SERIER. INFINIT. 131

lem. Quo autem valor harum ſummarum clarius perſpiciatur, plures hujuſmodi Serierum ſummas commodiori modo expreſſas hic adjiciam.

$$1+\tfrac{1}{2^2}+\tfrac{1}{3^2}+\tfrac{1}{4^2}+\tfrac{1}{5^2}+\&c.=\frac{2^0}{1.2.3}\,\pi^1$$
$$1+\tfrac{1}{2^4}+\tfrac{1}{3^4}+\tfrac{1}{4^4}+\tfrac{1}{5^4}+\&c.=\frac{2^3}{1.2.3.4.5}\cdot\frac{1}{3}\,\pi^4$$
$$1+\tfrac{1}{2^6}+\tfrac{1}{3^6}+\tfrac{1}{4^6}+\tfrac{1}{5^6}+\&c.=\frac{2^5}{1.2.3....7}\cdot\frac{1}{3}\,\pi^6$$
$$1+\tfrac{1}{2^8}+\tfrac{1}{3^8}+\tfrac{1}{4^8}+\tfrac{1}{5^8}+\&c.=\frac{2^7}{1.2.3....9}\cdot\frac{3}{5}\,\pi^8$$
$$1+\tfrac{1}{2^{10}}+\tfrac{1}{3^{10}}+\tfrac{1}{4^{10}}+\tfrac{1}{5^{10}}+\&c.=\frac{2^9}{1.2.3....11}\cdot\frac{5}{3}\,\pi^{10}$$
$$1+\tfrac{1}{2^{12}}+\tfrac{1}{3^{12}}+\tfrac{1}{4^{12}}+\tfrac{1}{5^{12}}+\&c.=\frac{2^{11}}{1.2.3....13}\cdot\frac{691}{105}\,\pi^{12}$$
$$1+\tfrac{1}{2^{14}}+\tfrac{1}{3^{14}}+\tfrac{1}{4^{14}}+\tfrac{1}{5^{14}}+\&c.=\frac{2^{13}}{1.2.3....15}\cdot\frac{35}{1}\,\pi^{14}$$
$$1+\tfrac{1}{2^{16}}+\tfrac{1}{3^{16}}+\tfrac{1}{4^{16}}+\tfrac{1}{5^{16}}+\&c.=\frac{2^{15}}{1.2.3....17}\cdot\frac{3617}{15}\,\pi^{16}$$
$$1+\tfrac{1}{2^{18}}+\tfrac{1}{3^{18}}+\tfrac{1}{4^{18}}+\tfrac{1}{5^{18}}+\&c.=\frac{2^{17}}{1.2.3....19}\cdot\frac{43867}{21}\,\pi^{18}$$
$$1+\tfrac{1}{2^{20}}+\tfrac{1}{3^{20}}+\tfrac{1}{4^{20}}+\tfrac{1}{5^{20}}+\&c.=\frac{2^{19}}{1.2.3....21}\cdot\frac{1222277}{55}\,\pi^{20}$$
$$1+\tfrac{1}{2^{22}}+\tfrac{1}{3^{22}}+\tfrac{1}{4^{22}}+\tfrac{1}{5^{22}}+\&c.=\frac{2^{20}}{1.2.3...23}\cdot\frac{854513}{3}\,\pi^{22}$$
$$1+\tfrac{1}{2^{24}}+\tfrac{1}{3^{24}}+\tfrac{1}{4^{24}}+\tfrac{1}{5^{24}}+\&c.=\frac{2^{23}}{1.\,2.\,3.\ldots\ldots\ldots 25}\cdot\frac{\frac{118118040455}{273}}{1}\,\pi^{24}$$
$$1+\tfrac{1}{2^{26}}+\tfrac{1}{3^{26}}+\tfrac{1}{4^{26}}+\tfrac{1}{5^{26}}+\&c.=\frac{2^{25}}{1.\,2.\,3.\ldots\ldots\ldots 27}\cdot\frac{76977927}{1}\,\pi^{26}.$$

Hucuſque iſtos Poteſtatum ipſius π Exponentes artificio alibi exponendo continuare licuit, quod ideo hic adjunxi, quod

R 2 Seriei

Страница 131 книги Л. Эйлера «Introductio in Analysin Infinitorum», 1748 г.

Рассматривая таблицу чисел Бернулли, мы снова получаем сумму $\sum\frac{1}{n^2}=\frac{\pi^2}{6}$ из главы 8 и, кроме того,

$$\sum_{n=1}^{\infty}\frac{1}{n^4}=\frac{\pi^4}{90}\,,\qquad \sum_{n=1}^{\infty}\frac{1}{n^6}=\frac{\pi^6}{945}\,,\qquad \sum_{n=1}^{\infty}\frac{1}{n^8}=\frac{\pi^8}{9450}\,,$$

$$\sum_{n=1}^{\infty}\frac{1}{n^{10}}=\frac{\pi^{10}}{93555}\,,\qquad \sum_{n=1}^{\infty}\frac{1}{n^{12}}=\frac{691\,\pi^{12}}{638512875}\,,\quad\ldots$$

Число Бернулли $B_{10}=\frac{5}{66}$, которое позволяет вычислить $\zeta(10)$, выглядит достаточно безобидно, но следующее значение $B_{12}=-\frac{691}{2730}$, необходимое для нахождения $\zeta(12)$, содержит в числителе большое простое число 691. Эйлер сначала вычислил несколько значений $\zeta(2k)$, не заметив связи с числами Бернулли. Лишь появление необычного простого числа 691 вывело его на правильный путь.

Кстати, поскольку $\zeta(2k)$ при $k\to\infty$ сходится к 1, равенство (9) означает, что числа $|B(2k)|$ очень быстро растут, о чем трудно догадаться по их значениям при малых k.

Однако о значениях дзета-функции Римана в нечетных целых точках $k\ge3$ известно очень мало (см. с. 60).

Литература

[1] Bochner S. *Book review of «Gesammelte Schriften» by Gustav Herglotz.* Bulletin Amer. Math. Soc., **1** (1979), 1020–1022.

[2] Elstrodt J. *Partialbruchzerlegung des Kotangens, Herglotz-Trick und die Weierstraßsche stetige, nirgends differenzierbare Funktion.* Math. Semesterberichte, **45** (1998), 207–220.

[3] Euler L. *Introductio in Analysin Infinitorum,* Tomus Primus, Lausanne 1748; Opera Omnia, Ser. 1, Vol. 8. In English: *Introduction to Analysis of the Infinite,* Book I, Springer-Verlag, New York, 1988. [Русский перевод: Леонард Эйлер. Введение в анализ бесконечных, т.1, изд. 2-е. М., Гос. изд-во физ.-матем. лит-ры, 1961.]

[4] Euler L. *Institutiones calculi differentialis cum ejus usu in analysi finitorum ac doctrina serierum.* Petersburg 1755; Opera Omnia, Ser. 1, Vol. 10.

[5*] Гельфонд А. О. *Исчисление конечных разностей, изд. 2-е.* М., Гос. изд-во физ.-матем. лит-ры, 1959.

Глава 24 Задача Бюффона об игле

Граф де Бюффон

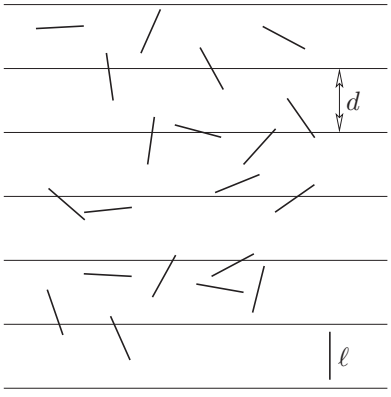
Французский дворянин Жорж Луи Леклерк, граф де Бюффон (1707–1788) в 1777 году предложил следующую задачу.

> *Предположим, что короткую иглу бросают на лист линованной бумаги. Какова вероятность того, что упавшая игла пересекает одну из прямых?*

Вероятность зависит от расстояния d между соседними прямыми на линованной бумаге и от длины ℓ бросаемой иглы; точнее, она зависит лишь от отношения $\frac{\ell}{d}$. *Короткой* мы считаем иглу длины $\ell \le d$. Другими словами, короткая игла — та, которая не может пересечь две прямые одновременно (и может касаться двух линий лишь с вероятностью 0). Ответ в задаче Бюффона может удивить: он включает число π.

Теорема («задача Бюффона об игле»). *Если короткая игла длины l брошена на бумагу, которая разлинована так, что расстояния между соседними прямыми линиями одинаковы и равны $d \ge \ell$, то вероятность того, что упавшая игла пересечет одну из прямых, равна*

$$p \;=\; \frac{2}{\pi}\frac{\ell}{d}\,.$$



Это утверждение означает, что можно экспериментальным путем найти приближенное значение π. Если при N бросаниях иглы положительный ответ (пересечение) получился в P случаях, то $\frac{P}{N}$ должно быть приближенно равно $\frac{2}{\pi}\frac{\ell}{d}$, т. е. величина $\frac{2\ell N}{dP}$ должна быть приближением к числу π. Наиболее обширная (и исчерпывающая) проверка теоремы, возможно, была проведена Лаззарини в 1901 году; он утверждал, что построил машину, с помощью которой бросил стержень (с $\frac{\ell}{d} = \frac{5}{6}$) 3408 раз. При этом получилось 1808 пересечений, что дало аппроксимацию $\pi \approx 2 \cdot \frac{5}{6}\,\frac{3408}{1808} = 3.1415929...$, верную до шестого знака π. Такая точность неправдоподобно высока. (Число экспериментов 3408 и длина стержня $\frac{5}{6}$, выбранные Лаззарини, соответствуют известной аппроксимации $\pi \approx \frac{355}{113}$, см. с. 50: число $\frac{5}{6}\,3408 = 2840$ кратно 355. Мистификация Лаззарини обсуждалась в книге [5].)

Задачу об игле можно решить вычислением интеграла. Мы проведем такое вычисление ниже, и с помощью этого метода решим также задачу для длинной иглы. Но Доказательство из Книги, найденное Е.Барбье в 1860 году [1], не нуждается в интегралах. Он просто рассмотрел задачу о бросании игл другого вида...

При бросании *любой* иглы, короткой или длинной, среднее число пересечений равно

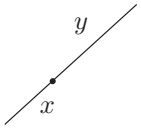
$$E \;=\; p_1 + 2p_2 + 3p_3 + \ldots,$$

где p_1 — вероятность того, что игла пересечет точно одну прямую, p_2 — вероятность того, что получится ровно два пересечения, p_3 — вероятность появления трех пересечений и т. д. Вероятность того, что получится хотя бы одно пересечение, о чем идет речь в задаче Бюффона, равна

$$p \;=\; p_1 + p_2 + p_3 + \dots$$

(События, при которых игла лежит точно на некоторой прямой или касается одним из концов одной из линий, имеют вероятность нуль, так что в ходе нашего обсуждения ими можно пренебречь.)

С другой стороны, если игла *короткая*, то вероятность более одного пересечения равна нулю ($p_2 = p_3 = \dots = 0$), и поэтому $E = p$, т. е. интересующая нас вероятность есть как раз среднее число пересечений. Эта новая формулировка очень полезна и позволяет воспользоваться линейностью математического ожидания (см. с. 103). Действительно, обозначим через $E(\ell)$ среднее число пересечений, когда бросается прямая игла длины ℓ. Если эта длина есть $\ell = x + y$, и мы рассмотрим «начало» иглы длины x и ее «конец» длины y отдельно, то получим



$$E(x+y) \;=\; E(x) + E(y),$$

поскольку множество пересечений иглы с прямыми является объединением множества пересечений, порожденных ее началом, и множества пересечений, порожденных ее концом.

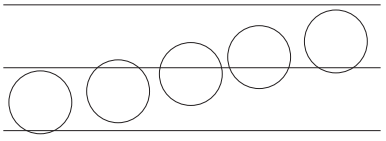
С помощью индукции по n из этого «функционального уравнения» находим, что $E(nx) = nE(x)$ для всех $n \in \mathbb{N}$, и затем, что $mE(\frac{n}{m}x) = E(m\frac{n}{m}x) = E(nx) = nE(x)$, для любых $m, n \in \mathbb{N}$, так что для всех *рациональных* $r \in \mathbb{Q}$ справедливо равенство $E(rx) = rE(x)$. Кроме того, ясно, что $E(x)$ монотонно возрастает по $x \geq 0$, откуда мы находим, что $E(x) = cx$ для всех $x \geq 0$, где $c = E(1)$ — некоторая константа.

Но чему равна эта константа?

Чтобы найти ее, используем иглы различных форм. В самом деле, пусть бросают «ломаную» иглу, состоящую из прямолинейных отрезков, общая длина которых равна ℓ. Тогда полученное число пересечений есть (с вероятностью 1) сумма чисел пересечений, образуемых прямолинейными частями иглы. Значит, среднее число пересечений ввиду линейности математического ожидания снова равно

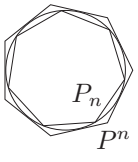
$$E \;=\; c\,\ell.$$

(При этом даже не важно, будут прямолинейные части иглы соединены жестким или эластичным способом!)



Ключ к предложенному Барбье решению задачи Бюффона об игле заключается в том, чтобы рассматривать иглу, которая является полной окружностью C диаметра d, имеющей длину $x = d\pi$. Такая игла, будучи брошена на линованную бумагу, всегда дает ровно два пересечения![1]

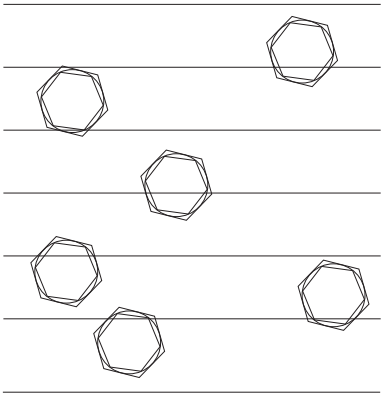
Окружность можно аппроксимировать многоугольниками. Представим себе, что вместе с круглой иглой C мы бросаем вписанный в нее многоугольник P_n, а также описанный около нее многоугольник P^n. Каждая прямая, которая пересекает P_n, пересекает также и C, а если C пересекает прямую, то ее пересекает и P^n. Поэтому средние числа



[1] Расстояние между прямыми на бумаге равно d, а вероятность того, что окружность касается некоторых прямых, равна 0. — *Прим. перев.*

пересечений удовлетворяют неравенствам

$$E(P_n) \;\le\; E(C) \;\le\; E(P^n).$$



Далее, и P_n, и P^n — многоугольники, так что среднее число пересечений для каждого из них равно произведению его периметра и константы c, в то время как для иглы C это число равно 2. Таким образом,

$$c\,\ell(P_n) \;\le\; 2 \;\le\; c\,\ell(P^n). \tag{1}$$

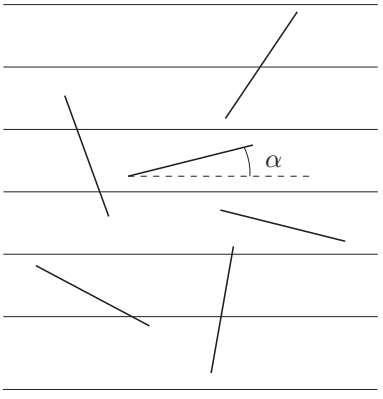
Многоугольники P_n и P^n при $n\to\infty$ стремятся к C. В частности,

$$\lim_{n\to\infty}\ell(P_n) \;=\; d\pi \;=\; \lim_{n\to\infty}\ell(P^n),$$

и поэтому при $n\to\infty$ из (1) вытекает, что

$$c\,d\pi \;\le\; 2 \;\le c\,d\pi,$$

значит, $c=\frac{2}{\pi}\frac{1}{d}$. □



Но мы также *могли бы* доказать эту теорему с помощью математического анализа! Для вывода «берущегося» интеграла нужно сначала фиксировать угол α между иглой и положительным направлением на прямых, считая, что $0\le\alpha\le\frac{\pi}{2}$. (Случай, когда $\frac{\pi}{2}\le\alpha\le\pi$, можно не рассматривать, так как он симметричен случаю $0\le\alpha\le\frac{\pi}{2}$ и имеет ту же самую вероятность.) Игла, которая лежит под углом α, имеет проекцию $\ell\sin\alpha$ на прямую T, перпендикулярную семейству параллельных горизонтальных прямых, и поэтому вероятность того, что такая игла пересечет одну из прямых, расстояние между которыми есть d, равна $\frac{\ell\sin\alpha}{d}$. Усредняя по возможным углам α, мы получим искомую вероятность[2]:

$$p \;=\; \frac{2}{\pi}\int\limits_0^{\pi/2}\frac{\ell\sin\alpha}{d}\,d\alpha \;=\; \frac{2}{\pi}\frac{\ell}{d}\Big[-\cos\alpha\Big]_0^{\pi/2} \;=\; \frac{2}{\pi}\frac{\ell}{d}.$$

В случае длинной иглы вероятность ее пересечения хотя бы с одной прямой равна $\frac{\ell\sin\alpha}{d}$, если $\ell\sin\alpha\le d$, т. е. если $0\le\alpha\le\arcsin\frac{d}{\ell}$. При бóльших углах α игла *обязательно* пересекает какую-нибудь прямую, так что вероятность равна 1. Поэтому при $\ell\ge d$

$$\begin{aligned} p \;&=\; \frac{2}{\pi}\Big(\int_0^{\arcsin(d/\ell)}\frac{\ell\sin\alpha}{d}\,d\alpha \;+\; \int\limits_{\arcsin(d/\ell)}^{\pi/2}1\;d\alpha\Big) = \\ &=\; \frac{2}{\pi}\Big(\frac{\ell}{d}\Big[-\cos\alpha\Big]_0^{\arcsin(d/\ell)} + \Big(\frac{\pi}{2}-\arcsin\frac{d}{\ell}\Big)\Big) = \\ &=\; 1+\frac{2}{\pi}\Big(a\frac{\ell}{d}\Big(1-\sqrt{1-\frac{d^2}{\ell^2}}\Big)-\arcsin\frac{d}{l}\Big). \end{aligned}$$

В случае длинной иглы ответ не так красив, но он дает основу для хорошего упражнения: проверьте, что выражение для p при $\ell=d$ равно $\frac{2}{\pi}$, что оно монотонно возрастает по ℓ и стремится к 1, когда $\ell\to\infty$.

[2] Аналогичное доказательство для короткой иглы имеется в [6*]. — *Прим. перев.*

Литература

[1] Barbier E. *Note sur le problème de l'aiguille et le jeu du joint couvert.* J. Mathématiques Pures et Appliquées, (2) **5** (1860), 273–286.

[2] Berggren L., Borwein J., Borwein P., eds. *Pi: A Source Book.* Springer-Verlag, New York, 1997.

[3] Leclerc G. L., Comte de Buffon. *Essai d'arithmétique morale.* Appendix to «Histoire naturelle générale et particulière», Vol. 4, 1777.

[4] Klain D. A., Rota G.-C. *Introduction to Geometric Probability.* «Lezioni Lincee», Cambridge University Press, 1997.

[5] O'Beirne T. H. *Puzzles and Paradoxes.* Oxford University Press, London, 1965.

[6*] Гнеденко Б. В. *Курс теории вероятностей, изд. 3-е.* М., Гос. изд-во физ.-матем. лит-ры, 1961.

«Получил задачу?»

Комбинаторика

«Меланхолический латинский квадрат»

Глава 25 Принцип Дирихле и двойной счет

«Голубиные гнезда с точки зрения птиц»

Некоторые математические принципы, в частности, указанные в названии этой главы, настолько очевидны, что может показаться, будто они позволяют получать лишь столь же очевидные результаты. Чтобы убедить вас в том, что «это не всегда так», мы иллюстрируем их примерами, которые предложил включить в нашу книгу Пауль Эрдёш. Эти принципы будут использоваться и в последующих главах.

Принцип Дирихле.
Если n предметов разместить по r ячейкам, где $r < n$, то хотя бы в одну ячейку попадет больше одного предмета.

Это утверждение действительно очевидно; здесь нечего доказывать. На языке отображений принцип Дирихле[1] записывается следующим образом. Пусть N и R — два конечных множества,

$$|N| = n > r = |R|,$$

и $f : N \longrightarrow R$ — отображение из N в R. Тогда найдется такой элемент $a \in R$, что $|f^{-1}(a)| \geq 2$. Мы можем установить даже более сильное неравенство: существует такое $a \in R$, что

$$|f^{-1}(a)| \ \geq \ \left\lceil \frac{n}{r} \right\rceil. \tag{1}$$

В самом деле, в противном случае мы имели бы $|f^{-1}(a)| < \frac{n}{r}$ для всех $a \in R$, и тогда выполнялось бы неравенство

$$n = \sum_{a \in R} |f^{-1}(a)| < r\,\frac{n}{r} = n,$$

что невозможно.

1. Числа

Утверждение. *Если из множества $\{1, 2, 3, \ldots, 2n\}$ выбрать любые $n+1$ чисел, то среди них найдутся два взаимно простых.*

Это утверждение тоже очевидно: среди выбранных должны найтись два числа, которые отличаются на 1 и поэтому взаимно просты[2].

Теперь давайте изменим формулировку этого утверждения.

[1] В англоязычной литературе используется термин «pigeon-hole principle», дословно: принцип голубиных гнезд. — *Прим. перев.*

[2] Можно рассмотреть n «ячеек» $\{1, 2\}$, $\{3, 4\}$, …, $\{2n-1, 2n\}$. — *Прим. перев.*

Утверждение. *Пусть снова* $A \subseteq \{1, 2, \ldots, 2n\}$ *и* $|A| = n + 1$. *Тогда в* A *найдутся два такие числа, что одно делит другое.*

Это утверждение менее очевидно. Как рассказал нам Эрдёш, он поставил эту задачу юному Лайошу Поза за обедом, а когда обед закончился у Лайоша уже был ответ. Задача оставалась у Эрдёша одним из излюбленных вопросов для вступающих в математику. Ее (положительное) решение основано на принципе Дирихле. Представим каждое число $a \in A$ в виде $a = 2^k m$, где m — нечетное число, $1 \leq m \leq 2n - 1$. Так как в A содержится $n + 1$ чисел, а количество нечетных чисел, меньших $2n$, равно n, то в A должны найтись два числа с *одинаковыми* нечетными делителями. Поэтому одно из них делится на другое. □

Оба утверждения становятся неверными при замене $n+1$ на n. Примерами являются множества $\{2, 4, 6, \ldots, 2n\}$ и $\{n+1, n+2, \ldots, 2n\}$ соответственно.

2. Последовательности

Рассмотрим другую любимую задачу Эрдёша из статьи Эрдёша и Секереша [4] о задачах Рамсея.

Утверждение. *Любая последовательность* $a_1, a_2, \ldots, a_{mn+1}$ *из* $mn + 1$ *различных действительных чисел содержит либо возрастающую подпоследовательность*

$$a_{i_1} < a_{i_2} < \ldots < a_{i_{m+1}} \qquad (i_1 < i_2 < \ldots < i_{m+1})$$

длины $m + 1$, *либо убывающую подпоследовательность*

$$a_{j_1} > a_{j_2} > \ldots > a_{j_{n+1}} \qquad (j_1 < j_2 < \ldots < j_{n+1})$$

длины $n + 1$, *либо обе такие подпоследовательности.*

На этот раз применение принципа Дирихле более сложно. Поставим в соответствие каждому a_i число t_i, равное длине *наибольшей возрастающей* подпоследовательности, которая начинается с a_i. Если $t_i \geq m + 1$ для некоторого i, то с a_i начинается возрастающая подпоследовательность длины $m + 1$. Поэтому предположим, что $t_i \leq m$ для всех i. Для функции $f : a_i \longmapsto t_i$, отображающей $\{a_1, \ldots, a_{mn+1}\}$ в $\{1, \ldots, m\}$, в силу (1) существует такое $s \in \{1, \ldots, m\}$, что $f(a_i) = s$ для $\frac{mn}{m} + 1 = n + 1$ чисел a_i. Пусть $a_{j_1}, a_{j_2}, \ldots, a_{j_{n+1}}$ $(j_1 < \ldots < j_{n+1})$ — эти числа. Рассмотрим теперь пары последовательных чисел a_{j_i}, $a_{j_{i+1}}$. Если $a_{j_i} < a_{j_{i+1}}$ хотя бы при одном $i \in \{1, \ldots, n\}$, то существует возрастающая подпоследовательность длины s, начинающаяся с $a_{j_{i+1}}$, и, следовательно, возрастающая подпоследовательность длины $s + 1$, начинающаяся с a_{j_i}, что противоречит предположению $f(a_{j_i}) = s$. Значит, $a_{j_1} > a_{j_2} > \ldots > a_{j_{n+1}}$, т. е. существует убывающая подпоследовательность длины $n + 1$. □

Читателю полезно доказать, что для последовательности из mn чисел утверждение в общем случае не верно.

Это просто формулируемое утверждение о монотонных подпоследовательностях имеет весьма неочевидное следствие, относящееся к *размерности графов*. Нам потребуется здесь понятие размерности не для общих, а лишь для полных графов K_n, для которых ее можно определить следующим образом. Пусть $N = \{1, \ldots, n\}$, $n \geq 3$; рассмотрим m перестановок $\pi_1, \ldots, \pi_m$ множества N. Скажем, что перестановки π_i *представляют* K_n, если для любых трех различных

чисел i, j, k из N найдется перестановка π, в которой k появляется *позже* i и j. *Размерность* $\dim(K_n)$ есть наименьшее m, для которого существует представление $\pi_1, \ldots, \pi_m$.

В качестве примера укажем, что $\dim(K_3) = 3$, так как каждое из трех чисел $1, 2, 3$ должно хотя бы раз оказаться последним, как в $\pi_1 = (1, 2, 3)$, $\pi_2 = (2, 3, 1)$, $\pi_3 = (3, 1, 2)$. Что можно сказать о $\dim(K_4)$? Заметим вначале, что $\dim(K_n) \le \dim(K_{n+1})$ (для доказательства достаточно вычеркнуть число $n + 1$ в представлении K_{n+1}). Поэтому $\dim(K_4) \ge 3$, а на самом деле $\dim(K_4) = 3$, так как можно взять

$$\pi_1 = (1, 2, 3, 4), \quad \pi_2 = (2, 4, 3, 1), \quad \pi_3 = (1, 4, 3, 2).$$

π_1: 1 2 3 5 6 7 8 9 10 11 12 4
π_2: 2 3 4 8 7 6 5 12 11 10 9 1
π_3: 3 4 1 11 12 9 10 6 5 8 7 2
π_4: 4 1 2 10 9 12 11 7 8 5 6 3

Эти четыре перестановки представляют K_{12}

Совсем не так просто доказать, что $\dim(K_5) = 4$, и совершенно неожиданно, что размерность графов K_n до $n = 12$ включительно остается равной 4, в то время как $\dim(K_{13}) = 5$. Поэтому кажется, что $\dim(K_n)$ является довольно «дикой» функцией. Однако это не так! В действительности функция $\dim(K_n)$ ведет себя очень хорошо, если n стремится к бесконечности, и ключом к нахождению нижней оценки для $\dim(K_n)$ является принцип Дирихле.

Мы утверждаем, что

$$\dim(K_n) \ \ge \ \log_2 \log_2 n. \tag{2}$$

Поскольку, как мы уже видели, $\dim(K_n)$ — монотонная функция n, достаточно проверить (2) для $n = 2^{2^p} + 1$, т. е. показать, что

$$\dim(K_n) \ \ge \ p + 1 \qquad \text{при} \quad n = 2^{2^p} + 1.$$

Предположим обратное: $\dim(K_n) \le p$ и $\pi_1, \ldots, \pi_p$ — представляющие K_n перестановки элементов множества $N = \{1, 2, \ldots, 2^{2^p} + 1\}$. Теперь p раз воспользуемся нашим утверждением о монотонных подпоследовательностях. В π_1 существует монотонная подпоследовательность A_1 длины $2^{2^{p-1}} + 1$ (не существенно, возрастает она или убывает). Рассмотрим в π_2 множество элементов из A_1. Согласно утверждению о монотонных подпоследовательностях, в последовательности, образованной в π_2 элементами из A_1 существует монотонная подпоследовательность A_2 длины $2^{2^{p-2}} + 1$. Конечно, элементы из A_2 образуют монотонную подпоследовательность и в π_1. Продолжая таким же образом, мы в конце концов докажем существование подпоследовательности A_p объема $2^{2^0} + 1 = 3$, которая монотонна во *всех* перестановках π_i. Пусть $A_p = (a, b, c)$; тогда для *каждой* перестановки π_i либо $a < b < c$, либо $a > b > c$. Но это противоречит нашему предположению, так как согласно ему должна существовать перестановка, в которой b появляется позже a и c. □

Правильную асимптотику роста $\dim(K_n)$ нашли Джоэль Спенсер [7] (оценка сверху) и Фюреди, Хайнал, Рёдл и Троттер [9], [10] (оценка снизу):

$$\dim(K_n) \ \sim \ \log_2 \log_2 n + \left(\frac{1}{2} + o(1)\right) \log_2 \log_2 \log_2 n.$$

Но и это еще не все. Совсем недавно Моррис и Хостен [5] построили метод, который в принципе находит *точное* значение $\dim(K_n)$. Используя их результат и компьютер, можно получить значения, представленные на полях. Это поистине поразительно! Только подумайте, как много имеется перестановок порядка 1422564. Как решить, 7 или 8 из них требуется, чтобы представить $K_{1422564}$?

$\dim(K_n) \le 4 \iff n \le 12$
$\dim(K_n) \le 5 \iff n \le 81$
$\dim(K_n) \le 6 \iff n \le 2646$
$\dim(K_n) \le 7 \iff n \le 1422564$

3. Суммы

Пауль Эрдёш приписывает Эндрю Васоньи и Марте Сведа авторство следующего тонкого применения принципа Дирихле.

Утверждение. *Для любой последовательности n целых чисел $a_1, \dots, a_n$ (не обязательно различных) найдется ее отрезок $a_{k+1}, a_{k+2}, \dots, a_\ell$, сумма элементов которого $\sum_{i=k+1}^{\ell} a_i$ кратна n.*

Для доказательства положим $N = \{0, a_1, a_1 + a_2, \dots, a_1 + a_2 + \dots + a_n\}$ и $R = \{0, 1, \dots, n-1\}$. Рассмотрим отображение $f : N \to R$, где $f(m)$ — остаток при делении m на n. Так как $|N| = n + 1 > n = |R|$, то существуют две суммы $a_1 + \dots + a_k$, $a_1 + \dots + a_\ell$ $(k < \ell)$ с *одним и тем же* остатком при делении на n, причем первая сумма может быть пустой (если $k = 0$, то она равна 0). В силу этого

$$\sum_{i=k+1}^{\ell} a_i \;=\; \sum_{i=1}^{\ell} a_i \;-\; \sum_{i=1}^{k} a_i$$

дает при делении на n остаток 0. □

Обратимся ко второму принципу — перечислению двумя способами, — под которым понимается следующее.

Двойной счет.
Пусть даны два конечных множества R и C и подмножество $S \subseteq R \times C$. Если $(p, q) \in S$, то мы говорим, что p и q инцидентны.
Если r_p обозначает число элементов, инцидентных $p \in R$, и c_q обозначает число элементов, инцидентных $q \in C$, то

$$\sum_{p \in R} r_p \;=\; |S| \;=\; \sum_{q \in C} c_q. \tag{3}$$

Снова ничего доказывать не нужно. Первая сумма классифицирует пары из S в соответствии с первым элементом, в то время как вторая сумма классифицирует те же самые пары в соответствии со вторым элементом.

Удобным способом представления множества S является *матрица инцидентности* $A = (a_{pq})$: строки и столбцы матрицы A нумеруются

элементами множеств R и C, а элементы матрицы определяются условием

$$a_{pq} = \begin{cases} 1, & \text{если } (p,q) \in S, \\ 0, & \text{если } (p,q) \notin S. \end{cases}$$

Число единиц в матрице A равно числу элементов множества S, r_p есть сумма элементов p-й строки матрицы A, а c_q — сумма элементов q-го столбца. Значит, в первой сумме в (3) элементы матрицы A суммируются (и тем самым находится число элементов множества S) по строкам, а во второй — по столбцам.

Проиллюстрируем это соответствие примером. Пусть $R = C = \{1, 2, \ldots, 8\}$ и $S = \{(i,j) : i \text{ делит } j\}$. Матрица инцидентности множества S приведена на полях (указаны лишь ненулевые элементы).

R \ C	1	2	3	4	5	6	7	8
1	1	1	1	1	1	1	1	1
2		1		1		1		1
3			1			1		
4				1				1
5					1			
6						1		
7							1	
8								1

n	1	2	3	4	5	6	7	8
$\bar{t}(n)$	1	$\frac{3}{2}$	$\frac{5}{3}$	2	2	$\frac{7}{3}$	$\frac{16}{7}$	$\frac{5}{2}$

Несколько первых значений $\bar{t}(n)$

4. Снова числа

Рассмотрим еще раз матрицу инцидентности на полях. Число единиц в j-м столбце равно в точности числу делителей j. Обозначим это число через $t(j)$. Как велико число $t(j)$ *в среднем*, когда j пробегает значения от 1 до n, т. е. насколько велика величина

$$\bar{t}(n) = \frac{1}{n} \sum_{j=1}^{n} t(j)$$

для произвольного n? На первый взгляд этот вопрос кажется неразрешимым. Для простых чисел p мы имеем $t(p) = 2$, тогда как для $n = 2^k$ мы получаем большое число $t(2^k) = k + 1$. Так что функция $t(n)$ ведет себя крайне нерегулярно, и можно подумать, что то же самое справедливо для $\bar{t}(n)$. Неправильное предположение, верно противное! Вычисление двумя способами дает неожиданный и простой ответ.

Рассмотрим матрицу инцидентности A для целых чисел от 1 до n, аналогичную приведенной на полях. Подсчет по столбцам дает $\sum_{j=1}^{n} t(j)$. Сколько единиц содержит строка i? Легко понять, что единицы в ней соответствуют числам, кратным i: $1i, 2i, \ldots$, и последнее кратное, не превосходящее n, есть $\lfloor \frac{n}{i} \rfloor i$. Отсюда получаем:

$$\bar{t}(n) \;=\; \frac{1}{n} \sum_{j=1}^{n} t(j) \;=\; \frac{1}{n} \sum_{i=1}^{n} \left\lfloor \frac{n}{i} \right\rfloor \;\le\; \frac{1}{n} \sum_{i=1}^{n} \frac{n}{i} \;=\; \sum_{i=1}^{n} \frac{1}{i}\,,$$

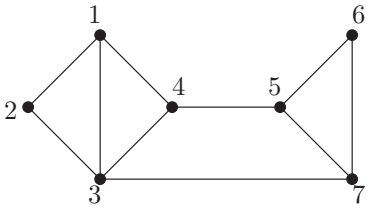
причем i-е слагаемое при замене $\lfloor \frac{n}{i} \rfloor$ на $\frac{n}{i}$ увеличивается меньше, чем на 1.[3] Поэтому разность между правой частью и $\bar{t}(n)$ тоже меньше 1. Правая часть есть n-е гармоническое число H_n, так что $H_n - 1 < \bar{t}(n) < H_n$, и эти неравенства вместе с оценками H_n на с. 19 дают:

$$\ln n - 1 \;<\; H_n - 1 \;<\; \bar{t}(n) \;<\; H_n \;<\; \ln n + 1.$$

Таким образом, мы получили замечательный результат: хотя последовательность $t(n)$ совершенно беспорядочна, ее средние $\bar{t}(n)$ ведут себя прекрасно: $\bar{t}(n)$ отличается от $\ln n$ меньше, чем на 1.

[3] А при замене $\lfloor \frac{n}{i} \rfloor$ на $\frac{n}{i} - 1$ уменьшается меньше, чем на 1. — *Прим. ред.*

5. Графы



Пусть G — конечный простой граф с множеством вершин V и множеством ребер E. В главе 12 мы определили *степень* $d(v)$ вершины v как число ребер, имеющих v в качестве концевой вершины. Граф, изображенный на полях, имеет вершины $1, 2, \ldots, 7$, степени которых равны $3, 2, 4, 3, 3, 2, 3$ соответственно.

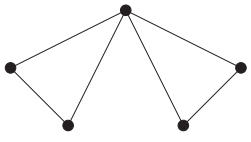
Почти каждая книга по теории графов начинается со следующего утверждения, которое уже встречалось нам в гл.12 и 18:

$$\sum_{v\in V} d(v) \;=\; 2|E|. \tag{4}$$

Для доказательства формулы (4) обозначим через $S \subseteq V \times E$ множество таких пар (v, e), что $v \in V$ есть концевая вершина ребра $e \in E$. Перечисляя S двумя способами, имеем, с одной стороны, $|S| = \sum_{v\in V} d(v)$, так как каждая вершина вносит в сумму вклад $d(v)$; с другой стороны, $|S| = 2|E|$, поскольку каждое ребро имеет два конца. □

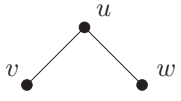
Из простой формулы (4) вытекает много важных следствий; некоторые из них будут обсуждаться далее. В этом разделе мы рассмотрим следующее красивое применение к одной *экстремальной задаче* на графах:

Пусть простой граф $G = (V, E)$ имеет n вершин и не содержит циклов длины 4, обозначаемых C_4, т. е. не содержит подграфов вида  *. Какое наибольшее число ребер может иметь G?*



Например, граф с 5 вершинами, изображенный на полях, не содержит ни одного 4-цикла и имеет 6 ребер. Читатель может легко проверить, что для графов с 5 вершинами без 4-циклов максимальное число ребер равно 6 и что этот граф — единственный граф с 6 ребрами, не имеющий 4-циклов.

Приступим к решению задачи в общем случае. Пусть G — граф с n вершинами без 4-циклов. Как и выше, обозначим через $d(u)$ степень вершины u. Перечислим двумя способами множество S таких пар $(u, \{v, w\})$, что вершина u смежна вершинам v и w, $v \neq w$. Другими словами, мы подсчитываем в G все подграфы вида



Суммируя по u, мы находим $|S| = \sum_{u\in V} \binom{d(u)}{2}$. С другой стороны, ввиду отсутствия 4-циклов каждая пара $\{v, w\}$ имеет не более одной вершины, смежной с v и w. Поэтому $|S| \le \binom{n}{2}$. Значит,

$$\sum_{u\in V} \binom{d(u)}{2} \;\le\; \binom{n}{2},$$

или

$$\sum_{u\in V} d(u)^2 \;\le\; n(n-1) + \sum_{u\in V} d(u). \tag{5}$$

Далее (и это типично для экстремальных задач такого рода) применяем неравенство Коши – Буняковского – Шварца к векторам $(d(u_1), \ldots, d(u_n))$ и $(1, 1, \ldots, 1)$:

$$\Big(\sum_{u\in V} d(u)\Big)^2 \;\le\; n\sum_{u\in V} d(u)^2.$$

Отсюда и из (5) следует, что

$$\Big(\sum_{u\in V} d(u)\Big)^2 \;\le\; n^2(n-1) + n\sum_{u\in V} d(u).$$

Учитывая (4), находим

$$4\,|E|^2 \;\;\le\;\; n^2(n-1) + 2n\,|E|,$$

или

$$|E|^2 - \frac{n}{2}|E| - \frac{n^2(n-1)}{4} \;\;\le\;\; 0.$$

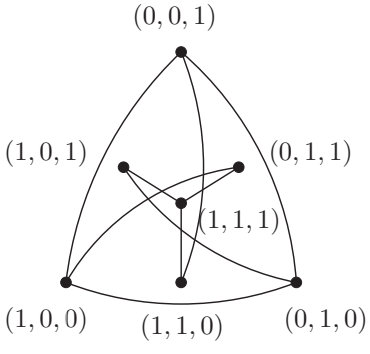
Решая соответствующее квадратное уравнение, получаем следующий результат Иштвана Реймана [6].

Теорема. *Если простой граф G с n вершинами не содержит 4-циклов, то*

$$|E| \;\;\le\;\; \left\lfloor \frac{n}{4}\left(1+\sqrt{4n-3}\right)\right\rfloor. \tag{6}$$

При $n = 5$ неравенство принимает вид $|E| \le 6$, и рассмотренный выше граф показывает, что равенство может иметь место.

Итак, двойной счет позволил легко получить оценку сверху для числа ребер. Но насколько хороша оценка (6) в общем случае? Следующий прекрасный пример (см. [2], [3], [6]) показывает, что она является почти точной. Как часто бывает в задачах такого рода, ответ подсказывает конечная геометрия.



Граф G_2: его вершинами являются все семь ненулевых троек (x, y, z).

Описывая пример, мы предполагаем, что читатель знает определение конечного поля $\mathbb{Z}_p$ целых чисел по простому модулю p (см. с. 27). Рассмотрим 3-мерное векторное пространство $X = \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$ над полем $\mathbb{Z}_p$. По пространству X построим граф G_p: его вершины — это одномерные подпространства $[\boldsymbol{v}] := \mathrm{span}_{\mathbb{Z}_p}\{\boldsymbol{v}\} = \{k\boldsymbol{v} : k \in \mathbb{Z}_p\}$, $\mathbf{0} \ne \boldsymbol{v} \in X$; подпространства[4] $[\boldsymbol{v}] = [(v_1, v_2, v_3)]$, $[\boldsymbol{w}] = [(w_1, w_2, w_3)]$ связаны ребром, если

$$\langle \boldsymbol{v}, \boldsymbol{w}\rangle \;=\; v_1w_1 + v_2w_2 + v_3w_3 \;=\; 0$$

(действия проводятся в $\mathbb{Z}_p$). Заметим, что не имеет значения, какой ненулевой вектор выбирается из подпространства. На геометрическом языке вершины G_p — *точки* проективной плоскости над $\mathbb{Z}_p$, и $[\boldsymbol{w}]$ смежна с $[\boldsymbol{v}]$, если $\boldsymbol{w}$ лежит на *полярной прямой* к $\boldsymbol{v}$.

Например, граф G_2 не имеет 4-циклов и содержит 9 ребер, что близко к оценке 10, которую дает неравенство (6). Мы хотим показать, что это верно для любого простого p.

[4] Не совпадающие. — *Прим. ред.*

Сначала докажем, что G_p не содержит 4-циклов. Если $[\boldsymbol{u}]$ — общий сосед $[\boldsymbol{v}]$ и $[\boldsymbol{w}]$, то $\boldsymbol{u} = (x, y, z)$ — решение системы линейных уравнений

$$\begin{aligned} v_1x + v_2y + v_3z &= 0,\\ w_1x + w_2y + w_3z &= 0. \end{aligned}$$

Так как $\boldsymbol{v}$ и $\boldsymbol{w}$ линейно независимы, то пространство решений имеет размерность 1 и, следовательно, общий сосед $[\boldsymbol{u}]$ единствен.

Далее, выясним, сколько вершин имеет граф G_p. Снова воспользуемся двойным счетом. Пространство X содержит $p^3 - 1$ ненулевых векторов. Так как каждое одномерное подпространство содержит $p - 1$ ненулевых векторов, то[5] X имеет $\frac{p^3-1}{p-1} = p^2 + p + 1$ одномерных подпространств, т. е. G_p имеет $n = p^2 + p + 1$ вершин. Аналогично, любое двумерное подпространство имеет $p^2 - 1$ ненулевых векторов и поэтому является объединением $\frac{p^2-1}{p-1} = p + 1$ одномерных подпространств.

Остается определить число ребер графа G_p или, что в силу (4) то же самое, полусумму степеней его вершин. По построению G_p вершины, смежные с $[\boldsymbol{u}]$, соответствуют решениям уравнения

$$u_1x + u_2y + u_3z = 0. \tag{7}$$

Множество решений уравнения (7) есть двумерное подпространство в X, оно является объединением $p+1$ одномерных подпространств. Если все они отличны от $[\boldsymbol{u}]$, то существует $p+1$ вершин графа G_p, смежных с $[\boldsymbol{u}]$; если же точки из $[\boldsymbol{u}]$ удовлетворяют (7), то существует ровно p вершин графа G_p, смежных с $[\boldsymbol{u}]$.

В итоге мы приходим к следующему выводу: если $\boldsymbol{u}$ лежит на *коническом сечении*, которое задается равенством $x^2 + y^2 + z^2 = 0$, то $d([\boldsymbol{u}]) = p$; в противном случае $d([\boldsymbol{u}]) = p + 1$. Поэтому осталось найти число одномерных подпространств на коническом сечении

$$x^2 + y^2 + z^2 = 0.$$

Воспользуемся утверждением, которое будет доказано позже.

> ***Утверждение.*** *Существует ровно p^2 решений (x, y, z) уравнения $x^2 + y^2 + z^2 = 0$ и, следовательно, ровно $\frac{p^2-1}{p-1} = p + 1$ вершин степени p в графе G_p.*

С его помощью завершим наш анализ G_p. В этом графе есть $p + 1$ вершин степени p и поэтому $(p^2 + p + 1) - (p + 1) = p^2$ вершин степени $p + 1$. Используя (4), получаем

$$\begin{aligned} |E| &= \frac{(p+1)p}{2} + \frac{p^2(p+1)}{2} = \frac{(p+1)^2p}{2} = \\ &= \frac{(p+1)p}{4}\,(1 + (2p+1)) = \frac{p^2+p}{4}\,(1 + \sqrt{4p^2+4p+1}). \end{aligned}$$

Полагая $n = p^2 + p + 1$, запишем последнее равенство в виде

$$|E| = \frac{n-1}{4}\,(1 + \sqrt{4n-3}),$$

и мы видим, что это мало отличается от (6).

[5] Так как множества ненулевых векторов одномерных подпространств попарно не пересекаются. — *Прим. ред.*

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Матрица для графа G_2

Теперь докажем утверждение. Следующее доказательство является прекрасным применением линейной алгебры, в том числе свойств симметричных матриц и их собственных чисел. Тот же метод будет использован в гл. 39, и это не простое совпадение: оба доказательства содержатся в одной и той же статье Эрдёша, Ре́ньи и Шош [3].

Представим одномерные подпространства пространства X, как и раньше, с помощью векторов $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{p^2+p+1}$, любые два из которых линейно независимы. Аналогично можно представить двумерные подпространства, используя *то же самое* множество векторов: множество точек подпространства, соответствующего вектору $\boldsymbol{u} = (u_1, u_2, u_3)$, есть множество решений уравнения $u_1x+u_2y+u_3z = 0$, как и в (7). (Конечно, это всего лишь принцип двойственности в линейной алгебре.) Отсюда и из (7) следует, что одномерное подпространство, представленное вектором $\boldsymbol{v}_i$, содержится в двумерном подпространстве, представленном вектором $\boldsymbol{v}_j$, тогда и только тогда, когда $\langle \boldsymbol{v}_i, \boldsymbol{v}_j \rangle = 0$.

Рассмотрим матрицу $A = (a_{ij})$ размера $(p^2+p+1)\times(p^2+p+1)$: строки и столбцы A соответствуют векторам $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{p^2+p+1}$ (мы используем одинаковую нумерацию строк и столбцов) и

$$a_{ij} \;:=\; \begin{cases} 1, & \text{если } \langle \boldsymbol{v}_i, \boldsymbol{v}_j \rangle = 0, \\ 0 & \text{в противном случае.} \end{cases}$$

Таким образом, A — вещественная симметричная матрица, и $a_{ii} = 1$ тогда и только тогда, когда $\langle \boldsymbol{v}_i, \boldsymbol{v}_i \rangle = 0$, т. е. когда $\boldsymbol{v}_i$ находится в коническом сечении $x^2 + y^2 + z^2 = 0$. Значит, нам остается показать, что сумма диагональных элементов матрицы A равна $p + 1$:

$$\operatorname{trace} A \;=\; p + 1.$$

(Действительно, каждый вектор $\boldsymbol{v}_i$, для которого $\langle \boldsymbol{v}_i, \boldsymbol{v}_i \rangle = 0$, порождает одномерное подпространство, содержащее $p - 1$ ненулевых решений уравнения $x^2 + y^2 + z^2 = 0$; эти подпространства пересекаются только по нулевому вектору, соответствующему нулевому решению уравнения. Поэтому уравнение $x^2 + y^2 + z^2 = 0$ имеет $1 + (p - 1)\operatorname{trace} A = 1 + (p - 1)(p + 1) = p^2$ решений. — *Прим. ред.*)

Из линейной алгебры известно, что след матрицы равен сумме ее собственных чисел. Нас ждет подарок судьбы: хотя A выглядит сложно, матрица A^2 легко вычисляется. Отметим два факта.

- Любая строка матрицы A содержит ровно $p+1$ единиц. Это означает, что A имеет собственное число, равное $p + 1$, так как $A\mathbf{1} = (p+1)\mathbf{1}$, где $\mathbf{1}$ — вектор, состоящий из единичных элементов.
- Для любых двух различных строк $\boldsymbol{v}_i, \boldsymbol{v}_j$ имеется только один столбец, содержащий единичные элементы в обеих строках (столбец соответствует единственному подпространству — линейной оболочке векторов $\boldsymbol{v}_i, \boldsymbol{v}_j$).

Используя эти факты, находим:

$$A^2 = \begin{pmatrix} p+1 & 1 & \cdots & 1 \\ 1 & p+1 & & \vdots \\ \vdots & & \ddots & \\ 1 & \cdots & & p+1 \end{pmatrix} \;=\; pI \;+\; J,$$

где I — единичная матрица, J — матрица, все элементы которой равны 1. Далее, J имеет следующие собственные числа: p^2+p+1 (кратности 1) и 0 (кратности p^2+p). Так как для матрицы pI все векторы — собственные с собственным числом p, то собственными числами A^2 являются: $p^2+2p+1=(p+1)^2$ (кратности 1) и p (кратности p^2+p). Так как A — вещественная симметричная матрица и, следовательно, ортогональным преобразованием приводится к диагональному виду, то A имеет одно собственное число, равное $p+1$ или $-(p+1)$, и p^2+p собственных чисел $\pm\sqrt{p}$. Согласно первому из двух приведенных выше фактов первое собственное число должно быть равно $p+1$. Предположим, что $\sqrt{p}$ имеет кратность r, а $-\sqrt{p}$ — кратность s. Тогда

$$\text{trace } A \;=\; (p+1)+r\sqrt{p}-s\sqrt{p}.$$

Остается заметить, что след A — целое число, а $\sqrt{p}$ — иррациональное; поэтому $r=s$, так что trace $A=p+1$. □

6. Лемма Шпернера

В 1912 году Лёйтзен Брауэр опубликовал свою знаменитую теорему о неподвижной точке [1]:

> *Каждая непрерывная функция $f\colon B^n \longrightarrow B^n$, отображающая n-мерный шар B^n в себя, имеет неподвижную точку (точку $\boldsymbol{x}\in B^n$, для которой $f(\boldsymbol{x})=\boldsymbol{x}$).*

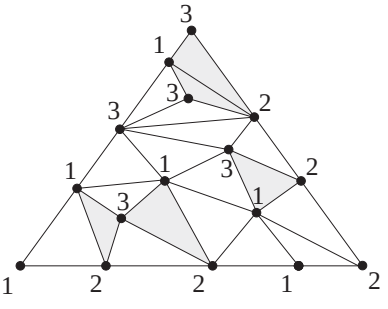
Для $n=1$, т. е. для интервала, это утверждение легко вытекает из теоремы о среднем значении, но для бóльших размерностей доказательство Брауэра использовало изощренные рассуждения. Поэтому настоящей неожиданностью явилась доказанная 1928 году молодым Эмануэлем Шпернером (ему тогда было 23 года) простая комбинаторная лемма [8], из которой можно вывести и теорему Брауэра о неподвижной точке, и инвариантность размерности при непрерывных отображениях. Кроме того, остроумная лемма Шпернера имеет красивое доказательство, основанное на двойном счете.

Мы обсудим лемму Шпернера и, как следствие, теорему Брауэра для первого интересного случая, каким является $n=2$. У читателя не должно возникнуть трудностей при обобщении доказательства на более высокие размерности (индукцией по размерности).

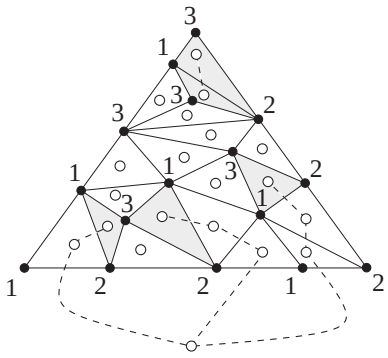
Лемма Шпернера. *Пусть некоторый «большой» треугольник с вершинами V_1, V_2, V_3 триангулирован, т. е. разбит на конечное число «малых» треугольников, любые два из которых либо имеют общую сторону, либо общую вершину, либо не пересекаются.*

Пусть вершины в триангуляции окрашены красками из множества $\{1,2,3\}$ так, что для каждого i вершина V_i окрашена в цвет i и при окраске вершин на ребре, соединяющем V_i и V_j $(i\neq j)$, используются лишь краски i и j, а внутренние вершины раскрашиваются в цвета 1, 2, 3 произвольным образом.

Тогда в триангуляции существует малый треугольник, все три вершины которого окрашены в различные цвета.



Треугольники, вершины которых окрашены в три различных цвета, заштрихованы.



■ **Доказательство.** Мы докажем более сильное утверждение: число трехцветных треугольников не просто положительно, а *нечетно*.

Рассмотрим граф, двойственный к триангуляции, и оставим в нем только те его ребра, которые пересекают стороны малых треугольников, соединяющие вершины с (различными) цветами 1 и 2. Тогда получится «частично двойственный граф». Все его вершины, лежащие в трехцветных треугольниках, имеют степень 1; степени вершин в треугольниках, окрашенных ровно в два цвета 1 и 2, равны 2, а у вершин в треугольниках, в окраске которых отсутствует хотя бы один из цветов 1 или 2, степень равна 0. Поэтому только трехцветные малые треугольники соответствуют вершинам нечетной степени (степени 1).

Вершина графа, лежащая во внешней области триангуляции, имеет нечетную степень. Действительно, на большом ребре, соединяющем V_1 и V_2, имеется нечетное число отрезков, концы которых окрашены в разные цвета 1 и 2. Таким образом, это большое ребро пересекает нечетное число ребер частично двойственного графа, а на других больших ребрах отсутствуют отрезки с концами двух цветов: 1 и 2.

Так как в силу равенства (4) число вершин нечетной степени в любом конечном графе четно, то число малых трехцветных треугольников, которым соответствуют внутренние вершины нечетной степени в частично двойственном графе, нечетно. □

С помощью этой леммы легко доказывается теорема Брауэра.

■ **Доказательство теоремы Брауэра о неподвижной точке (для $n=2$).** Пусть Δ — треугольник в $\mathbb{R}^3$ с вершинами $\boldsymbol{e}_1 = (1,0,0)$, $\boldsymbol{e}_2 = (0,1,0)$ и $\boldsymbol{e}_3 = (0,0,1)$. Так как Δ гомеоморфен двумерному шару (т. е. кругу) B^2, то нам достаточно доказать, что каждое непрерывное отображение $f\colon \Delta \longrightarrow \Delta$ имеет неподвижную точку.

Обозначим $\delta(\mathcal{T})$ максимальную длину ребер в триангуляции $\mathcal{T}$. Легко построить бесконечную последовательность триангуляций $\mathcal{T}_1, \mathcal{T}_2, \ldots$ треугольника Δ, для которой последовательность $\delta(\mathcal{T}_k)$ стремится к 0. Такую последовательность можно получить либо явно, либо индуктивно, например, выбирая в качестве $\mathcal{T}_{k+1}$ барицентрическое подразбиение триангуляции $\mathcal{T}_k$ (соединяя вершины каждого малого треугольника с точкой пересечения его медиан. — *Прим. ред.*).

В каждой из этих триангуляций каждой вершине $\boldsymbol{v}$ сопоставим цвет $\lambda(\boldsymbol{v}) := \min\{i : f(\boldsymbol{v})_i < v_i\} \in \{1,2,3\}$, т. е. $\lambda(\boldsymbol{v})$ — наименьший индекс i, для которого i-я компонента разности $f(\boldsymbol{v}) - \boldsymbol{v}$ отрицательна. Если f не имеет неподвижных точек, то цвета $\lambda(\boldsymbol{v})$ определяются корректно. Чтобы убедиться в этом, заметим, что каждая точка $\boldsymbol{v} \in \Delta$, $\boldsymbol{v} = (v_1, v_2, v_3)$, лежит в плоскости $x_1 + x_2 + x_3 = 1$, так что $\sum_i v_i = 1$. Поэтому при $f(\boldsymbol{v}) \neq \boldsymbol{v}$ и $f(\boldsymbol{v}) \in \Delta$ по крайней мере одна из координат вектора $f(\boldsymbol{v}) - \boldsymbol{v}$ должна быть отрицательной (и по меньшей мере одна — положительной).

Проверим, что так определенная окраска удовлетворяет предположениям леммы Шпернера. Во-первых, вершина $\boldsymbol{e}_i$ должна быть окрашена в цвет i, поскольку единственной возможной отрицательной компонентой вектора $f(\boldsymbol{e}_i) - \boldsymbol{e}_i$ является i-я. Более того, если точка $\boldsymbol{v}$ принадлежит ребру, противолежащему $\boldsymbol{e}_i$, то $v_i = 0$, так что i-я компонента $f(\boldsymbol{v}) - \boldsymbol{v}$ не может быть отрицательной, вследствие чего точка $\boldsymbol{v}$ окрашена в цвет, отличный от i.

Поэтому согласно лемме Шпернера в каждой триангуляции $\mathcal{T}_k$ существует трехцветный треугольник с множеством вершин $\{\boldsymbol{v}^{k:1}, \boldsymbol{v}^{k:2}, \boldsymbol{v}^{k:3}\}$, так что $\lambda(\boldsymbol{v}^{k:i}) = i,\ i = 1, 2, 3$. Последовательность точек $(\boldsymbol{v}^{k:1})_{k\geq 1}$ не обязана сходиться, но некоторая ее подпоследовательность имеет предел, так как симплекс Δ является компактом. Выберем из последовательности триангуляций $\mathcal{T}_k$ подпоследовательность, по которой $(\boldsymbol{v}^{k:1})$ сходится к точке $\boldsymbol{v} \in \Delta$, и для простоты сохраним для нее обозначение $\mathcal{T}_k$. Расстояния от точек $\boldsymbol{v}^{k:2}$ и $\boldsymbol{v}^{k:3}$ до $\boldsymbol{v}^{k:1}$ не превосходят величины $\delta(\mathcal{T}_k)$, которая стремится к 0. Следовательно, последовательности $\left(\boldsymbol{v}^{k:2}\right)_{k\geq 1}$ и $\left(\boldsymbol{v}^{k:3}\right)_{k\geq 1}$ сходятся к *той же самой* точке $\boldsymbol{v}$.

Но чему равно $f(\boldsymbol{v})$? Мы знаем, что для всех k первая координата $f(\boldsymbol{v}^{k:1})$ меньше первой координаты $\boldsymbol{v}^{k:1}$. Далее, так как f непрерывна, то первая координата $f(\boldsymbol{v})$ не больше первой координаты $\boldsymbol{v}$. Те же самые соображения применимы ко второй и третьей координатам. Поэтому у разности $f(\boldsymbol{v}) - \boldsymbol{v}$ нет положительных координат, а это, как мы уже видели, противоречит предположению $f(\boldsymbol{v}) \neq \boldsymbol{v}$. □

Литература

[1] Brouwer L. E. J. *Über Abbildungen von Mannigfaltigkeiten.* Math. Annalen, **71** (1912), 97–115.

[2] Brown W. G. *On graphs that do not contain a Thomsen graph.* Canadian Math. Bull., **9** (1966), 281–285.

[3] Erdős P., Rényi A., Sós V. *On a problem of graph theory.* Studia Sci. Math. Hungar., **1** (1966), 215–235.

[4] Erdős P., Szekeres G. *A combinatorial problem in geometry.* Compositio Math., (1935), 463–470.

[5] Hoşten S., Morris W. D. *The order dimension of the complete graph.* Discrete Math., **201** (1999), 133–139.

[6] Reiman I. *Über ein Problem von K. Zarankiewicz.* Acta Math. Acad. Sci. Hungar., **9** (1958), 269–273.

[7] Spencer J. *Minimal scrambling sets of simple orders.* Acta Math. Acad. Sci. Hungar., **22** (1971), 349–353.

[8] Sperner E. *Neuer Beweis für die Invarianz der Dimensionszahl und des Gebietes.* Abh. Math. Sem. Hamburg, **6** (1928), 265–272.

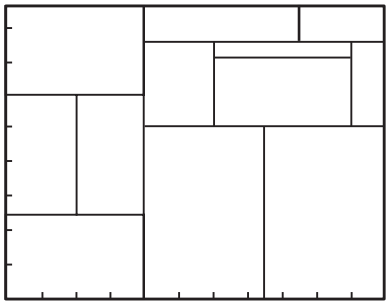
[9] Trotter W. T. *Combinatorics and Partially Ordered Sets: Dimension Theory.* John Hopkins University Press, Baltimore and London, 1992.

Глава 26 Плиточные разбиения прямоугольников

Некоторые математические теоремы имеют специфическое свойство: формулировка теоремы элементарна и проста, но попытки доказать ее будут безуспешными, пока Вы не откроете некую волшебную дверь, после чего все становится ясным и прозрачным.

Примером такой теоремы является следующее утверждение, принадлежащее Николасу де Брёйну [2].

> ***Теорема.*** *Если прямоугольник разбит на прямоугольники, у каждого из которых есть хотя бы одна сторона целочисленной длины, то и у этого прямоугольника есть сторона, длина которой — целое число.*



Длины сторон большого прямоугольника равны 11 и 8.5.

Под разбиением большого прямоугольника R на прямоугольники мы понимаем покрытие его содержащимися в нем прямоугольниками $T_1, \ldots, T_m$, не имеющими общих внутренних точек (как на чертеже на полях).

Фактически де Брёйн доказал следующее утверждение о разбиении прямоугольника размера $c \times d$ на одинаковые прямоугольники размера $a \times b$.

Если a, b, c, d — целые, то каждое из чисел a, b должно делить c или d.

Это утверждение можно доказать двукратным применением сформулированной выше более общей теоремы. После преобразования подобия с коэффициентом $\frac{1}{a}$ каждый малый прямоугольник будет иметь одну сторону, равную 1, и поэтому хотя бы одно из чисел $\frac{c}{a}$ и $\frac{d}{a}$ должно быть целым. Точно так же, применяя преобразование подобия с коэффициентом $\frac{1}{b}$, приходим к выводу о том, что хотя бы одно из чисел $\frac{c}{b}$ и $\frac{d}{b}$ должно быть целым.

Поиск доказательства теоремы почти каждый начнет с попытки провести индукцию по числу малых прямоугольников. Индукцию можно использовать, но при этом придется рассуждать очень аккуратно, и такой способ — не самый изящный. Например, в восхитительном обзоре [4] Стэн Вэган описал не менее четырнадцати разных доказательств, из которых мы выбрали три; ни одно из них не использует индукцию. Первое доказательство, по существу принадлежащее самому де Брёйну, основано на искусном аналитическом приеме. Второе доказательство Рихарда Рохберга и Шермана Штейна является дискретным упрощенным вариантом первого доказательства. Но чемпионом можно считать третье

доказательство, которое предложил Майкл Патерсон. Оно использует двойной счет (см. гл. 25) и почти умещается в одну строку.

Далее мы предполагаем, что стороны большого прямоугольника R параллельны осям x и y, а точка $(0,0)$ является его нижним левым углом.

■ **Первое доказательство.** Пусть T — произвольный прямоугольник на плоскости, который располагается от a до b вдоль оси x и от c до d вдоль оси y.

Прием де Брёйна состоит в следующем. Рассмотрим двойной интеграл по T:

$$\int_c^d \int_a^b e^{2\pi i(x+y)} dxdy. \tag{1}$$

Так как

$$\int_c^d \int_a^b e^{2\pi i(x+y)} dxdy = \int_a^b e^{2\pi ix} dx \int_c^d e^{2\pi iy} dy,$$

то интеграл (1) равен нулю тогда и только тогда, когда хотя бы один из интегралов $\int_a^b e^{2\pi ix} dx$ и $\int_c^d e^{2\pi iy} dy$ равен нулю.

Если мы покажем, что

$$\int_a^b e^{2\pi ixdx} = 0 \quad \Longleftrightarrow \quad b-a \text{ — целое число}, \tag{2}$$

то все будет сделано! Действительно, согласно предположению теоремы о виде разбиения каждый интеграл $\iint_{T_i}$ равен нулю и, следовательно, ввиду аддитивности интеграла также и $\iint_R = 0$, откуда заключаем, что R имеет целочисленную сторону.

$$\iint_R f(x,y)\,dxdy = \sum_i \iint_{T_i} f(x,y)\,dxdy$$

Аддитивность интеграла

Остается убедиться в справедливости (2). Так как

$$\int_a^b e^{2\pi ix} dx = \frac{1}{2\pi i} e^{2\pi ix}\Big|_a^b = \frac{1}{2\pi i}(e^{2\pi ib} - e^{2\pi ia}) = \frac{1}{2\pi i}(e^{2\pi i(b-a)} - 1),$$

то

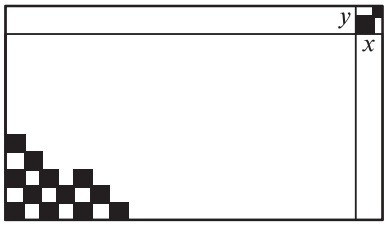
$$\int_a^b e^{2\pi ix} dx = 0 \quad \Longleftrightarrow \quad e^{2\pi i(b-a)} = 1. \tag{3}$$

Из формулы $e^{2\pi ix} = \cos 2\pi x + i \sin 2\pi x$ мы находим, что второе равенство в (3), в свою очередь, эквивалентно системе равенств

$$\cos 2\pi(b-a) = 1 \quad \text{и} \quad \sin 2\pi(b-a) = 0.$$

Так как равенство $\cos x = 1$ справедливо тогда и только тогда, когда x есть целое кратное 2π, то $b-a \in \mathbb{Z}$. Отсюда также вытекает, что $\sin 2\pi(b-a) = 0$. □

■ **Второе доказательство.** Раскрасим первую четверть плоскости как шахматную доску черными и белыми клетками размера $\frac{1}{2} \times \frac{1}{2}$, начав с



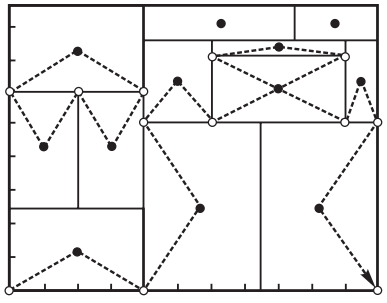
Площадь черной части в прямоугольнике в верхнем правом углу равна $\min\left(x, \frac{1}{2}\right) \cdot \min\left(y, \frac{1}{2}\right) + \max\left(x - \frac{1}{2}, 0\right) \cdot \max\left(y - \frac{1}{2}, 0\right)$, и она всегда больше $\frac{1}{2}xy$.

черной клетки с углом в начале координат $(0, 0)$. По предположению о разбиении в каждом малом прямоугольнике T_i площади белой и черной частей должны быть одинаковыми. Поэтому в большом прямоугольнике R площади белой и черной частей тоже должны быть одинаковыми.

Но тогда R должен иметь целочисленную сторону. В противном случае его можно разбить на четыре прямоугольника, в трех из которых площади черной и белой частей одинаковы, тогда как для четвертого прямоугольника в правом верхнем углу это не так. Действительно, если $x = a - \lfloor a \rfloor, y = b - \lfloor b \rfloor$, так что $0 < x, y < 1$, то площадь черной части в четвертом прямоугольнике больше площади белой части.

Это рассуждение иллюстрируется рисунком на полях. □

■ **Третье доказательство.** Пусть C — множество вершин малых прямоугольников, у которых обе координаты являются целыми числами (например, $(0, 0) \in C$). Пусть, далее, T — множество малых прямоугольников в разбиении R . Построим двудольный граф G с множеством вершин $C \cup T$, соединив ребром каждую точку $c \in C$ со всеми прямоугольниками из T, имеющими ее своей вершиной. Из условия теоремы следует, что каждый прямоугольник соединен с 0, 2 или 4 точками из C, так как если одна из вершин малого прямоугольника входит в C, то в C входит и другой конец его целочисленной стороны. Следовательно, граф G имеет *четное* число ребер.



Здесь изображен двудольный граф G с белыми вершинами из C и черными вершинами из T; пунктиром обозначены ребра.

Теперь рассмотрим множество C. Любая вершина, лежащая внутри R или на одной из его сторон, соединена ребрами с *четным* числом прямоугольников, но вершина $(0, 0)$ соединена лишь с одним прямоугольником. Поэтому должна существовать другая вершина $c \in C$ нечетной степени, а такой вершиной c может быть лишь одна из других вершин R. Доказательство закончено. □

Все три доказательства несложно перенести на n-мерный вариант утверждения де Брёйна:

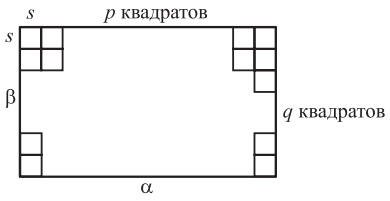
Если n-мерный прямоугольный параллелепипед R разбит на прямоугольные параллелепипеды так, что у каждого из них есть хотя бы одно ребро целочисленной длины, то у R тоже есть ребро целочисленной длины.

Однако в этой главе мы продолжим обсуждение разбиений плоских фигур и рассмотрим «дополнение» к утверждению де Брёйна; оно доказано Максом Деном [3] на много лет раньше и, несмотря на похожесть формулировки, основано на других идеях.

> ***Теорема.*** *Прямоугольник можно разбить на квадраты тогда и только тогда, когда отношение его сторон — рациональное число.*

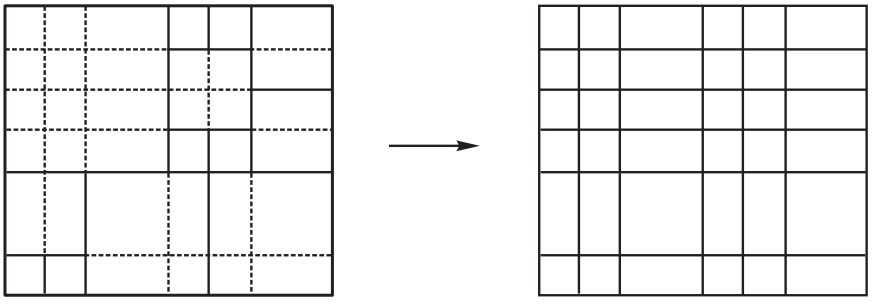
В одну сторону теорема доказывается просто. Предположим, что прямоугольник R имеет стороны, длины которых равны α и β, причем

$\frac{\alpha}{\beta} \in \mathbb{Q}$, т. е. $\frac{\alpha}{\beta} = \frac{p}{q}$, где $p, q \in \mathbb{N}$. Если $s = \frac{\alpha}{p} = \frac{\beta}{q}$, то можно разбить R на квадраты размера $s \times s$, как показано на полях.



Для доказательства в другую сторону Макс Ден применил то же элегантное рассуждение, которое он успешно использовал в своем решении третьей проблемы Гильберта (см. гл. 9). Эти две его статьи были опубликованы в журнале Mathematische Annalen с перерывом в 1 год.

■ **Доказательство.** Пусть R разбит на квадраты, возможно, со сторонами разной длины. Изменив масштаб, мы можем считать, что R — прямоугольник размера $a \times 1$. Допустим, что $a \notin \mathbb{Q}$, и покажем, что это приводит к противоречию. Первый шаг — продолжим стороны квадратов до границ R, как показано на рисунке.



Тем самым R разбивается на несколько малых прямоугольников; пусть $a_1, a_2, \ldots, a_m$ — длины их сторон (в любом порядке). Рассмотрим множество

$$A = \{1, a, a_1, \ldots, a_m\} \subseteq \mathbb{R}.$$

Следующая часть доказательства использует линейную алгебру. Пусть $V(A)$ — (конечномерное) векторное пространство всех линейных комбинаций чисел из A с рациональными коэффициентами. Заметим, что $V(A)$ содержит длины сторон всех квадратов исходного разбиения, так как длина каждой такой стороны есть сумма нескольких чисел a_i. Поскольку по предположению число a не является рациональным, мы можем дополнить пару $\{1, a\}$ до базиса B пространства $V(A)$:

$$B = \{b_1 = 1, b_2 = a, b_3, \ldots, b_m\}.$$

Определим функцию $f : B \to \mathbb{R}$, положив

$$f(1) := 1, f(a) := -1 \text{ и } f(b_i) := 0 \text{ для } i \geq 3,$$

и линейно продолжим ее на $V(A)$.

Линейное продолжение:

$$f(q_1 b_1 + \cdots + q_m b_m) := q_1 f(b_1) + \cdots + q_m f(b_m)$$

для $q_1, \ldots, q_m \in \mathbb{Q}$.

С помощью следующего определения «площади» (будем обозначать ее «area») прямоугольников доказательство завершается тремя простыми шагами. Для $c, d \in V(A)$ определим площадь прямоугольника размера $c \times d$ соотношением

$$\text{area}(\underset{c}{\boxed{}}\, d) = f(c)f(d).$$

(a) $\text{area}(\underset{c_1\ c_2}{\boxed{\vert}}\, d) = \text{area}(\underset{c_1}{\boxed{}}\, d) + \text{area}(\underset{c_2}{\boxed{}}\, d)$.

Это равенство немедленно вытекает из линейности f. Аналогичное утверждение, конечно, имеет место и для вертикальных полос.

(b) $\operatorname{area}(R) = \sum_{\text{квадраты}} \operatorname{area}(\square)$,
где сумма берется по всем квадратам разбиения.

В самом деле, отметим, что $\operatorname{area}(R)$ согласно (a) равна сумме площадей всех малых прямоугольников в разбиении, полученном при продолжении сторон квадратов. Поскольку всякий такой прямоугольник содержится в точности в одном из квадратов исходного разбиения, мы находим (снова с помощью (a)), что эта сумма равна также и правой части (b).

(c) Имеем

$$\operatorname{area}(R) = f(a)f(1) = -1,$$

но $\operatorname{area}(\underset{t}{\square}) = (f(t))^2 \geq 0$ для квадрата со стороной длины t, и поэтому

$$\sum_{\text{квадраты}} \operatorname{area}(\square) \geq 0,$$

и это есть искомое противоречие. □

Тем, кто хочет продолжить знакомство с миром разбиений, можно рекомендовать прекрасную обзорную статью [1] Федерико Ардилы и Рихарда Стенли.

Литература

[1] Ardila F., Stanley R. P. *Tilings.* Mathematical Intelligencer, **32** (2010), № 4, 32–43 [см. также http://arxiv.org/abs/math/0501170]

[2] de Bruin N. G. *Filling boxes with bricks* . Amer. Math. Monthly, **76** (1969), 37–40.

[3] Dehn M. *Über die Zerlegung von Rechtecken in Rechtecke.* Mathematische Annalen, **57** (1903), 314–332.

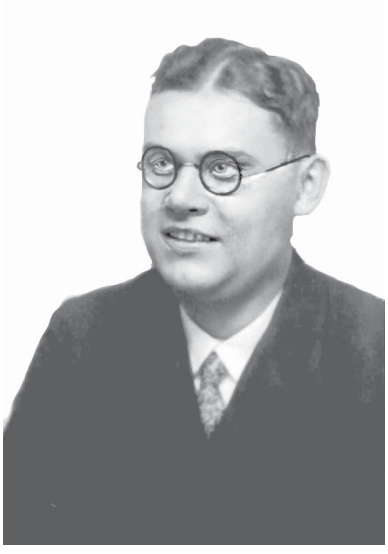
[4] Wagon S. *Fourteen proofs of a result about tiling a rectangle.* Amer. Math. Monthly, **94** (1987), 601–617.

«Новые классики:
Не наступать на линии!»

Три знаменитых теоремы о конечных множествах

Глава 27

В этой главе мы затрагиваем основную тему комбинаторики — свойства и размеры специальных семейств $\mathcal{F}$ подмножеств конечного множества $N = \{1, 2, \ldots, n\}$. Начнем с двух классических утверждений в этой области: теорем Шпернера и Эрдёша – Ко – Радо. Оба эти результата много раз передоказывались, и каждый из них положил начало новому направлению комбинаторной теории множеств. Кажется, что обе теоремы естественно доказывать индукцией, однако приводимые ниже рассуждения имеют совершенно другой характер и являются в полном смысле слова вдохновляющими.



Эмануэль Шпернер

В 1928 году Эмануэль Шпернер поставил и решил следующую задачу [8]. Пусть задано множество $N = \{1, 2, \ldots, n\}$. Назовем семейство $\mathcal{F}$ подмножеств множества N *антицепью*, если никакое множество из $\mathcal{F}$ не содержит другие множества этого семейства. Каков размер наибольшей антицепи? Ясно, что семейство $\mathcal{F}_k$ всех k-подмножеств множества N является антицепью, и $|\mathcal{F}_k| = \binom{n}{k}$. Выбирая максимальный биномиальный коэффициент (см. с. 20), находим, что существует антицепь размера $\binom{n}{\lfloor n/2 \rfloor} = \max_k \binom{n}{k}$. *Теорема Шпернера* утверждает, что антицепей бóльшего размера нет.

Теорема 1. *Размер наибольшей антицепи в n-множестве равен $\binom{n}{\lfloor n/2 \rfloor}$.*

■ **Доказательство.** Из многих доказательств следующее (принадлежащее Дэвиду Лабеллу [7]) является, вероятно, самым коротким и изящным. Пусть $\mathcal{F}$ — произвольная антицепь. Мы должны показать, что $|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$. Ключ к доказательству состоит в рассмотрении *цепи* подмножеств $\varnothing = C_0 \subset C_1 \subset C_2 \subset \ldots \subset C_n = N$, в которой $|C_i| = i$ при $i = 0, \ldots, n$. Сколько существует цепей? Ясно, что мы получим цепь, добавляя к пустому множеству последовательно элементы из N по одному, так что число цепей равно числу перестановок элементов множества N, а именно, $n!$ Далее, пусть множество $A \in \mathcal{F}$. Сколько существует цепей, проходящих через A? Ответ снова прост. Чтобы получить часть цепи от $\varnothing$ до A, мы должны добавлять к пустому множеству элементы множества A по одному, а затем, чтобы продолжить цепь от A до N, мы должны добавлять оставшиеся элементы из $N \setminus A$. Значит, если A содержит k элементов, то, рассматривая все пары таких отрезков цепи, мы находим, что число цепей, проходящих через A, равно $k!(n-k)!$ Заметим, что если $\mathcal{F}$ — антицепь, то не существует цепей, проходящих через два различных множества A и B из $\mathcal{F}$.

Чтобы завершить доказательство, обозначим через m_k число k-множеств в $\mathcal{F}$, так что $|\mathcal{F}| = \sum_{k=0}^{n} m_k$. Тогда из наших рассуждений

следует, что число цепей, пересекающихся с антицепью $\mathcal{F}$, равно

$$\sum_{k=0}^{n} m_k\, k!\,(n-k)!,$$

и это выражение не может быть больше числа $n!$ *всех* цепей. Значит,

$$\sum_{k=0}^{n} m_k \frac{k!(n-k)!}{n!} \;\leq\; 1, \qquad \text{или} \qquad \sum_{k=0}^{n} \frac{m_k}{\binom{n}{k}} \;\leq\; 1.$$

Проверьте, что при четных n семейство всех $\frac{n}{2}$-множеств (а при нечетных n два семейства всех $\frac{n-1}{2}$- и $\frac{n+1}{2}$-множеств) — это *все* антицепи максимального размера!

Заменяя в последней сумме все знаменатели наибольшим биномиальным коэффициентом, получаем

$$\frac{1}{\binom{n}{\lfloor n/2\rfloor}} \sum_{k=0}^{n} m_k \;\leq\; 1, \qquad \text{т. е.} \qquad |\mathcal{F}| \;=\; \sum_{k=0}^{n} m_k \;\leq\; \binom{n}{\lfloor n/2\rfloor},$$

и доказательство закончено. □

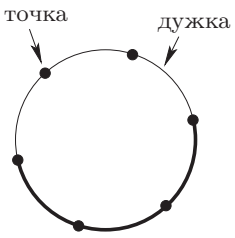
Наше второе утверждение имеет совершенно другую природу. Снова рассмотрим множество $N = \{1, \ldots, n\}$. Назовем семейство $\mathcal{F}$ подмножеств множества N *пересекающимся* , если любые два множества из $\mathcal{F}$ имеют по крайней мере один общий элемент. Несложно убедиться в том, что размер наибольшего пересекающегося семейства равен 2^{n-1}. Действительно, если $A \in \mathcal{F}$, то дополнение $A^c = N \backslash A$ имеет пустое пересечение с A и поэтому не может принадлежать $\mathcal{F}$. Отсюда вытекает, что пересекающее семейство содержит не более половины числа 2^n всех подмножеств, т. е. $|\mathcal{F}| \leq 2^{n-1}$. С другой стороны, семейство всех подмножеств, содержащих некоторый фиксированный элемент, например, семейство $\mathcal{F}_1$ всех подмножеств, содержащих 1, имеет объем $|\mathcal{F}_1| = 2^{n-1}$, и задача решена.

Но теперь поставим следующий вопрос. Как велико может быть пересекающееся семейство $\mathcal{F}$, если все множества в $\mathcal{F}$ имеют один и тот же размер, например, k? Назовем такие семейства *пересекающимися k-семействами*. Чтобы избежать тривиальных затруднений, предположим, что $n \geq 2k$, так как в противном случае любые два k-множества пересекаются и, следовательно, доказывать нечего! Используя предыдущую идею, мы, конечно, получим такое множество $\mathcal{F}_1$, рассматривая все k-множества, содержащие некоторый фиксированный элемент множества N, например, 1. Ясно, что мы получим все множества, входящие в $\mathcal{F}_1$, добавляя к 1 все $(k-1)$-подмножества множества $\{2, 3, \ldots, n\}$, в силу чего $|\mathcal{F}_1| = \binom{n-1}{k-1}$. Можно ли найти большее пересекающееся семейство? Нет, и в этом состоит утверждение теоремы Эрдёша – Ко – Радо.

Теорема 2. *Наибольший размер пересекающегося k-семейства в n-множестве равен $\binom{n-1}{k-1}$, если $n \geq 2k$.*

Пауль Эрдёш, Чао Ко и Рихард Радо получили этот результат в 1938 году, но не публиковали его в течение последующих 23 лет [2]. Затем появилось много доказательств и вариантов теоремы 2, но следующее рассуждение, принадлежащее Дьюле Катона [5], особенно изящно.

■ **Доказательство.** Ключ к доказательству — следующая простая лемма, которая на первый взгляд кажется совершенно не связанной с нашей задачей. Рассмотрим окружность C, разделенную n точками на n дужек. *Дуга* длины k окружности C состоит из $k+1$ последовательных точек и k дужек между ними.



Окружность C для $n = 6$. «Жирные» дужки изображают дугу длины 3.

Лемма. *Пусть $n \geq 2k$ и t различных дуг $A_1, \ldots, A_t$ длины k таковы, что любые две дуги имеют общую дужку. Тогда $t \leq k$.*

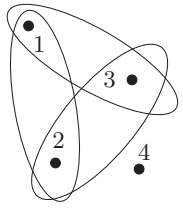
Для доказательства леммы заметим вначале, что любая из выделенных точек на окружности C является концом не более чем одной дуги. Действительно, пусть дуги A_i и A_j, $i \neq j$, имеют общую концевую точку v. Тогда эти дуги должны идти в разные стороны от v, так как они различны и имеют одинаковую длину. Но тогда A_i и A_j не могут иметь общих дужек, поскольку $n \geq 2k$.

Зафиксируем дугу A_1. Так как любая дуга A_i ($i \geq 2$) имеет с A_1 общую дужку, то один из концов A_i является внутренней точкой A_1. Как уже показано, все эти концевые точки должны быть разными. Поскольку A_1 имеет $k-1$ внутренних точек, число дуг, отличных от A_1, не больше $k-1$. Значит, общее число дуг не превосходит k. □

Теперь продолжим доказательство теоремы Эрдёша – Ко – Радо. Пусть $\mathcal{F}$ — пересекающееся k-семейство. Рассмотрим, как и выше, окружность C с n точками и n дужками. Зададим произвольную циклическую перестановку $\pi = (a_1, a_2, \ldots, a_n)$ чисел $1, \ldots, n$ и, двигаясь по часовой стрелке, припишем числа a_i дужкам C. Найдем число множеств $A \in \mathcal{F}$, элементы которых приписаны k *последовательным* дужкам C. Так как $\mathcal{F}$ — пересекающееся семейство, то согласно лемме существует не более k таких множеств. Это справедливо для любой циклической перестановки. Поэтому общее (по всем $(n-1)!$ циклическим перестановкам n-множества) число появлений множеств семейства $\mathcal{F}$ не превзойдет $k(n-1)!$

Сколько раз при этом появится фиксированное множество $A \in \mathcal{F}$? Понятно, что k-множество A появляется в π, если его элементы в цикловой записи π стоят подряд. Объединяя такую последовательность элементов множества A в новый элемент $*$, получим из π циклическую перестановку $(n-k+1)$-множества $N_A = \{*\} \cup N \setminus A$. Существует $(n-k)!$ циклических перестановок множества N_A и $k!$ возможных способов замены $*$ последовательностью элементов множества A. Отсюда вытекает, что фиксированное k-множество A входит ровно в $k!(n-k)!$ циклических перестановок, так что

$$|\mathcal{F}| \;\leq\; \frac{k(n-1)!}{k!(n-k)!} \;=\; \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} \;=\; \binom{n-1}{k-1}. \qquad \square$$



Пересекающееся семейство для $n = 4$, $k = 2$

Обязательно ли для максимального пересекающегося k-семейства существует элемент, принадлежащий всем множествам? Это заведомо не так для $n = 2k$. Например, при $n = 4$ и $k = 2$ семейство, состоящее из множеств $\{1,2\}, \{1,3\}, \{2,3\}$, тоже имеет размер $\binom{3}{1} = 3$. Вообще, при $n = 2k$ мы получим максимальное пересекающееся k-семейство размера $\frac{1}{2}\binom{n}{k} = \binom{n-1}{k-1}$, произвольно включая в него по одному из каждой пары множеств, состоящей из k-множества A и его дополнения $N \setminus A$. Но для $n > 2k$ совокупность максимальных пересекающихся k-семейств состо-

ит только из семейств множеств, содержащих фиксированный элемент. Читателю предлагается доказать это своими силами.

Наконец, обратимся к третьему утверждению, которое можно считать наиболее важной теоремой в теории конечных множеств: к теореме о выборе Филипа Холла, доказанной в 1935 году [3]. Из нее выросла современная теория паросочетаний. Эта теория имеет различные применения, часть из которых будет описана позднее.

Пусть X — конечное множество и $A_1, \ldots, A_n$ — совокупность подмножеств множества X (не обязательно различных). Назовем последовательность $x_1, \ldots, x_n$ *системой различных представителей* $\{A_1, \ldots, A_n\}$, если $x_1, \ldots, x_n$ — различные элементы из X и $x_i \in A_i$ для всех i. Разумеется, такая система (сокращенно СРП) может и не существовать (например, если одно из множеств A_i пусто). Теорема Холла дает точные условия, при которых СРП существует.

«Коллективная свадьба»

Прежде чем формулировать теорему, приведем интерпретацию, объясняющую ее фольклорное название *теорема о свадьбах*. Рассмотрим множество девушек $\{1, \ldots, n\}$ и множество X парней. Включение $x \in A_i$ означает, что девушка i и парень x не прочь пожениться, так что A_i есть множество всех возможных женихов девушки i. Тогда СРП соответствует коллективной свадьбе, когда каждая девушка выходит замуж за парня, который ей нравится.

Теперь сформулируем утверждение в терминах множеств.

Теорема 3. *Пусть $A_1, \ldots, A_n$ — совокупность подмножеств конечного множества X. Система различных представителей существует тогда и только тогда, когда объединение любых m множеств A_i содержит не менее m элементов при любом $m \in \{1, \ldots, n\}$.*

Ясно, что условие теоремы необходимо: если объединение каких-нибудь m множеств A_i содержит меньше m элементов, то эти множества нельзя представить различными элементами. Удивительно, что это очевидное условие является также достаточным.

Первоначальное доказательство Холла довольно сложное; позднее было предложено много других доказательств. Приведенное ниже доказательство (которое принадлежит Истерфилду [1] и переоткрыто Халмошем и Воханом [4]) кажется наиболее естественным.

■ **Доказательство.** Используем индукцию по n. Для $n = 1$ доказывать нечего. Пусть $n > 1$; предположим, что система множеств $\{A_1, \ldots, A_n\}$ удовлетворяет условию теоремы, которое мы для краткости обозначим (Н). При $1 \leq \ell < n$ назовем совокупность ℓ множеств A_i *критическим семейством*, если их объединение имеет мощность ℓ. Будем различать два случая.

Случай 1: Критические семейства отсутствуют.

Выберем произвольный элемент $x \in A_n$. Удалим x из X и рассмотрим совокупность $A'_1, \ldots, A'_{n-1}$, где $A'_i = A_i \backslash \{x\}$. Так как критических семейств не существует, то объединение любых m множеств A'_i содержит не менее m элементов. Тогда по предположению индукции существует СРП $x_1, \ldots, x_{n-1}$ совокупности $\{A'_1, \ldots, A'_{n-1}\}$, которая вместе с $x_n = x$ образует СРП для исходной совокупности.

Случай 2: Критические семейства существуют.

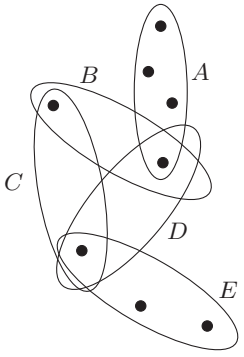
Без ограничения общности предположим, что $\{A_1, \ldots, A_\ell\}$ — критическое семейство. Тогда $\bigcup_{i=1}^{\ell} A_i = \widetilde{X}$ и $|\widetilde{X}| = \ell$. Так как $\ell < n$, то по предположению индукции для совокупности $A_1, \ldots, A_\ell$ существует СРП. Перенумеруем элементы множества $\widetilde{X}$ так, что $x_i \in A_i$ для всех $i \le \ell$.

Рассмотрим теперь оставшиеся множества $A_{\ell+1}, \ldots, A_n$ исходной совокупности и возьмем любые m из них. Согласно условию (H) объединение $A_1, \ldots, A_l$ и этих m множеств содержит не менее $l+m$ элементов. Поэтому выбранные m множеств содержат не менее m элементов из $X \backslash \widetilde{X}$. Другими словами, для семейства

$$A_{\ell+1} \backslash \widetilde{X}, \ \ldots \ , A_n \backslash \widetilde{X}$$

выполняется условие (H). Тогда по предположению индукции найдется СРП для $A_{\ell+1}, \ldots, A_n$, не содержащая элементов из $\widetilde{X}$. Вместе с $x_1, \ldots, x_\ell$ это дает СРП для всех множеств A_i.

Доказательство закончено. □



$\{B, C, D\}$ — критическое семейство

Как мы упоминали, теорема Холла положила начало обширной теории паросочетаний [6]. Из многих вариантов и ответвлений приведем особенно привлекательное утверждение, которое читатель может попытаться доказать самостоятельно.

> *Пусть все множества $A_1, \ldots, A_n$ имеют размер $k \ge 1$. Далее, пусть любой элемент содержится не более чем в k множествах. Тогда существуют такие k СРП, что для любого i все k представителей множества A_i различны и, следовательно, вместе образуют A_i.*

Прекрасный результат, который может открыть новые горизонты свадебных возможностей.

Литература

[1] Easterfield T. E. *A combinatorial algorithm.* J. London Math. Soc., **21** (1946), 219–226.

[2] Erdős P., Ko C., Rado R. Intersection theorems for systems of finite sets. Quart. J. Math. (Oxford), Ser. (2), **12** (1961), 313–320.

[3] Hall P. *On representatives of subsets.* J. London Math. Soc., **10** (1935), 26–30.

[4] Halmos P. R., Vaughan H. E. *The marriage problem.* Amer. J. Math., **72** (1950), 214–215.

[5] Katona G. *A simple proof of the Erdős-Ko-Rado theorem.* J. Combinatorial Theory, Ser. B, **13** (1972), 183–184.

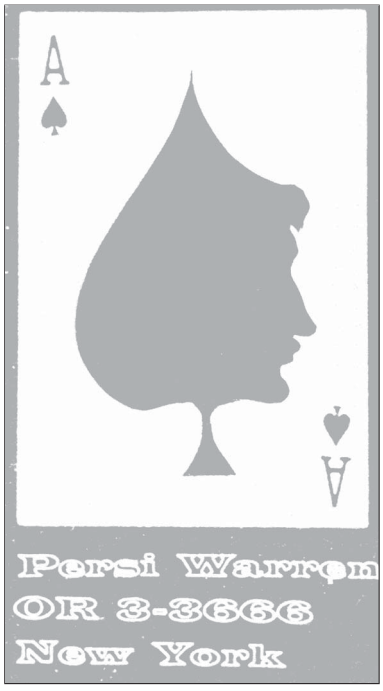
[6] Lovász L., Plummer M. D. *Matching Theory.* Akadémiai Kiadó, Budapest, 1986; русский перевод: Ловас Л., Пламмер М. *Прикладные задачи теории графов. Теория паросочетаний в математике, физике, химии.* М., Мир, 1998.

[7] Lubell D. *A short proof of Sperner's theorem.* J. Combinatorial Theory, **1** (1966), 299.

[8] Sperner E. *Ein Satz über Untermengen einer endlichen Menge.* Math. Zeitschrift, **27** (1928), 544–548.

Глава 28 Тасование карт

Сколько раз нужно тасовать колоду карт, чтобы она стала случайной?



Визитная карточка Перси Диакониса как фокусника. Позднее в интервью он заметил: «Если Вы скажете, что Вы профессор в Стэнфорде, то люди отнесутся к Вам с уважением. Если же Вы скажете, что придумываете фокусы, то они не захотят знакомить Вас со своей дочерью.»

Анализ случайных процессов — обычное дело как в жизни («Сколько времени занимает дорога до аэропорта в час пик?»), так и в математике. Конечно, получение осмысленных ответов в таких задачах в значительной степени зависит от постановки осмысленных вопросов. Для задачи тасования карт это означает, что мы должны:

- точно указать объем колоды (например, $n = 52$ карты),
- указать способ тасования (вначале мы рассмотрим тасование случайными сдвигами верхней карты, а затем более практичное и эффективное тасование вставкой), и, наконец,
- объяснить, какую колоду мы считаем «случайной» или «близкой к случайной».

Итак, наша цель в этой главе — анализ тасования вставкой, исследовавшегося Эдгардом Н.Гильбертом и Клодом Шенноном (1955 г., [6], не опубликовано) и Джимом Ридсом (1981 г., не опубликовано). Наше изложение следует статье [1] статистика Дэвида Олдуса и математика Перси Диакониса, который сначала был фокусником. Вместо точного окончательного результата (чтобы сделать колоду из 52 карт близкой к случайной, семи тасований вставками достаточно, а шести таких тасований не достаточно) мы получим в качестве верхней оценки числа тасований число 12. Попутно мы познакомимся с несколькими чрезвычайно красивыми идеями: с понятиями правил остановки и «строго равномерных» моментов остановки, с леммой о том, что строго равномерный момент остановки ограничивает расстояние по вариации, с леммой обращения Ридса и с интерпретацией тасования как обратной сортировки. В конце концов все сведется к двум классическим комбинаторным задачам, а именно, к задачам о собирании купонов и о парадоксе дней рождения. В путь!

Парадокс дней рождения

Рассмотрим n случайных человек, например, участников семинара. Какова вероятность того, что у всех них дни рождения разные? При обычных упрощающих предположениях (в году 365 дней, отсутствуют

сезонные эффекты, нет близнецов) эта вероятность равна

$$p(n) \;=\; \prod_{i=1}^{n-1}\Bigl(1-\frac{i}{365}\Bigr);$$

она меньше $\frac{1}{2}$ при $n=23$ (в этом и состоит «парадокс дней рождения»!), меньше 9% для $n=42$ и в точности равна нулю для $n>365$ («принцип Дирихле», см. гл. 22). Формулу для $p(n)$ легко вывести, если рассматривать людей в каком-нибудь фиксированном порядке. Если дни рождения первых i человек различны, то вероятность того, что $(i+1)$-й человек не нарушит это свойство, есть $1-\frac{i}{365}$, так как осталось $365-i$ не занятых дней рождения.

Аналогично, если n шаров независимо, случайно и равновероятно размещаются по K ячейкам, то вероятность того, что в каждую ячейку попадет не более одного шара, есть

$$p(n,K) \;=\; \prod_{i=1}^{n-1}\Bigl(1-\frac{i}{K}\Bigr).$$

Собирание купонов

Некоторые фирмы для увеличения продаж вкладывают в упаковки своих товаров разные картинки (купоны) и обещают выдавать премии покупателям, собравшим полные коллекции таких купонов. Если число различных видов купонов равно n, то сколько в среднем покупок придется сделать, чтобы собрать коллекцию из всех n видов купонов?

Другими словами, если мы случайно вынимаем шары из урны с n различными шарами, каждый раз возвращаем шар обратно и затем хорошо их перемешиваем, то сколько раз (в среднем) нам придется извлекать шары, пока каждый шар не будет извлечен хотя бы однажды?

Если мы уже извлекли k различных шаров, то вероятность не получить новый шар при следующем извлечении равна $\frac{k}{n}$. Поэтому вероятность того, что до появления следующего нового шара потребуется точно s извлечений, есть $(\frac{k}{n})^{s-1}(1-\frac{k}{n})$; следовательно, среднее число извлечений до появления следующего нового шара равно

$$\sum_{s\ge1}\Bigl(\frac{k}{n}\Bigr)^{s-1}\Bigl(1-\frac{k}{n}\Bigr)s \;=\; \frac{1}{1-\frac{k}{n}}\,,$$

как это вытекает из вычислений, приведенных на полях. Значит, среднее число извлечений до появления *всех* n различных шаров есть

$$\sum_{k=0}^{n-1}\frac{1}{1-\frac{k}{n}} \;=\; \frac{n}{n}+\frac{n}{n-1}+\cdots+\frac{n}{2}+\frac{n}{1} \;=\; nH_n \;\approx\; n\log n;$$

оценки для гармонических чисел H_n были получены в приложении к гл. 2. Таким образом, ответ в задаче о собирании купонов состоит в том, что в среднем потребуется примерно $n\log n$ извлечений.

В дальнейшем нам понадобится оценка для вероятности того, что придется сделать существенно больше $n\log n$ извлечений. Если V_n — число извлечений до появления всех шаров (это и есть случайная величина, математическое ожидание которой равно $E[V_n]\approx n\log n$), то для

$$\begin{aligned}\sum_{s\ge1}x^{s-1}(1-x)s \;&=\\ =\;\sum_{s\ge1}x^{s-1}s \;&-\;\sum_{s\ge1}x^s s\\ =\;\sum_{s\ge0}x^s(s+1) \;&-\;\sum_{s\ge0}x^s s\\ =\;\sum_{s\ge0}x^s \;&=\;\frac{1}{1-x},\end{aligned}$$

где в конце суммируется геометрический ряд (см. с. 47).

$n \ge 1$ и $c \ge 0$ вероятность того, что потребуется более $m := \lceil n \log n + cn \rceil$ извлечений, удовлетворяет неравенству

$$\mathrm{Prob}\big[V_n > m\big] \quad \le \quad e^{-c}.$$

Действительно, если событие A_i состоит в том, что шар i не появился при первых m извлечениях, то

$$\begin{aligned}\mathrm{Prob}\big[V_n > m\big] &= \mathrm{Prob}\Big[\bigcup_i A_i\Big] \le \sum_i \mathrm{Prob}\big[A_i\big] \\ &= n\Big(1-\frac{1}{n}\Big)^m < ne^{-m/n} \le e^{-c}.\end{aligned}$$

Простые вычисления показывают, что $\big(1-\frac{1}{n}\big)^n$ — возрастающая функция от n, стремящаяся к $1/e$ при $n \to \infty$. Поэтому $\big(1-\frac{1}{n}\big)^n < \frac{1}{e}$ при всех $n \ge 1$.

Рассмотрим теперь колоду из n карт. Перенумеруем их от 1 до n в том порядке, в котором они лежат, так что номер «1» получает верхняя карта колоды, а номер «n» — нижняя карта. С этого момента будем обозначать через $\mathfrak{S}_n$ множество всех перестановок чисел $1, \ldots, n$. *Тасование* колоды означает применение некоторой *случайной перестановки* к порядку карт. Идеально, это могло бы означать, что к исходному порядку $(1, 2, \ldots, n)$ применяется случайная перестановка π, выбираемая равновероятно из всех $n!$ перестановок множества $\mathfrak{S}_n$. Тогда после однократного применения такой перестановки мы получили бы колоду карт в порядке $\pi = (\pi(1), \pi(2), \ldots, \pi(n))$, который является совершенно случайным. Но в реальной жизни так не бывает. При тасовании обычно используются лишь «некоторые» перестановки (вообще говоря, не все из них берутся с одинаковой вероятностью), и это повторяется «некоторое» число раз. Мы надеемся, что после этого колода будет по крайней мере «близка к случайной».

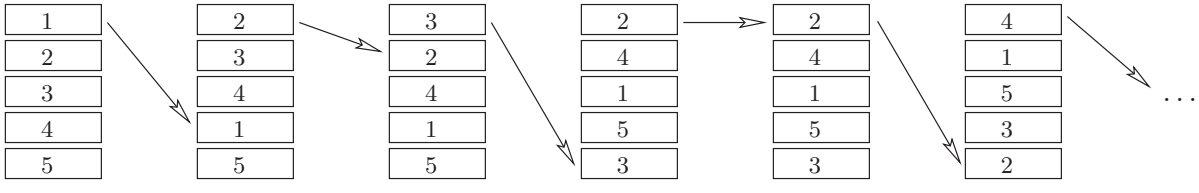
«Случайный сдвиг верхней карты»

Тасование случайными сдвигами верхней карты

Эти тасования выполняются так: верхняя карта снимается с колоды и вставляется обратно в одно из n возможных различных мест в колоде; каждое место выбирается с вероятностью $\frac{1}{n}$. Таким образом, применяется одна из перестановок

$$\tau_i \;=\; \big(2, 3, \ldots, \underset{\downarrow}{i}, 1, i{+}1, \ldots, n\big).$$

После одного такого тасования колода не выглядит случайной, и естественно ожидать, что для достижения нашей цели потребуется довольно много таких тасований. Типичный ход тасования сдвигами верхней карты для $n = 5$ выглядит следующим образом:



Как измерить «близость к случайности»? Вероятностники придумали «расстояние по вариации» как довольно строгую меру случайности. Рассмотрим распределение вероятностей на $n!$ различных упорядочениях нашей колоды или, что эквивалентно, на соответствующих им $n!$ различных перестановках $\sigma \in \mathfrak{S}_n$. Двумя примерами таких распределений являются исходное распределение E, которое задается равенствами

$$\begin{aligned} \mathsf{E}(\mathrm{id}) &= 1, \\ \mathsf{E}(\pi) &= 0 \quad \text{для всех } \pi \in \mathfrak{S}_n \setminus \{\mathrm{id}\}, \end{aligned}$$

(id — тождественная перестановка), и равномерное распределение U:

$$\mathsf{U}(\pi) = \tfrac{1}{n!} \quad \text{для всех } \pi \in \mathfrak{S}_n.$$

Расстояние по вариации между двумя вероятностными распределениями Q_1 и Q_2 на $\mathfrak{S}_n$ определяется формулой

$$\|\mathsf{Q}_1 - \mathsf{Q}_2\| := \tfrac{1}{2} \sum_{\pi \in \mathfrak{S}_n} |\mathsf{Q}_1(\pi) - \mathsf{Q}_2(\pi)|.$$

Полагая $S := \{\pi \in \mathfrak{S}_n : \mathsf{Q}_1(\pi) > \mathsf{Q}_2(\pi)\}$ и используя равенства $\sum_\pi \mathsf{Q}_1(\pi) = \sum_\pi \mathsf{Q}_2(\pi) = 1$, можно переписать эту величину в виде

$$\|\mathsf{Q}_1 - \mathsf{Q}_2\| = \max_{S \subseteq \mathfrak{S}_n} |\mathsf{Q}_1(S) - \mathsf{Q}_2(S)|,$$

где $\mathsf{Q}_i(S) := \sum_{\pi \in S} \mathsf{Q}_i(\pi)$. Ясно, что $0 \le \|\mathsf{Q}_1 - \mathsf{Q}_2\| \le 1$. В дальнейшем слова «близкая к случайности» мы будем понимать как «имеющая малое расстояние по вариации до равномерного распределения»[1]. Для исходного распределения E и равномерного распределения U расстояние по вариации очень близко к 1:

$$\|\mathsf{E} - \mathsf{U}\| = 1 - \tfrac{1}{n!}\,.$$

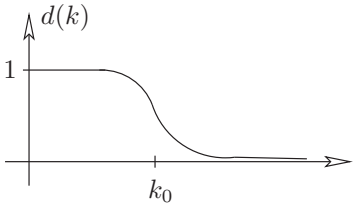
Расстояние между U и распределением колоды Top после одного тасования сдвигом верхней карты будет не намного лучше:

$$\|\mathsf{Top} - \mathsf{U}\| = 1 - \tfrac{1}{(n-1)!}.$$

Вероятностное распределение на $\mathfrak{S}_n$, которое получится после k-кратного тасования сдвигом верхней карты, будем обозначать Top^{*k}. Как ведет себя $\|\mathsf{Top}^{*k} - \mathsf{U}\|$, когда k растет, т. е. при повторении тасований? Аналогичный вопрос представляет интерес и для других способов тасования. Из общей теории (в частности, из теории цепей Маркова на конечных группах, см., например, книгу Берендса [3]) следует, что при $k \to \infty$ расстояние по вариации $d(k) := \|\mathsf{Top}^{*k} - \mathsf{U}\|$ стремится к нулю экспоненциально быстро, но при тасовании карт возникает интересный «пороговый эффект»: после некоторого числа k_0 тасований $d(k)$ очень быстро устремляется к нулю. График на полях в общих чертах описывает картину.

Для игрока в карты вопрос не в том, насколько близка к равномерности колода после миллиона тасований, а в том, достаточно ли семи тасований.

(Олдус, Диаконис [1])



[1] Следует четко понимать, что расстояние по вариации характеризует близость *вероятностных распределений*, а не самих случайных величин (как функций на пространстве элементарных событий Ω, см. приложение к гл. 15). Выражение «близкая к случайной» характеризует не конкретное состояние колоды, а его *распределение*. Например, даже случайная перестановка π с равномерным распределением U на $\mathfrak{S}_n$ с положительной вероятностью $\frac{1}{n!}$ принимает «заведомо не случайное» значение $(1, 2, \ldots, n)$. — *Прим. ред.*

Правила сильно равномерной остановки

Удивительная идея правил сильно равномерной остановки Олдуса и Диакониса схватывает самую суть дела. Допустим, что крупье в казино следит за процессом тасования, анализирует перестановки, применяемые к колоде на каждом шаге, и после некоторого числа шагов (зависящего от уже примененных перестановок) он говорит: «Стоп!». Иначе говоря, у него есть *правило остановки* для прерывания процесса тасования, зависящее лишь от уже проведенных (случайных) тасований. Правило остановки является *сильно равномерным*, если для всех $k \geq 0$ выполняется следующее условие:

> ***Если*** *процесс останавливается точно после k шагов,* ***то*** *перестановка колоды имеет равномерное распределение* (*точно*!).

Пусть T — число шагов до момента, когда согласно правилу остановки крупье говорит «Стоп!», так что T — случайная величина. Упорядочение колоды после k тасований задается случайной величиной X_k (со значениями в $\mathfrak{S}_n$). Правило остановки является сильно равномерным, если для всех допустимых значений k

$$\mathrm{Prob}\big[X_k = \pi \mid T = k\big] \;=\; \frac{1}{n!} \quad \text{для всех } \pi \in \mathfrak{S}_n.$$

Три обстоятельства делают это понятие интересным, полезным и удивительным.

1. Сильно равномерные правила остановки существуют. Во многих случаях они весьма просты.

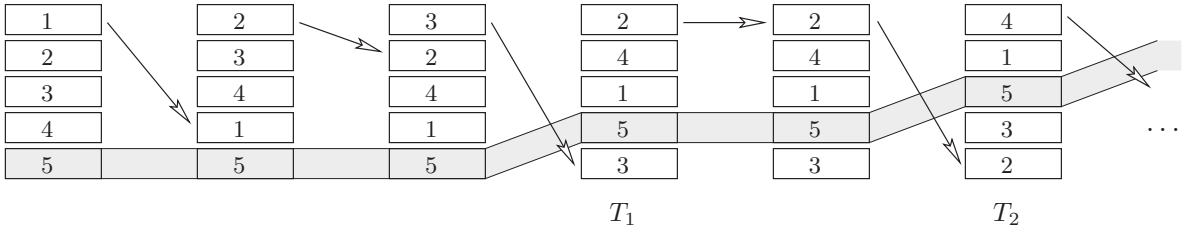
2. Более того, их можно исследовать. Попытки вычислить $\mathrm{Prob}[T > k]$ часто приводят к простым комбинаторным задачам.

3. Они дают эффективные оценки сверху для расстояний по вариации, например, для $d(k) = \|\mathsf{Top}^{*k} - \mathsf{U}\|$.

В частности, для тасований сдвигом верхней карты сильно равномерное правило остановки таково:

> «Остановиться, как только карта, которая вначале была внизу (имела метку n), впервые вставляется обратно в колоду.»

Действительно, если проследить за картой n во время этих тасований:



то легко заметить, что в течение всего процесса порядок карт, расположенных ниже карты n, имеет равномерное распределение.[2] Поэтому в момент, когда карта n оказывается сверху, порядок карт $1, \ldots, n-1$

[2] Точнее: для любого $M \subseteq \{1, \ldots, n-1\}$ при условии «ниже карты n лежит множество карт M» условная вероятность любого порядка карт в M (из $|M|!$ возможных порядков) равна $\frac{1}{M!}$. — *Прим. ред.*

Условные вероятности

Условная вероятность

$$\mathrm{Prob}[A \mid B]$$

— это вероятность события A при условии, что осуществилось событие B. Она равна отношению вероятности того, что осуществились оба события, и вероятности того, что осуществилось B:

$$\mathrm{Prob}[A \mid B] \;=\; \frac{\mathrm{Prob}[A \wedge B]}{\mathrm{Prob}[B]}.$$

имеет равномерное распределение, а после того, как карта n снимается и равновероятно вставляется обратно, распределение всей колоды становится равномерным. Мы не знаем, когда это происходит (но крупье, следящий за положением карты n, может определить этот момент).

Пусть теперь T_i — случайная величина, равная числу тасований до момента, когда впервые ниже карты n оказывается i карт. Нам нужно найти распределение суммы

$$T \;=\; T_1 + (T_2 - T_1) + \ldots + (T_{n-1} - T_{n-2}) + (T - T_{n-1}).$$

Слагаемые в ней связаны с задачей о собирании купонов: $T_i - T_{i-1}$ есть время до момента, когда верхняя карта вставляется в одно из i возможных мест ниже карты n. Оно имеет такое же распределение, как время, за которое коллекционер, имея $(n-i)$ видов купонов, приобретает новый вид купона. Пусть V_i — число купонов, купленных к моменту приобретения i различных купонов. Тогда

$$V_n \;=\; V_1 + (V_2 - V_1) + \ldots + (V_{n-1} - V_{n-2}) + (V_n - V_{n-1}),$$

и, как мы заметили, $\mathrm{Prob}[T_i - T_{i-1} = j] = \mathrm{Prob}[V_{n-i+1} - V_{n-i} = j]$ для всех i и j. Значит, коллекционирование купонов и тасование колоды с помощью случайных сдвигов верхней карты порождают эквивалентные последовательности независимых случайных величин, хотя и в обратном порядке (при собирании купонов дольше ждать приходится в конце). Таким образом, сильно равномерное правило остановки для тасования сдвигом верхней карты срабатывает после более чем $k = \lceil n \log n + cn \rceil$ шагов с вероятностью, которая при больших c мала:

$$\mathrm{Prob}\big[T > k\big] \;\le\; e^{-c}.$$

Следующая простая, но важная лемма показывает, что после $k = \lceil n \log n + cn \rceil$ тасований перемещением верхней карты наша колода становится «близкой к случайной» с расстоянием по вариации

$$d(k) \;=\; \|\mathsf{Top}^{*k} - \mathsf{U}\| \;\le\; e^{-c}.$$

Лемма. *Пусть* $\mathsf{Q} : \mathfrak{S}_n \longrightarrow \mathbb{R}$ *— любое распределение вероятностей, определяющее процесс тасования* Q^{*k} *с сильно равномерным правилом остановки и моментом остановки* T*. Тогда для всех* $k \ge 0$

$$\|\mathsf{Q}^{*k} - \mathsf{U}\| \;\le\; \mathrm{Prob}\big[T > k\big].$$

■ **Доказательство.** Пусть X — случайная величина, принимающая значения в $\mathfrak{S}_n$ с распределением вероятностей Q; вероятность попадания X в множество $S \subseteq \mathfrak{S}_n$ будем обозначать $\mathsf{Q}(S)$. Итак, $\mathsf{Q}(S) = \mathrm{Prob}[X \in S]$, и в случае равномерного распределения $\mathsf{Q} = \mathsf{U}$

$$\mathsf{U}(S) \;=\; \mathrm{Prob}\big[X \in S\big] \;=\; \frac{|S|}{n!}\,.$$

Для каждого подмножества $S \subseteq \mathfrak{S}_n$ рассмотрим вероятность того, что после k шагов колода упорядочена согласно перестановке из S:

$$\begin{aligned}
\mathsf{Q}^{*k}(S) &= \mathrm{Prob}[X_k \in S] \\
&= \sum_{j \le k} \mathrm{Prob}[X_k \in S \ \wedge\ T = j] \ +\ \mathrm{Prob}[X_k \in S \ \wedge\ T > k] \\
&= \sum_{j \le k} \mathsf{U}(S)\,\mathrm{Prob}[T = j] \ +\ \mathrm{Prob}[X_k \in S \,|\, T > k] \cdot \mathrm{Prob}[T > k] \\
&= \mathsf{U}(S)\,(1 - \mathrm{Prob}[T > k]) \ +\ \mathrm{Prob}[X_k \in S \,|\, T > k] \cdot \mathrm{Prob}[T > k] \\
&= \mathsf{U}(S) \ +\ \big(\mathrm{Prob}[X_k \in S \,|\, T > k] - \mathsf{U}(S)\big) \cdot \mathrm{Prob}[T > k].
\end{aligned}$$

Отсюда вытекает, что для любого $S \subseteq \mathfrak{S}_n$

$$|\mathsf{Q}^{*k}(S) - \mathsf{U}(S)| \ \le\ \mathrm{Prob}[T > k],$$

так как разность двух вероятностей

$$\mathrm{Prob}[X_k \in S \,|\, T > k] \ -\ \mathsf{U}(S)$$

по абсолютной величине не превосходит 1. □

На этом мы завершим анализ тасования случайными сдвигами верхней карты. Мы получили следующую оценку сверху для меры близости колоды к «случайной» после k тасований.

Теорема 1. *Пусть $c \ge 0$ и $k := \lceil n \log n + cn \rceil$. Тогда после k тасований колоды объема n сдвигами верхней карты расстояние по вариации от равномерного распределения удовлетворяет неравенству*

$$d(k) \ :=\ \|\mathsf{Top}^{*k} - \mathsf{U}\| \ \le\ e^{-c}.$$

Можно проверить также, что расстояние по вариации $d(k)$ остается большим, если число случайных тасований сдвигом верхней карты существенно меньше $n \log n$. Дело в том, что при таком числе тасований с положительной вероятностью сохраняется относительное расположение нескольких самых нижних карт в колоде.

Конечно, тасования сдвигом верхней карты крайне неэффективны: согласно оценке из теоремы 1 требуется не менее $n \log n + n \approx 257$ таких тасований для не слишком плохого ($d(257) \le e^{-1}$) перемешивания колоды с $n = 52$ картами. Поэтому теперь мы переключим наше внимание на более интересную и реалистичную модель тасования.

«Тасование вставками»

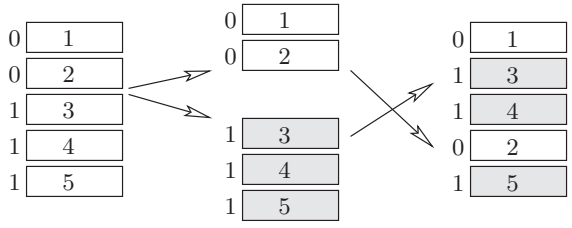
Тасования вставками

Вот что делают крупье в казино при раздаче карт. Берут колоду, разбивают ее на две части и затем вставляют их одна в другую, например, сбрасывая нерегулярным образом нижние карты то из одной, то из другой части колоды.

Тасование вставками тоже порождает некоторую перестановку карт в колоде, которые мы предполагаем изначально помеченными номерами от 1 до n, где 1 — номер верхней карты. Тасования вставками соответствуют таким перестановкам $\pi \in \mathfrak{S}_n$, что последовательность

$$(\pi(1), \pi(2), \ \ldots\ , \pi(n))$$

состоит из двух возрастающих подпоследовательностей (она образует одну возрастающую последовательность лишь для тождественной перестановки). Для колоды из n карт существует ровно $2^n - n$ различных тасований вставками.



Действительно, если колода карт разбита так, что t верхних карт взяты в правую руку ($0 \le t \le n$), а остальные $n - t$ карт — в левую руку, то существует $\binom{n}{t}$ способов вставить эти части одна в другую, и все они порождают различные перестановки (за исключением того, что при каждом из $n + 1$ значений t существует ровно одна возможность получить тождественную перестановку).

Не ясно, каким распределением вероятностей следует описывать тасование вставками: однозначного ответа нет, так как любители и профессионалы тасуют по-разному. Однако следующая модель, разработанная впервые Эдгардом Н. Гильбертом и Клодом Шенноном в 1955 г. (работавшими тогда в легендарном отделе «Математика связи» Лабораторий Белла), имеет несколько достоинств:

- она изящна, проста и кажется естественной,
- она хорошо описывает используемый любителями вариант тасования вставками,
- она допускает возможность анализа.

Дадим три описания модели; они определяют одно и то же вероятностное распределение Rif на $\mathfrak{S}_n$:

1. $\mathsf{Rif} : \mathfrak{S}_n \longrightarrow \mathbb{R}$ определяется соотношениями

$$\mathsf{Rif}(\pi) \quad := \quad \begin{cases} \frac{n+1}{2^n}, & \text{если } \pi = \mathrm{id}, \\ \frac{1}{2^n}, & \text{если } \pi \ne \mathrm{id} \text{ и состоит из двух возрастающих} \\ & \text{последовательностей}, \\ 0 & \text{в противном случае.} \end{cases}$$

2. С вероятностью $\frac{1}{2^n}\binom{n}{t}$ снять с колоды верхние t карт, взять их в правую руку, а остаток колоды — в левую руку. Далее проводить следующие операции, пока колоды в руках не опустеют: если в правой руке r карт, а в левой руке ℓ карт, то с вероятностью $\frac{r}{r+\ell}$ сбросить нижнюю карту из колоды в правой руке и с вероятностью $\frac{\ell}{r+\ell}$ — из колоды в левой руке.

3. При *обратном тасовании* в колоде нужно выбрать подмножество карт, удалить его из колоды и положить поверх оставшихся карт, сохраняя при этом порядок в обеих ее частях. Такое тасование определяется выбранным подмножеством карт; все подмножества нужно выбирать с одной и той же вероятностью. Для равновероятного выбора подмножества можно приписать каждой карте случайно и

Обратное тасование задает перестановки $\pi = (\pi(1), \ldots, \pi(n))$, элементы которых возрастают, за исключением не более одного убывания. (Лишь тождественная перестановка не имеет убываний.)

независимо от других карт метку «0» или «1» с вероятностью $\frac{1}{2}$; после этого нужно переместить карты с меткой «0» на верх колоды с сохранением их порядка.[3]

Легко видеть, что эти описания приводят к одному и тому же вероятностному распределению. Чтобы убедиться в эквивалентности первого и третьего описаний, достаточно заметить, что тождественная перестановка получается тогда и только тогда, когда все карты с меткой «0» находятся в колоде выше всех карт с меткой «1».

Модель определена. Как ее исследовать? Сколько тасований вставками необходимо, чтобы порядок карт в колоде стал близким к случайному? Мы не будем искать точный, наилучший возможный ответ, а получим вполне удовлетворительный результат в три этапа:

(1) рассматриваем обратные тасования вставками вместо прямых,

(2) для них описываем сильно равномерное правило остановки,

(3) показываем, что парадокс о днях рождения — ключ к решению!

Теорема 2. *После k тасований вставками колоды из n карт расстояние по вариации от равномерного распределения удовлетворяет неравенству*

$$\|\mathsf{Rif}^{*k} - \mathsf{U}\| \quad \leq \quad 1 - \prod_{i=1}^{n-1} \left(1 - \frac{i}{2^k}\right).$$

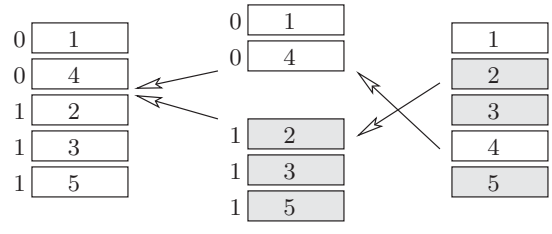
■ **Доказательство.** (1) Рассмотрим обратные тасования вставками и оценим, как быстро они переводят исходное распределение в окрестность равномерного. Обратным тасованиям соответствует распределение вероятностей на $\mathfrak{S}_n$, определяемое равенством $\overline{\mathsf{Rif}}(\pi) := \mathsf{Rif}(\pi^{-1})$.

Далее, поскольку каждая перестановка имеет единственную обратную и $\mathsf{U}(\pi) = \mathsf{U}(\pi^{-1})$, получаем:

$$\|\mathsf{Rif}^{*k} - \mathsf{U}\| \quad = \quad \|\,\overline{\mathsf{Rif}}^{*k} - \mathsf{U}\|.$$

(Это и есть лемма обращения Ридса!)

(2) При каждом обратном тасовании вставками каждой карте сопоставляется знак 0 или 1:



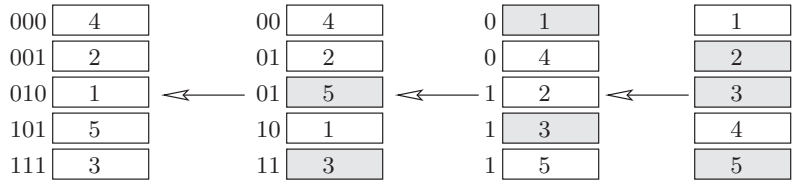
[3] Нетрудно проверить, что множество перестановок, порождаемых обратным тасованием, совпадает с множеством перестановок, обратных к перестановкам, порождаемым тасованием вставками. При этом вероятности, приписываемые взаимно обратным перестановкам схемой тасования вставками и схемой обратного тасования, одинаковы. В частности, при обратном тасовании тождественная перестановка получается тогда и только тогда, когда все 0-карты находятся выше всех карт, имеющих метку 1, и вероятность этого события равна $\frac{n+1}{2^n}$. — *Прим. ред.*

Если запомнить эти знаки (например, записать их прямо на картах), то после k обратных тасований на каждой карте окажется упорядоченная цепочка из k знаков. Правило остановки звучит так:

> «Остановиться, как только на всех картах окажутся разные цепочки.»

Когда это происходит, карты в колоде оказываются *рассортированными* в соответствии с двоичными числами $b_k b_{k-1} \dots b_2 b_1$, где b_i — бит, который карта получила при i-м обратном тасовании. Так как эти биты случайны, равновероятны и независимы, то указанное правило остановки сильно равномерно.

В следующем примере с $n = 5$ картами число обратных тасований до остановки $T = 3$.



(3) Распределение момента остановки T при этом правиле остановки связано с парадоксом дней рождения для $K = 2^k$. Будем помещать две карты в одну и ту же ячейку, если они имеют одинаковые цепочки $b_k b_{k-1} \dots b_2 b_1 \in \{0,1\}^k$. Таким образом, число ячеек $K = 2^k$, вероятность того, что хотя бы в одной ячейке окажется более одной карты, равна

$$\mathrm{Prob}[T > k] \quad = \quad 1 - \prod_{i=1}^{n-1} \left(1 - \frac{i}{2^k}\right),$$

и в силу леммы эта величина является верхней оценкой для расстояния по вариации $\|\mathsf{Rif}^{*k} - \mathsf{U}\| = \|\,\overline{\mathsf{Rif}}^{*k} - \mathsf{U}\|$. □

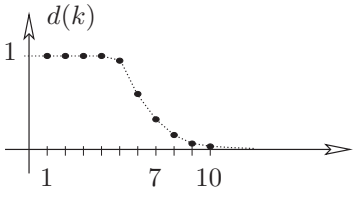
Итак, сколько же раз следует тасовать? Для больших n требуется примерно $k = 2\log_2(n)$ тасований. В самом деле, полагая $k := 2\log_2(cn)$ для некоторого $c \geq 1$, мы находим (проводя несложные вычисления), что $P[T > k] \approx 1 - e^{-\frac{1}{2c^2}} \approx \frac{1}{2c^2}$.

Для $n = 52$ карт явная оценка сверху из теоремы 2 дает: $d(10) \leq 0.73$, $d(12) \leq 0.28$, $d(14) \leq 0.08$, так что $k = 12$ тасований обеспечивают «достаточную случайность» для всех практических целей. Но «на практике» не обязательно производить 12 тасований, и в действительности, как показывает более детальный анализ, это не требуется (результаты приведены на полях). Исследование тасований вставками есть часть продолжающейся дискуссии о правильном понимании того, что есть «достаточно случайно». Работа Диакониса [4] содержит обзор недавних результатов.

Важно ли это? Да, важно. Даже после трех хороших тасований вставками перемешанная колода с $n = 52$ картами выглядит вполне случайной ..., но это не так. Мартин Гарднер [5, гл. 7] описал ряд удивительных карточных фокусов, основанных на скрытом порядке в такой колоде!

k	$d(k)$
1	1.000
2	1.000
3	1.000
4	1.000
5	0.952
6	0.614
7	0.334
8	0.167
9	0.085
10	0.043

Расстояние по вариации после k обратных тасований в соответствии с [2]



Литература

[1] Aldous D., Diaconis P. *Shuffling cards and stopping times.* Amer. Math. Monthly, **93** (1986), 333–348.

[2] Bayer D., Diaconis P. *Trailing the dovetail shuffle to its lair.* Annals Applied Probability, **2** (1992), 294–313.

[3] Behrends E. *Introduction to Markov Chains.* Vieweg, Braunschweig/ Wiesbaden, 2000.

[4] Diaconis P. *Mathematical developments from the analysis of riffle shuffling.* В: «Groups, Combinatorics and Geometry. Durham 2001» (Ivanov A. A., Liebeck M. W., Saxl J., eds.), World Scientific, Singapore, 2003, pp. 73–97.

[5] Gardner M. *Mathematical Magic Show.* Knopf, New York/Allen & Unwin, London, 1977.

[6] Gilbert E. N. *Theory of Shuffling.* Technical Memorandum, Bell Laboratories, Murray Hill, NJ, 1955.

«Достаточно случайно?»

Пути на решетке и определители

Глава 29

Суть математики заключается в доказательстве теорем, и математики занимаются именно этим: доказывают теоремы. Но, по правде говоря, на самом деле они мечтают хотя бы раз в жизни доказать *Лемму*, подобную Лемме Фату в анализе, Лемме Гаусса в теории чисел или Лемме Бернсайда – Фробениуса в комбинаторике.

Что делает математическое утверждение истинной Леммой? Во-первых, оно должно быть применимо к широкому кругу задач, даже к таким, которые кажутся никак с ним не связанными. Во-вторых, формулировка утверждения должна казаться совершенно очевидной. Оно может вызывать у читателя легкое чувство зависти: почему я не заметил этого прежде? И в-третьих, на эстетическом уровне, Лемма, включая ее доказательство, должна быть прекрасной!

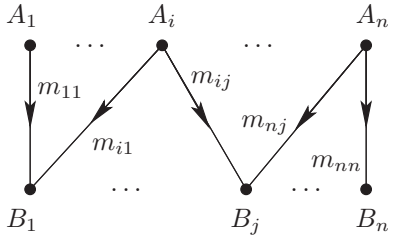
В этой главе мы рассмотрим один из таких изумительных примеров: перечислительную лемму, впервые появившуюся в 1972 г. в статье Бернта Линдстрема [2]. Тогда она осталась незамеченной, но мгновенно стала классической в 1985 г., когда Ира Гессель и Герард Вьеннот переоткрыли ее и в замечательной статье [1] показали, что она применима к многим трудным комбинаторным перечислительным задачам.

Начнем с обычного перестановочного представления определителя матрицы. Если $M = (m_{ij})$ — вещественная $n \times n$-матрица, то

$$\det M \;=\; \sum_{\sigma} \operatorname{sign}\sigma \; m_{1\sigma(1)}\, m_{2\sigma(2)} \cdots m_{n\sigma(n)}, \tag{1}$$

где $\sigma = (\sigma(1), \sigma(2), \ldots, \sigma(n))$ пробегает все перестановки множества $\{1, 2, \ldots, n\}$, и $\operatorname{sign}\sigma$ равен 1 или -1 в зависимости от того, является σ произведением четного или нечетного числа транспозиций.

Теперь рассмотрим *ориентированные двудольные графы с весами*. Пусть вершины $A_1, \ldots, A_n$ соответствуют строкам матрицы M, а $B_1, \ldots, B_n$ — столбцам. Каждую пару вершин A_i и B_j соединим ребром, исходящим из A_i и входящим в B_j, и снабдим его весом m_{ij}, как на рисунке. Формула (1) имеет следующую интерпретацию.



- Левая часть (1) есть определитель *матрицы путей* $M = (m_{ij})$, где m_{ij} есть *вес* $w(A_i \to B_j)$ единственного ориентированного пути из A_i в B_j.

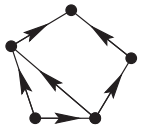
- Правая часть (1) есть знакопеременная сумма весов всех *систем путей из* $\mathcal{A} = \{A_1, \ldots, A_n\}$ *в* $\mathcal{B} = \{B_1, \ldots, B_n\}$ *без общих вершин*. Система путей $\mathcal{P}_\sigma$ задается путями $A_1 \to B_{\sigma(1)}, \ \ldots \ , A_n \to B_{\sigma(n)}$, и *вес* системы путей $\mathcal{P}_\sigma$ есть произведение весов отдельных путей:

$$w(\mathcal{P}_\sigma) \;=\; w(A_1 \to B_{\sigma(1)}) \;\cdots\; w(A_n \to B_{\sigma(n)}).$$

В этой интерпретации формула (1) принимает вид

$$\det M \;=\; \sum_{\sigma} \operatorname{sign}\sigma \; w(\mathcal{P}_\sigma).$$

В чем же состоит результат Гессель и Вьеннота? Он дает естественное обобщение формулы (1) с двудольных графов на произвольные. Именно этот шаг сильно расширил область применения Леммы; к тому же ее доказательство ошарашивающе просто и элегантно.



Ациклический ориентированный граф

Вначале соберем необходимые понятия. Пусть $G = (V, E)$ — конечный ориентированный *ациклический граф*; в ациклическом графе нет ориентированных циклов и поэтому для любых вершин A и B существует лишь конечное число ориентированных путей $A \longrightarrow B$ из A в B, включая все тривиальные пути $A \longrightarrow A$ длины 0. Каждому ребру e приписан вес $w(e)$. Запись $P : A \to B$ означает, что P — ориентированный путь из A в B. Определим *вес* пути P равенством

$$w(P) \;:=\; \prod_{e\in P} w(e),$$

полагая $w(P) = 1$, если P — путь длины 0.

Пусть теперь $\mathcal{A} = \{A_1, \ldots, A_n\}$ и $\mathcal{B} = \{B_1, \ldots, B_n\}$ — два n-множества вершин графа G (возможно, пересекающихся). С множествами $\mathcal{A}$ и $\mathcal{B}$ свяжем *матрицу путей* $M = (m_{ij})$, где

$$m_{ij} \;:=\; \sum_{P:A_i\to B_j} w(P).$$

Система путей $\mathcal{P}$ *из* $\mathcal{A}$ *в* $\mathcal{B}$ состоит из перестановки σ множества $\{1, \ldots, n\}$ и n путей $P_i : A_i \to B_{\sigma(i)}$, $i = 1, \ldots, n$. Положим $\operatorname{sign}\mathcal{P} = \operatorname{sign}\sigma$. *Вес* системы $\mathcal{P}$ есть произведение весов ее путей

$$w(\mathcal{P}) \;=\; \prod_{i=1}^{n} w(P_i), \tag{2}$$

которое равно произведению весов всех ребер в системе путей.

Наконец, будем говорить, что $\mathcal{P} = (P_1, \ldots, P_n)$ — *система путей без общих вершин*, если любые два пути из $\mathcal{P}$ не имеют общих вершин.

Лемма. *Пусть* $G = (V, E)$ *— конечный ациклический ориентированный граф с весами,* $\mathcal{A} = \{A_1, \ldots, A_n\}$ *и* $\mathcal{B} = \{B_1, \ldots, B_n\}$ *— два множества вершин и* M *— матрица путей из* $\mathcal{A}$ *в* $\mathcal{B}$*. Тогда*

$$\det M \;=\; \sum_{\substack{\mathcal{P}\text{— система путей без}\\ \text{общих вершин}}} \operatorname{sign}\mathcal{P} \; w(\mathcal{P}). \tag{3}$$

■ **Доказательство.** Типичное слагаемое в сумме, определяющей $\det M$, есть $\operatorname{sign}\sigma\ m_{1\sigma(1)}\cdots m_{n\sigma(n)}$, что можно записать в виде

$$\operatorname{sign}\sigma\ \left(\sum_{P_1:A_1\to B_{\sigma(1)}} w(P_1)\right)\ \cdots\ \left(\sum_{P_n:A_n\to B_{\sigma(n)}} w(P_n)\right).$$

Суммируя по σ и учитывая (2), мы получим равенство

$$\det M\ =\ \sum_{\mathcal{P}} \operatorname{sign}\mathcal{P}\ w(\mathcal{P}),$$

где $\mathcal{P}$ пробегает *все* системы путей из $\mathcal{A}$ в $\mathcal{B}$ (не только системы путей без общих вершин). Поэтому (3) следует из равенства

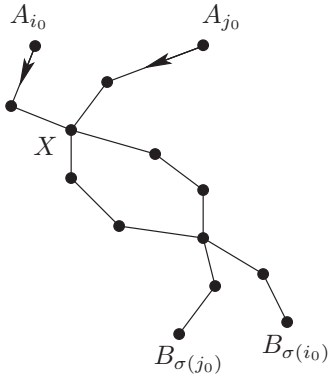
$$\sum_{\mathcal{P}\in N} \operatorname{sign}\mathcal{P}\ w(\mathcal{P})\ =\ 0, \tag{4}$$

где N — множество всех систем путей с общими вершинами. И тут используется рассуждение исключительной красоты. А именно, мы укажем такую инволюцию $\pi : N \to N$ (без неподвижных точек), что для систем путей $\mathcal{P}$ и $\pi\mathcal{P}$ выполняются равенства

$$w(\pi\mathcal{P})\ =\ w(\mathcal{P}) \qquad \text{и} \qquad \operatorname{sign}\pi\mathcal{P}\ =\ -\operatorname{sign}\mathcal{P}\ .$$

Ясно, что отсюда будет следовать (4), а из нее — формула (3) Леммы.

Инволюция π определяется самым естественным образом. Пусть система $\mathcal{P}\in N$ содержит пути $P_i : A_i \to B_{\sigma(i)}$. По определению N некоторые пары путей из $\mathcal{P}$ пересекаются.



- Пусть i_0 — минимальное значение, при котором P_{i_0} имеет общую вершину с другими путями из системы $\mathcal{P}$.
- Пусть X — первая такая общая вершина, принадлежащая пути P_{i_0}.
- Пусть $j_0 > i_0$ — минимальное значение, при котором P_{j_0} имеет с P_{i_0} общую вершину X.

Теперь построим новую систему $\pi\mathcal{P} = (P'_1, \ldots, P'_n) \in N$:

- Положим $P'_k = P_k$ для всех $k \neq i_0, j_0$.
- Новый путь P'_{i_0} проходит из A_{i_0} до X вдоль P_{i_0}, а затем продолжается до $B_{\sigma(j_0)}$ вдоль P_{j_0}. Аналогично P'_{j_0} проходит из A_{j_0} до X по P_{j_0}, а затем продолжается до $B_{\sigma(i_0)}$ вдоль P_{i_0}.

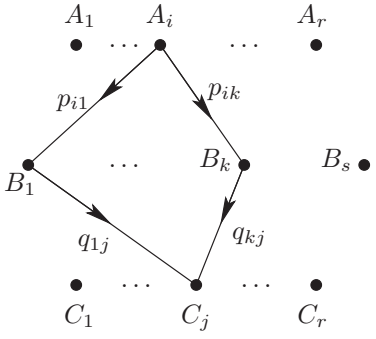
Ясно, что $\pi(\pi\mathcal{P}) = \mathcal{P}$, так как индексы i_0, j_0 и вершина X в системе $\pi\mathcal{P}$ те же самые, что и в $\mathcal{P}$. Значит, применяя π дважды, мы вернемся к прежним путям P_i. Далее, $w(\pi\mathcal{P}) = w(\mathcal{P})$, поскольку $\pi\mathcal{P}$ и $\mathcal{P}$ имеют одни и те же ребра. Наконец, так как подстановка σ', соответствующая системе $\pi\mathcal{P}$, получается умножением σ на транспозицию (i_0, j_0), то $\operatorname{sign}\pi\mathcal{P}\ = -\operatorname{sign}\mathcal{P}$, и доказательство завершено. □

Лемма Гессель – Вьеннота позволяет вывести все основные свойства определителей, рассматривая соответствующие графы. Приведем один поразительный пример — формулу Бине – Коши, которая дает полезное обобщение формулы для определителя произведения матриц.

Теорема. *Если $P = (p_{ik})$ — матрица размера $(r \times s)$, $Q = (q_{kj})$ — матрица размера $(s \times r)$ и $r \le s$, то*

$$\det(PQ) \;=\; \sum_{\mathcal{Z}} (\det P_{\mathcal{Z}})(\det Q_{\mathcal{Z}}),$$

где $P_{\mathcal{Z}}$ — подматрица размера $(r \times r)$ матрицы P с множеством столбцов $\mathcal{Z}$, а $Q_{\mathcal{Z}}$ — подматрица размера $(r \times r)$ матрицы Q с множеством строк $\mathcal{Z}$.



■ **Доказательство.** Пусть, как и раньше, матрице P соответствует двудольный граф с множествами вершин $\mathcal{A} = \{A_1, \ldots, A_r\}$ и $\mathcal{B} = \{B_1, \ldots, B_s\}$, а матрице Q — двудольный граф с множествами вершин $\mathcal{B}$ и $\mathcal{C} = \{c_1, \ldots, c_r\}$. Рассмотрим теперь объединенный граф, изображенный на полях, и заметим, что (i, j)-элемент матрицы M путей из $\mathcal{A}$ в $\mathcal{C}$ есть в точности $m_{ij} = \sum_k p_{ik} q_{kj}$. Следовательно, $M = PQ$.

Системам путей из $\mathcal{A}$ в $\mathcal{C}$ без общих вершин в объединенном графе соответствуют пары систем путей из $\mathcal{A}$ в $\mathcal{Z} \subseteq \mathcal{B}$ и из $\mathcal{Z}$ в $\mathcal{C}$ соответственно. Поэтому утверждение теоремы немедленно следует из Леммы, если заметить, что $(\sigma\tau) = (\operatorname{sign}\sigma)\,(\operatorname{sign}\tau)$, где σ и τ — подстановки, действующие на r-элементном множестве. □

Из леммы Гессель – Вьеннота следует также много результатов, связывающих определители с перечислительными задачами. Способ действий всегда один и тот же: матрицу M интерпретируют как матрицу путей и пытаются вычислить выражение в правой части (3). В качестве иллюстрации рассмотрим задачу, которую решали Гессель и Вьеннот и которая привела их к Лемме.

> *Пусть $a_1 < a_2 < \ldots < a_n$ и $b_1 < b_2 < \ldots < b_n$ — два множества натуральных чисел. Вычислить определитель матрицы $M = (m_{ij})$, где m_{ij} — биномиальный коэффициент $\binom{a_i}{b_j}$.*

Другими словами, Гессель и Вьеннот рассматривали определители произвольных квадратных матриц, элементы которых выбираются из треугольника Паскаля, например

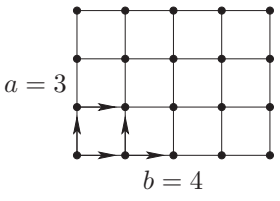
$$\det\begin{pmatrix} \binom{3}{1} & \binom{3}{3} & \binom{3}{4} \\ \binom{4}{1} & \binom{4}{3} & \binom{4}{4} \\ \binom{6}{1} & \binom{6}{3} & \binom{6}{4} \end{pmatrix} \;=\; \det\begin{pmatrix} 3 & 1 & 0 \\ 4 & 4 & 1 \\ 6 & 20 & 15 \end{pmatrix},$$

где матрица образована «жирными» элементами треугольника Паскаля, приведенного на полях.

1
1 1
1 2 1
1 **3** 3 **1**
1 **4** 6 **4** **1**
1 5 10 10 5 1
1 **6** 15 **20** **15** 6 1
1 7 21 35 35 21 7 1

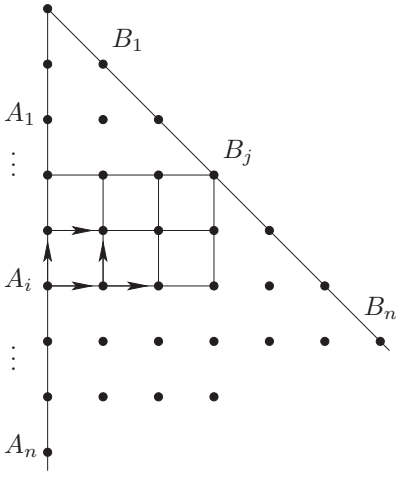
Напомним известное утверждение, связывающее биномиальные коэффициенты с путями на решетке. Рассмотрим изображенную на полях решетку размером $a \times b$. Если допускаются лишь шаги вверх (на север, N) и вправо (на восток, E), то число путей из левого нижнего угла в правый верхний угол есть $\binom{a+b}{a}$.

Доказать это утверждение несложно. Каждый путь — это последовательность, содержащая b шагов на восток и a шагов на север, поэтому его можно закодировать строкой вида NENEEEN из a знаков N и b знаков E. Число таких строк есть число способов выбрать a мест для знаков N из $a+b$ мест, что равно $\binom{a+b}{a} = \binom{a+b}{b}$.



Рассмотрим теперь рисунок на полях, на котором вершина A_i размещена в точке $(0, -a_i)$, а B_j — в точке $(b_j, -b_j)$, $i, j = 1, \ldots, n$.

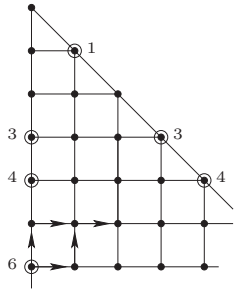
По только что доказанному, если двигаться по этой решетке только на север и восток, то число путей из A_i в B_j равно $\binom{b_j+(a_i-b_j)}{b_j} = \binom{a_i}{b_j}$. Значит, матрица M биномиальных коэффициентов — это матрица путей из $\mathcal{A}$ в $\mathcal{B}$ в образованном решеткой графе, в котором все ребра имеют вес 1 и ориентированы на север или на восток. Поэтому для вычисления $\det M$ можно применить лемму Гессель – Вьеннота. Легко понять, что каждая система $\mathcal{P}$ путей из $\mathcal{A}$ в $\mathcal{B}$ без общих вершин состоит из путей $P_i : A_i \to B_i$, $i = 1, \ldots, n$. Тогда каждой системе путей без общих вершин соответствует только тождественная перестановка, и так как ее знак равен 1, то мы получаем прекрасный результат:



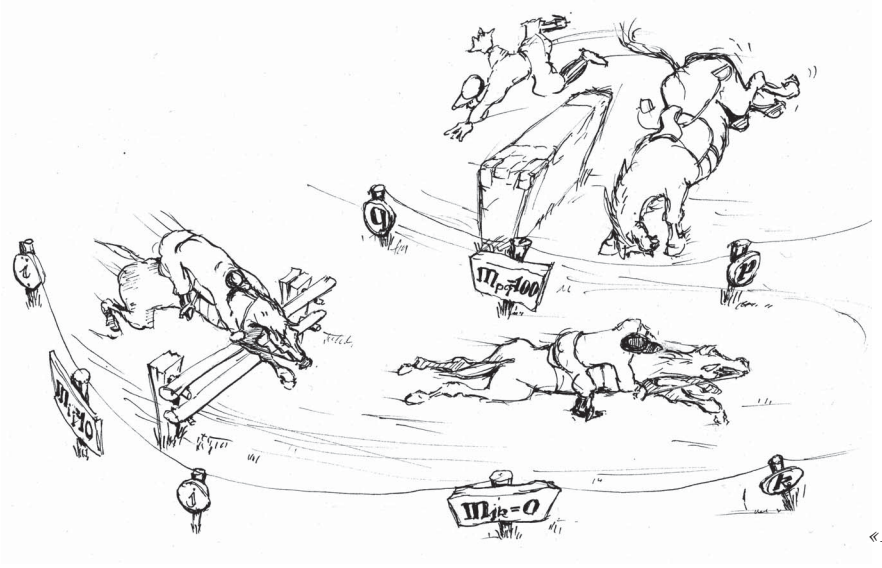
$$\det\left(\binom{a_i}{b_j}\right) \;=\; \#\,\{\text{системы путей из } \mathcal{A} \text{ в } \mathcal{B} \text{ без общих вершин}\}.$$

Например,

$$\det\begin{pmatrix} \binom{3}{1} & \binom{3}{3} & \binom{3}{4} \\ \binom{4}{1} & \binom{4}{3} & \binom{4}{4} \\ \binom{6}{1} & \binom{6}{3} & \binom{6}{4} \end{pmatrix} \;=\; \#\begin{array}{l}\text{систем путей}\\ \text{без общих}\\ \text{вершин в}\end{array}$$



В частности, отсюда вытекает совсем не очевидный факт: $\det M \geq 0$, так как в правой части стоит число элементов *некоторого множества*. Более того, согласно лемме Гессель – Вьеннота $\det M = 0$ тогда и только тогда, когда $a_i < b_i$ для некоторого i.



«Пути на решетке»

Литература

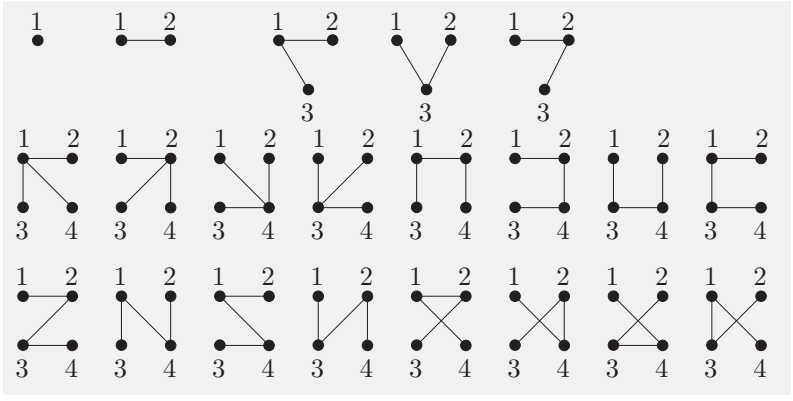
[1] Gessel I. M., Viennot G. *Binomial determinants, paths, and hook length formulae.* Advances in Math., **58** (1985), 300–321.

[2] Lindström B. *On the vector representation of induced matroids.* Bulletin London Math. Soc., **5** (1973), 85–90.

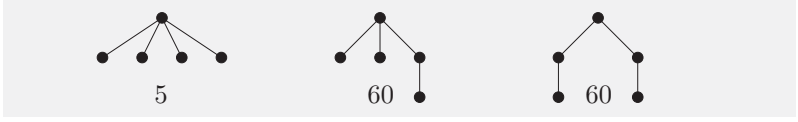
Формула Кэли для числа деревьев

Глава 30

Одна из самых красивых формул перечислительной комбинаторики — формула для числа помеченных деревьев. Рассмотрим множество $N = \{1, 2, \ldots, n\}$. Сколько различных деревьев можно построить на этом множестве вершин? Обозначим это число T_n. Перебирая все возможные варианты, находим: $T_1 = 1, T_2 = 1, T_3 = 3, T_4 = 16$. Эти деревья приведены в следующей таблице:



Заметим, что мы рассматриваем *помеченные* деревья, а поэтому, хотя все деревья порядка 3 изоморфны, существует 3 различных помеченных дерева, соответствующих выбору внутренней вершины. Для $n = 5$ имеется три неизоморфных дерева:

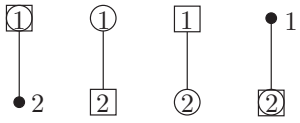


Ясно, что вершины первого дерева можно пометить 5 различными способами, а вершины второго и третьего деревьев можно пометить $\frac{5!}{2} = 60$ способами, и мы получаем $T_5 = 125$. Приведенных примеров должно быть достаточно для того, чтобы предположить, что $T_n = n^{n-2}$, а это и есть результат Кэли [3].

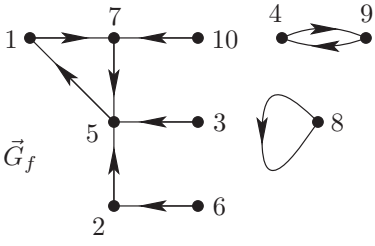
Теорема. *Существует n^{n-2} различных помеченных деревьев с n вершинами.*

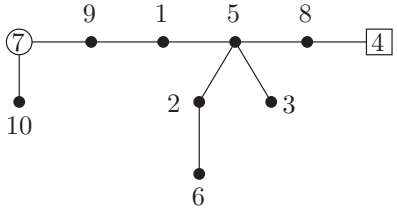
Эта замечательная формула имеет не менее замечательные доказательства, которые используют различные комбинаторные и алгебраические приемы. Сначала мы рассмотрим три доказательства, а затем перейдем к доказательству, которое пока что является самым красивым.

Артур Кэли



Четыре дерева, составляющие $\mathcal{T}_2$





■ **Первое доказательство (биекция).** Классический и самый прямой метод состоит в нахождении биекции из множества всех деревьев с n вершинами в множество мощности n^{n-2}. Естественно, на ум приходит множество всех упорядоченных последовательностей $(a_1, \ldots, a_{n-2})$, где $1 \le a_i \le n$. Итак, мы хотим однозначно закодировать каждое дерево T последовательностью $(a_1 \ldots, a_{n-2})$. Этот код был найден Прюфером [6], и его можно найти в большинстве книг по теории графов.

Здесь мы приведем биективное доказательство Жойяля [4], менее известное, но столь же элегантное и простое. Рассмотрим не сами деревья t на множестве вершин $N = \{1, \ldots, n\}$, а деревья с двумя выделенными вершинами — *левым концом* ◯ и *правым концом* □ (они могут совпадать). Пусть $\mathcal{T}_n = \{(t; ◯, □)$ — новое множество деревьев. Ясно, что $|\mathcal{T}_n| = n^2 T_n$. Таким образом, наша цель — доказать, что $|\mathcal{T}_n| = n^n$. Существует множество, объем которого известен и равен n^n, а именно, множество N^N всех отображений из N в N. Значит, формула Кэли будет доказана, если мы сможем найти биекцию из N^N в $\mathcal{T}_n$.

Пусть $f : N \longrightarrow N$ — произвольное отображение. Представим f в виде ориентированного графа $\vec{G}_f$, задав для каждого $i = 1, \ldots, n$ ребро, исходящее из i и входящее в $f(i)$. Например, отображение

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 5 & 5 & 9 & 1 & 2 & 5 & 8 & 4 & 7 \end{pmatrix}$$

представляется ориентированным графом, изображенным на полях.

Рассмотрим компоненты графа $\vec{G}_f$. Так как из каждой его вершины исходит ровно одно ребро, то каждая компонента содержит равное число вершин и ребер и, следовательно, ровно один ориентированный цикл. Пусть $M \subseteq N$ — объединение всех этих циклов. Нетрудно проверить, что M — *единственное* такое максимальное подмножество множества N, что ограничение f на M является биекцией M в себя. Положим $f|_M = \begin{pmatrix} a & b & \ldots & z \\ f(a) & f(b) & \ldots & f(z) \end{pmatrix}$, расположив в первой строке числа $a, b, \ldots, z$ в естественном порядке. Тогда вторая строка даст нам упорядочение элементов $f(a), f(b), \ldots, f(z)$ множества M. Назовем $f(a)$ его левым, а $f(z)$ — правым концом.

Построим теперь дерево t, соответствующее отображению f. Составим из $f(a), \ldots, f(z)$ в этом порядке (неориентированный) *путь*, соединяющий $f(a)$ с $f(z)$, и присоединим к нему остальные вершины так же, как в $\vec{G}_f$ (убрав ориентацию ребер). В рассмотренном выше примере получаем $M = \{1, 4, 5, 7, 8, 9\}$,

$$f|_M = \begin{pmatrix} 1 & 4 & 5 & 7 & 8 & 9 \\ 7 & 9 & 1 & 5 & 8 & 4 \end{pmatrix}$$

и изображенное на полях дерево t.

Построенное соответствие между отображениями и деревьями легко обратить. В заданном дереве t найдем единственный путь P из его левого конца в правый. Это даст множество M и отображение[1] $f|_M$. Затем доопределим отображение $i \to f(i)$ в соответствии с единственными путями из i в P. □

[1] Расположив элементы M в возрастающем порядке, получим первую строку $f|_M$. Вторую строку $f|_M$ образуют (начиная с левого конца) последовательные элементы пути P. — *Прим. перев.*

■ **Второе доказательство (линейная алгебра).** Мы можем понимать T_n как число остовных деревьев[2] в полном графе K_n. Рассмотрим произвольный простой связный граф $G = (V, E)$ с множеством вершин $V = \{1, 2, \ldots, n\}$, и множеством ребер E; пусть $t(G)$ — число его остовных деревьев, так что $T_n = t(K_n)$. Следующее замечательное утверждение есть *матричная теорема о деревьях* Кирхгофа (см. [1]).

Пусть $B = (b_{ie})$ — матрица инцидентности графа G; ее строки занумерованы элементами множества V, а столбцы — элементами множества E, так что $b_{ie} = 1$ при $i \in e$ и $b_{ie} = 0$ при $i \notin e$. Заметим, что $|E| \geq n-1$, так как граф G связен. Заменим в каждом столбце матрицы B одну из двух единиц на -1 (это равносильно заданию ориентации на ребрах графа G), и обозначим новую матрицу C. Тогда $M = CC^T$ — симметричная $(n \times n)$-матрица, и элементы $d_1, \ldots, d_n$ ее главной диагонали равны степеням вершин графа G.

Предложение. *Для всех $i = 1, \ldots, n$ выполняется равенство $t(G) = \det M_{ii}$, где M_{ii} получается из M удалением i-й строки и i-го столбца.*

■ **Доказательство.** Ключом к доказательству является доказанная в предыдущей главе теорема Бине – Коши: если P и Q — матрицы размеров $(r \times s)$ и $(s \times r)$, $r \leq s$, то $\det(PQ)$ равен сумме произведений определителей $(r \times r)$-подматриц P и Q, соответствующих одинаковым наборам индексов для r столбцов матрицы P и r строк матрицы Q. Применение этой теоремы к матрице M_{ii} дает равенство

$$\det M_{ii} \;=\; \sum\nolimits_N \det N \cdot \det N^T \;=\; \sum\nolimits_N (\det N)^2,$$

где N пробегает все $(n-1)\times(n-1)$-подматрицы матрицы C с удаленной строкой i. Каждой матрице N соответствует подграф графа G с $n-1$ ребрами и n вершинами, и остается показать, что

$$\det N = \begin{cases} \pm 1, & \text{если эти ребра образуют дерево,} \\ 0 & \text{в противном случае.} \end{cases}$$

Предположим, что эти $n-1$ ребер не образуют дерево. Тогда существует компонента, которая не содержит i. Так как соответствующие строки этой компоненты при сложении дают 0, мы заключаем, что они линейно зависимы, вследствие чего $\det N = 0$.

Предположим теперь, что столбцам N соответствует дерево. Тогда имеется вершина $j_1 \neq i$ степени 1; пусть e_1 — ребро, инцидентное этой вершине. Удаляя j_1 и e_1, мы получим дерево с $n-2$ ребрами. В нем снова найдутся вершина $j_2 \neq i$ степени 1 и инцидентное ей ребро e_2. Продолжая таким образом, определим вершины $j_1, j_2, \ldots, j_{n-1}$ и ребра $e_1, e_2, \ldots, e_{n-1}$, где $j_i \in e_i$. После этого переставим строки и столбцы N так, чтобы вершине j_k соответствовала k-я строка, а ребру e_k — k-й столбец. По построению $j_k \notin e_\ell$, если $k < \ell$. Поэтому новая матрица N' является нижней треугольной, и все элементы на ее главной диагонали равны ± 1. Таким образом, $\det N = \pm \det N' = \pm 1$, и предложение доказано[3].

«Нестандартный способ перечисления деревьев. Посадите на каждое дерево кошку, выпустите свою собаку и считайте, сколько раз она залает.»

[2] Остовным деревом связного графа называется его подграф, который является деревом и содержит все вершины. — *Прим. перев.*

[3] Приведенное доказательство матричной теоремы о деревьях Кирхгофа можно найти также в [9*, с.181–182]. — *Прим. перев.*

В частном случае $G = K_n$ мы, очевидно, имеем

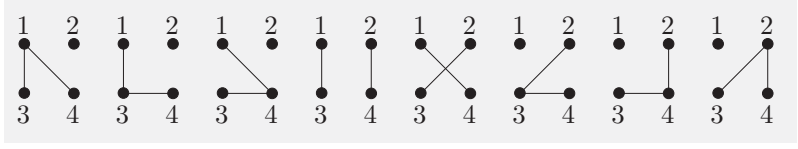
$$M_{ii} = \begin{pmatrix} n-1 & -1 & \dots & -1 \\ -1 & n-1 & & -1 \\ \vdots & & \ddots & \vdots \\ -1 & -1 & \dots & n-1 \end{pmatrix},$$

и простые вычисления[4] показывают, что $\det M_{ii} = n^{n-2}$. □

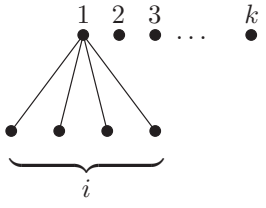
■ **Третье доказательство (рекурсия).** Другой классический метод перечислительной комбинаторики состоит в построении рекуррентного соотношения и его решении с помощью индукции. Следующая идея по существу принадлежит Реньи [7] и Риордану [8]. Чтобы найти подходящее рекуррентное соотношение, мы рассмотрим более общую задачу (которая появилась еще в статье Кэли [3]).

Пусть A — произвольное k-множество вершин. Обозначим через $T_{n,k}$ число (помеченных) лесов на множестве $\{1, \dots, n\}$, состоящих из k деревьев, в которых вершины из A принадлежат различным деревьям. Ясно, что важен не конкретный вид множества A, а лишь его объем k. Заметим, что $T_{n,1} = T_n$.

Например, $T_{4,2} = 8$ для $A = \{1, 2\}$



Рассмотрим такой лес F с $A = \{1, 2, \dots, k\}$; пусть вершина с пометкой 1 смежна с i вершинами, как указано на рисунке на полях. Если удалить вершину 1, то ее i соседей и вершины $2, \dots, k$ будут принадлежать разным компонентам леса, состоящего из $k - 1 + i$ деревьев. Так как мы можем построить F, сначала фиксируя i, затем выбирая i соседей вершины 1 и, наконец, лес $F \backslash \{1\}$, то



$$T_{n,k} \;=\; \sum_{i=0}^{n-k} \binom{n-k}{i} T_{n-1,k-1+i} \tag{1}$$

для всех $n \geq k \geq 1$, где мы полагаем $T_{0,0} = 1$, $T_{n,0} = 0$ для $n > 0$. Заметим, что условие $T_{0,0} = 1$ необходимо, чтобы $T_{n,n} = 1$ при всех n.

Предложение. *Имеет место равенство*

$$T_{n,k} \;=\; k\, n^{n-k-1}, \tag{2}$$

в частности, $\quad T_{n,1} \;=\; T_n \;=\; n^{n-2}$.

[4] Прибавление к первой строке M_{ij} всех остальных строк и вычитание первого столбца из остальных приводят матрицу к треугольному виду. — *Прим. ред.*

■ **Доказательство.** Используя (1) и индукцию, получаем

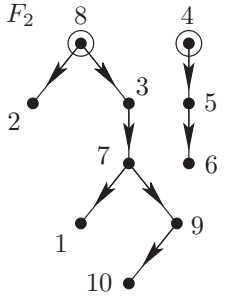
$$\begin{aligned}
T_{n,k} &= \sum_{i=0}^{n-k} \binom{n-k}{i} (k-1+i)(n-1)^{n-1-k-i} \qquad (i \to n-k-i) \\
&= \sum_{i=0}^{n-k} \binom{n-k}{i} (n-1-i)(n-1)^{i-1} \\
&= \sum_{i=0}^{n-k} \binom{n-k}{i} (n-1)^{i} - \sum_{i=1}^{n-k} \binom{n-k}{i} i(n-1)^{i-1} \\
&= n^{n-k} - (n-k) \sum_{i=1}^{n-k} \binom{n-1-k}{i-1} (n-1)^{i-1} \\
&= n^{n-k} - (n-k) \sum_{i=0}^{n-1-k} \binom{n-1-k}{i} (n-1)^{i} \\
&= n^{n-k} - (n-k) n^{n-1-k} \;=\; k\, n^{n-1-k}.
\end{aligned}$$

□

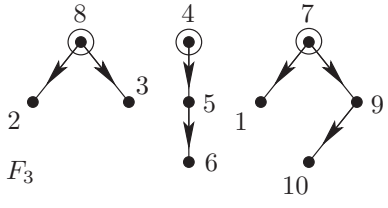
■ **Четвертое доказательство (двойной счет).** Следующая изумительная идея, принадлежащая Джиму Питмэну [5], позволяет доказать формулу Кэли и ее обобщение (2) без индукции или биекции; она состоит в остроумном перечислении двумя способами.

Корневой лес на множестве вершин $\{1, \ldots, n\}$ — это лес вместе с выбранным корнем в каждой компоненте-дереве. Пусть $\mathcal{F}_{n,k}$ — множество всех корневых лесов, состоящих из k корневых деревьев. Тогда $\mathcal{F}_{n,1}$ — множество всех корневых деревьев.

Заметим, что $|\mathcal{F}_{n,1}| = nT_n$, так как в каждом дереве с n помеченными вершинами можно выбрать корень n способами. Рассмотрим теперь лес $F_{n,k} \in \mathcal{F}_{n,k}$ как *ориентированный* граф, все дуги которого ориентированы от корней. Скажем, что лес F *содержит* другой лес F', если F содержит F' как ориентированный подграф. Ясно, что если F строго содержит F' (а множества вершин F и F' совпадают), то F имеет меньше компонент, чем F'. На рисунке показаны два таких леса, корнями которых являются самые верхние вершины.



F_2 содержит F_3



Теперь мы подошли к ключевой идее. Назовем последовательность лесов $F_1, \ldots, F_k$ *измельчающейся последовательностью*, если $F_i \in \mathcal{F}_{n,i}$ и при любом i лес F_i содержит F_{i+1}.

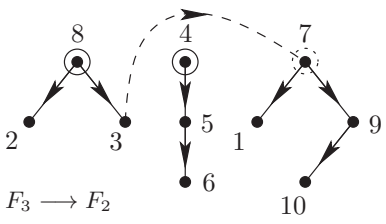
Далее, пусть F_k — фиксированный лес из $\mathcal{F}_{n,k}$; введем обозначения:

- $N(F_k)$ — число корневых деревьев, содержащих F_k,
- $N^*(F_k)$ — число измельчающихся последовательностей, оканчивающихся лесом F_k.

Подсчитаем $N^*(F_k)$ двумя способами: начиная с дерева и начиная с F_k. Пусть $F_1 \in \mathcal{F}_{n,1}$ содержит F_k. Так как при построении измельчающейся последовательности $k-1$ ребер $F_1 \backslash F_k$ можно удалять в любом порядке, то

$$N^*(F_k) \;=\; N(F_k)\,(k-1)! \tag{3}$$

Теперь начнем с другой стороны. Чтобы перейти от F_k к лесу F_{k-1}, мы должны добавить ребро, исходящее из произвольной вершины a



и входящее в любой из $k-1$ корней деревьев, не содержащих a (см. рисунок, где при переходе от F_3 к F_2 добавляется ребро $3 \bullet\!\!\rightarrow\!\!\bullet 7$). Следовательно, имеется $n(k-1)$ способов добавить ребро к F_k. Аналогично, в F_{k-1} мы можем провести ребро из любой вершины b к каждому из $k-2$ корней деревьев, не содержащих b, так что имеется $n(k-2)$ способов добавить ребро к F_{k-1}. Продолжая таким образом, мы приходим к равенству

$$N^*(F_k) \;=\; n^{k-1}(k-1)! \tag{4}$$

Отсюда и из (3) вытекает неожиданно простое соотношение

$$N(F_k) = n^{k-1} \qquad \text{для } \textit{любого } F_k \in \mathcal{F}_{n,k}.$$

Если $k=n$, то F_n содержит лишь n изолированных вершин. Поэтому $N(F_n)$ перечисляет *все* корневые деревья, и мы получаем $|\mathcal{F}_{n,1}| = n^{n-1}$, а это и есть формула Кэли. □

Последнее доказательство дает нам кое-что еще. Из формулы (4) при $k=n$ находим

$$\#\big\{\text{измельчающихся последовательностей } (F_1,\dots,F_n)\big\} = n^{n-1}(n-1)!. \tag{5}$$

Пусть $N^{**}(F_k)$ для $F_k \in \mathcal{F}_{n,k}$ обозначает число таких измельчающихся последовательностей $F_1,\dots,F_n$, в которых k-й член есть F_k. Ясно, что эта величина равна произведению $N^*(F_k)$ и числа способов задания $(F_{k+1},\dots,F_n)$. Но это последнее число есть $(n-k)!$, поскольку $n-k$ ребер из F_k можно удалять в любом порядке, и поэтому

$$N^{**}(F_k) \;=\; N^*(F_k)(n-k)! \;=\; n^{k-1}(k-1)!(n-k)! \tag{6}$$

Так как это число не зависит от выбора F_k, то, разделив (5) на (6), мы получим число корневых лесов, состоящих из k деревьев:

$$|\mathcal{F}_{n,k}| \;=\; \frac{n^{n-1}(n-1)!}{n^{k-1}(k-1)!(n-k)!} \;=\; \binom{n}{k} k\, n^{n-1-k}.$$

Поскольку k корней деревьев можно выбрать $\binom{n}{k}$ возможными способами, формула $T_{n,k} = kn^{n-k-1}$ вновь доказана без помощи индукции.

Закончим главу историческим замечанием. Статью Кэли 1889 года [3] предвосхитил Карл В. Борхард (1860), и этот факт признавал сам Кэли. Эквивалентный результат появился даже раньше в статье Сильвестра в 1857 г. (см. [2, гл. 3]). Новинкой статьи Кэли было использование терминов теории графов, и с тех пор теорема о числе помеченных деревьев связывается с его именем[5].

Литература

[1] Aigner M. *Combinatorial Theory.* Springer-Verlag, Berlin–Heidelberg–New York, 1979; Reprint 1997. [Русский перевод: Айгнер М. *Комбинаторная теория.*— М.: Мир, 1982]

[2] Biggs N. L., Lloyd E. K., Wilson R. J. *Graph Theory 1736-1936.* Clarendon Press, Oxford, 1976.

[5] Относительно формулы Кэли и ее обобщений см. также цикл задач с решениями в [10*], составленный переводчиком настоящей книги. — *Прим. перев.*

[3] Cayley A. *A theorem on trees.* Quart. J. Pure Appl. Math., **23** (1889), 376–378; Collected Mathematical Papers, Vol. 13, Cambridge University Press, 1897, 26–28.

[4] Joyal A. *Une théorie combinatoire des séries formelles.* Advances in Math., **42** (1981), 1–82.

[5] Pitman J. *Coalescent random forests.* J. Combinatorial Theory, Ser. A, **85** (1999), 165–193.

[6] Prüfer H. *Neuer Beweis eines Satzes über Permutationen.* Archiv der Math. u. Physik, (3) **27** (1918), 142–144.

[7] Rényi A. *Some remarks on the theory of trees.* MTA Mat. Kut. Inst. Kozl. (Publ. math. Inst. Hungar. Acad. Sci.), **4** (1959), 73–85; Selected Papers, Vol. 2, Akadémiai Kiadó, Budapest 1976, 363–374.

[8] Riordan J. *Forests of labeled trees.* J. Combinatorial Theory, **5** (1968), 90–103.

[9*] Харари Ф. *Теория графов.* М., Мир, 1973.

[10*] Рыбников К. А. (редактор). *Комбинаторный анализ. Задачи и упражнения.* М., изд-во МГУ, 1979; М., Наука, 1982.

Глава 31 Тождества и биекции

Рассмотрим бесконечное произведение $(1+x)(1+x^2)(1+x^3)(1+x^4)\cdots$ и разложим его обычным образом в ряд $\sum_{n\geq 0} a_n x^n$ по степеням x. Как нетрудно проверить, первые члены разложения имеют вид

$$\prod_{k\geq 1}(1+x^k) = 1 + x + x^2 + 2x^3 + 2x^4 + 3x^5 + 4x^6 + 5x^7 + \dots \qquad (1)$$

Таким образом, например, $a_6 = 4$, $a_7 = 5$, и можно (вполне законно) предположить, что a_n стремится к бесконечности при $n \longrightarrow \infty$.

Однако при рассмотрении столь же простого произведения $(1-x)(1-x^2)(1-x^3)(1-x^4)\cdots$ обнаруживается нечто неожиданное. Разлагая это произведение в ряд, получаем

$$\prod_{k\geq 1}(1-x^k) \;=\; 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \;\dots\,. \qquad (2)$$

Кажется, что все коэффициенты равны 1, -1 или 0. Но верно ли это? И если верно, то какой закон описывает последовательность коэффициентов?

Бесконечные суммы, произведения и условия их сходимости занимали центральное место в анализе с момента его возникновения, и большой вклад в эту область был сделан величайшими математиками от Леонарда Эйлера до Сринивасы Рамануджана.

Однако при выводе тождеств, подобных (1) и (2), мы игнорируем вопросы сходимости и просто манипулируем коэффициентами. Иначе говоря, мы работаем с «формальными» степенными рядами и произведениями. В рамках этого подхода мы покажем, как комбинаторные рассуждения приводят к изящным доказательствам на первый взгляд трудных комбинаторных тождеств.

Наше исходное понятие — *разбиение* натурального числа. Назовем любую сумму

$$\lambda: \quad n \;=\; \lambda_1 + \lambda_2 + \ldots + \lambda_t, \quad \text{где} \quad \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_t \geq 1,$$

разбиением числа n. Множество всех разбиений n обозначим $P(n)$; положим $p(n) := |P(n)|$ и будем считать, что $p(0) = 1$.

$5 = 5$
$5 = 4 + 1$
$5 = 3 + 2$
$5 = 3 + 1 + 1$
$5 = 2 + 2 + 1$
$5 = 2 + 1 + 1 + 1$
$5 = 1 + 1 + 1 + 1 + 1$.

Все $p(5) = 7$ разбиений числа 5.

Какое отношение имеют разбиения к нашей задаче? Рассмотрим произведение бесконечного множества рядов:

$$(1+x+x^2+x^3+\dots)(1+x^2+x^4+x^6+\dots)(1+x^3+x^6+x^9+\dots)\;\cdots, \qquad (3)$$

в котором k-й сомножитель есть $(1 + x^k + x^{2k} + x^{3k} + \dots)$. Чему будет равен коэффициент при x^n, если разложить это произведение в ряд $\sum_{n\geq 0} a_n x^n$? Небольшое размышление убеждает в том, что a_n есть

число способов записать n в виде суммы

$$\begin{aligned} n &= n_1 \cdot 1 + n_2 \cdot 2 + n_3 \cdot 3 + \dots \\ &= \underbrace{1 + \dots + 1}_{n_1} + \underbrace{2 + \dots + 2}_{n_2} + \underbrace{3 + \dots + 3}_{n_3} + \dots \end{aligned}$$

Поэтому коэффициент a_n есть не что иное, как число $p(n)$ разбиений n. Так как сумма геометрической прогрессии $1 + x^k + x^{2k} + \dots$ равна $\frac{1}{1-x^k}$, то тем самым доказано первое тождество:

$$\prod_{k\ge 1} \frac{1}{1-x^k} = \sum_{n\ge 0} p(n)\, x^n . \tag{4}$$

Более того, из наших рассуждений следует, что множитель $\frac{1}{1-x^k}$ учитывает вклад k в разбиение n. Значит, если исключить множитель $\frac{1}{1-x^k}$ из произведения в левой части (4), то k не появится ни в одном из разбиений, учитываемых в правой части. В качестве простого примера получаем соотношение

$$\prod_{i\ge 1} \frac{1}{1-x^{2i-1}} = \sum_{n\ge 0} p_o(n)\, x^n, \tag{5}$$

где $p_o(n)$ — число разбиений n, все слагаемые в которых *нечетны*. Аналогичное утверждение справедливо в случае, когда все слагаемые *четны*.

$6 = 5 + 1$
$6 = 3 + 3$
$6 = 3 + 1 + 1 + 1$
$6 = 1 + 1 + 1 + 1 + 1 + 1$
Разбиения 6 на нечетные слагаемые: $p_o(6) = 4$

Теперь должно быть ясно, каким будет n-й коэффициент в бесконечном произведении $\prod_{k\ge 1}(1+x^k)$. Из каждого множителя в произведении (3) мы берем либо 1, либо x^k, а это означает, что рассматриваются лишь такие разбиения, в которых любое слагаемое k появляется не более одного раза. Другими словами, исходное произведение (1) разлагается в ряд

$$\prod_{k\ge 1} (1 + x^k) = \sum_{n\ge 0} p_d(n)\, x^n , \tag{6}$$

где $p_d(n)$ — число разбиений n на *различные* слагаемые.

$7 = 7$
$7 = 5 + 1 + 1$
$7 = 3 + 3 + 1$
$7 = 3 + 1 + 1 + 1 + 1$
$7 = 1 + 1 + 1 + 1 + 1 + 1 + 1$

$7 = 7$
$7 = 6 + 1$
$7 = 5 + 2$
$7 = 4 + 3$
$7 = 4 + 2 + 1.$
Разбиения 7 на нечетные и на различные слагаемые: $p_o(7) = p_d(7) = 5$.

Сейчас метод формальных рядов продемонстрирует свою полную мощь. Так как $1 - x^2 = (1-x)(1+x)$, то справедливо тождество

$$\prod_{k\ge 1} (1 + x^k) = \prod_{k\ge 1} \frac{1-x^{2k}}{1-x^k} = \prod_{k\ge 1} \frac{1}{1-x^{2k-1}}$$

(все множители $1 - x^{2k}$ с четными показателями сокращаются). Таким образом, бесконечные произведения из равенств (5) и (6) одинаковы, следовательно, совпадают их разложения в степенные ряды, и мы получаем замечательный результат:

$$p_o(n) = p_d(n) \qquad \text{для всех } n \ge 0. \tag{7}$$

Это удивительное равенство должно иметь простое доказательство с помощью биекции — по крайней мере, таково мнение любого комбинаторика.

Задача. *Пусть $P_o(n)$ и $P_d(n)$ — множества разбиений числа n на нечетные и различные слагаемые соответственно. Найти биекцию $P_o(n)$ на $P_d(n)$.*

Известно несколько таких биекций; по-видимому, самая изящная из них была предложена Глэйшером (J. W. L. Glaisher) в 1907 году. Пусть λ — разбиение числа n на нечетные слагаемые. Соберем в нем равные слагаемые:

$$\begin{aligned} n &= \underbrace{\lambda_1 + \ldots + \lambda_1}_{n_1} + \underbrace{\lambda_2 + \ldots + \lambda_2}_{n_2} + \ldots + \underbrace{\lambda_t + \ldots + \lambda_t}_{n_t} \\ &= n_1 \cdot \lambda_1 + n_2 \cdot \lambda_2 + \ldots + n_t \cdot \lambda_t. \end{aligned}$$

Например, ϕ отображает
$\lambda : 25 = 5{+}5{+}5{+}3{+}3{+}1{+}1{+}1{+}1$
в
$\lambda' : 25 = (2{+}1)5 + (2)3 + (4)1$
$= 10 + 5 + 6 + 4$
$= 10 + 6 + 5 + 4\,.$

Рассмотрим двоичное представление $n_1 = 2^{m_1} + 2^{m_2} + \ldots + 2^{m_r}$ числа n_1 и аналогичные представления для остальных n_i. Тогда получается новое разбиение λ' числа n:

$$\lambda' : \quad n = 2^{m_1}\lambda_1 + 2^{m_2}\lambda_1 + \ldots + 2^{m_r}\lambda_1 + 2^{k_1}\lambda_2 + \ldots\,.$$

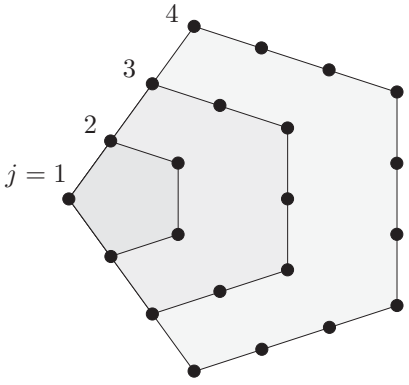
Покажем, что λ' принадлежит множеству $P_d(n)$ и что отображение $\phi : \lambda \longmapsto \lambda'$ действительно является биекцией. Оба утверждения легко проверить. Если $2^a\lambda_i = 2^b\lambda_j$, то $2^a = 2^b$, так как λ_i и λ_j нечетны, и поэтому $\lambda_i = \lambda_j$. Значит, λ' принадлежит $P_d(n)$. Обратно, если $n = \mu_1 + \mu_2 + \ldots + \mu_s$ — разбиение n на различные слагаемые, то можно обратить биекцию, собирая вместе все μ_i с одной и той же степенью 2 (в их разложениях на простые множители) и выписывая нечетные слагаемые с соответствующими кратностями. На полях приводится иллюстрирующий пример.

Представляя
$\lambda' : 30 = 12 + 6 + 5 + 4 + 3$
как $\quad 30 = 4(3{+}1) + 2(3) + 1(5{+}3)$
$= (1)5 + (4{+}2{+}1)3 + (4)1,$
получим в качестве $\phi^{-1}(\lambda')$
разбиение
$\lambda : 30 = 5 + 3 + 3 + 3 + 3 + 3 + 3 + 3 + 1 + 1 + 1 + 1$
на нечетные слагаемые.

Итак, манипуляции с формальными произведениями привели нас к равенству $p_o(n) = p_d(n)$ для разбиений, которое мы затем проверили с помощью биекции. Теперь пройдем по такому пути в обратном направлении, проведя для разбиений биективное доказательство, которое дает тождество. На этот раз нашей целью будет описание структуры разложения (2).

Посмотрим на ряд

$$1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - x^{35} - x^{40} + \ldots\,.$$



Пентагональные числа

В выписанном отрезке показатели степеней (за исключением 0) разбиваются на пары, и показатели степеней первых элементов пар образуют последовательность

$$1 \quad 5 \quad 12 \quad 22 \quad 35 \quad 51 \quad 70 \quad \ldots,$$

которая была хорошо известна Эйлеру. Это *пентагональные числа* $f(j)$, название которых поясняет чертеж на полях.

Легко проверить, что $f(j) = \frac{3j^2-j}{2}$ и что второе число каждой пары имеет вид $\bar{f}(j) = \frac{3j^2+j}{2}$. Поэтому предположим (как и Эйлер), что справедлива следующая формула.

Теорема.

$$\prod_{k\geq 1}(1-x^k) \;=\; 1+\sum_{j\geq 1}(-1)^j\Big(x^{\frac{3j^2-j}{2}}+x^{\frac{3j^2+j}{2}}\Big). \qquad (8)$$

Эйлер доказал эту замечательную теорему, используя вычисления с формальными рядами, но мы дадим биективное доказательство, достойное Книги[1]. Прежде всего заметим, что в силу (4) произведение $\prod_{k\geq 1}(1-x^k)$ является в точности обратным к ряду для разбиений $\sum_{n\geq 0}p(n)x^n$. Поэтому, полагая $\prod_{k\geq 1}(1-x^k)=\sum_{n\geq 0}c(n)x^n$, находим

$$\left(\sum_{n\geq 0}c(n)x^n\right)\cdot\left(\sum_{n\geq 0}p(n)x^n\right) \;=\; 1.$$

Сравнивая коэффициенты, отсюда получаем, что $c(n)$ — *единственная* последовательность, для которой $c(0)=1$ и

$$\sum_{k=0}^{n}c(k)p(n-k) \;=\; 0 \qquad \text{для всех } \; n\geq 1. \qquad (9)$$

Если представить правую часть формулы (8) в виде $\sum\limits_{j=-\infty}^{\infty}(-1)^j x^{\frac{3j^2+j}{2}}$, то нам остается показать, что эта единственная последовательность определяется формулами

$$c(k) \;=\; \begin{cases} 1 & \text{при } k=\frac{3j^2+j}{2},\ \text{если } j\in\mathbb{Z} \text{ четно},\\ -1 & \text{при } k=\frac{3j^2+j}{2},\ \text{если } j\in\mathbb{Z} \text{ нечетно},\\ 0 & \text{в противном случае.}\end{cases}$$

Положим $b(j)=\frac{3j^2+j}{2}$ для $j\in\mathbb{Z}$ и подставим эти значения в (9); тогда наше предположение примет простой вид:

$$\sum_{j \text{ четно}} p(n-b(j)) \;=\; \sum_{j \text{ нечетно}} p(n-b(j)) \qquad \text{для всех } \; n,$$

где, конечно, рассматриваются лишь такие j, для которых $b(j)\leq n$. Тем самым доказательство свелось к тому, чтобы найти биекцию

$$\phi:\ \bigcup_{j \text{ четно}} P(n-b(j)) \;\longrightarrow\; \bigcup_{j \text{ нечетно}} P(n-b(j)).$$

И в этом случае было предложено несколько биекций; следующая конструкция Давида Брессо и Дорона Цайлбергера [2] изумительно проста. Мы дадим лишь определение биекции ϕ (на самом деле она является инволюцией), и предлагаем читателю довести доказательство до конца.

[1] Аналитическое доказательство формулы (8) можно найти в [1], гл.1. – *Прим. перев.*

Для разбиения $\lambda : \lambda_1 + \ldots + \lambda_t \in P(n - b(j))$ положим

$$\phi(\lambda) \;:=\; \begin{cases} (t+3j-1) + (\lambda_1 - 1) + \ldots + (\lambda_t - 1), & \text{если } t + 3j \geq \lambda_1, \\ (\lambda_2 + 1) + \ldots + (\lambda_t + 1) + \underbrace{1 + \ldots + 1}_{\lambda_1 - t - 3j - 1}, & \text{если } t + 3j < \lambda_1, \end{cases}$$

где мы отбросили возможные нули. Тогда в первом случае $\phi(\lambda)$ лежит в $P(n - b(j-1))$, а во втором случае — в $P(n - b(j+1))$.

Пусть, например, $n = 15$ и $j = 2$, так что $b(2) = 7$. Разбиение $3+2+2+1$ из $P(15-b(2)) = P(8)$ отображается в разбиение $9+2+1+1$ из $P(15-b(1)) = P(13)$.

Это замечательно и позволяет получить еще кое-что. Мы уже доказали равенство

$$\prod_{k\geq 1}(1 + x^k) \;=\; \sum_{n\geq 0} p_d(n)\, x^n.$$

Как опытные преобразователи формальных рядов, заметим, что введение новой переменной y приводит к равенству

$$\prod_{k\geq 1}(1 + yx^k) \;=\; \sum_{n\geq 0} p_{d,m}(n)\, x^n y^m,$$

где $p_{d,m}(n)$ — число разбиений n ровно на m различных слагаемых. Полагая $y = -1$, находим:

$$\prod_{k\geq 1}(1 - x^k) \;=\; \sum_{n\geq 0}(E_d(n) - O_d(n))\, x^n, \tag{10}$$

здесь $E_d(n)$ — число разбиений n на *четное* число различных слагаемых, а $O_d(n)$ — число разбиений n на *нечетное* число слагаемых.

Например, для $n = 10$:
$10 = 9 + 1$
$10 = 8 + 2$
$10 = 7 + 3$
$10 = 6 + 4$
$10 = 4 + 3 + 2 + 1$
и
$10 = 10$
$10 = 7 + 2 + 1$
$10 = 6 + 3 + 1$
$10 = 5 + 4 + 1$
$10 = 5 + 3 + 2$,
так что $E_d(10) = O_d(10) = 5$.

Мы подошли к кульминационному пункту рассуждений. Сравнивая (10) и разложение Эйлера (8), мы приходим к прекрасному результату:

$$E_d(n) - O_d(n) \;=\; \begin{cases} 1 & \text{при } n = \frac{3j^2 \pm j}{2}, \text{ если } j \geq 0 \text{ четно}, \\ -1 & \text{при } n = \frac{3j^2 \pm j}{2}, \text{ если } j \geq 1 \text{ нечетно}, \\ 0 & \text{в противном случае.} \end{cases}$$

Сриниваса Рамануджан

Конечно, этот результат — только начало длинной и все еще продолжающейся истории. Теория бесконечных произведений изобилует неожиданными тождествами и их биективными аналогами. Наиболее известными примерами являются тождества Роджерса – Рамануджана, названные в честь их авторов Леонарда Роджерса [5] и Сринивасы Рамануджана [4], в которых число 5 играет загадочную роль:

$$\prod_{k\geq 1} \frac{1}{(1-x^{5k-4})(1-x^{5k-1})} \;=\; \sum_{n\geq 0} \frac{x^{n^2}}{(1-x)(1-x^2)\cdots(1-x^n)},$$

$$\prod_{k\geq 1} \frac{1}{(1-x^{5k-3})(1-x^{5k-2})} \;=\; \sum_{n\geq 0} \frac{x^{n^2+n}}{(1-x)(1-x^2)\cdots(1-x^n)}.$$

Предлагаем читателю преобразовать их в следующие тождества для разбиений, на которые впервые обратил внимание Перси МакМагон:

- Пусть $f(n)$ — число разбиений n, в которых все слагаемые имеют вид $5k+1$ или $5k+4$, а $g(n)$ — число разбиений, все слагаемые в которых различаются не менее, чем на 2. Тогда $f(n) = g(n)$.

- Пусть $r(n)$ — число разбиений n, в которых все слагаемые имеют вид $5k+2$ или $5k+3$, а $s(n)$ — число разбиений, все слагаемые в которых различаются не менее, чем на 2, и не содержат единичных слагаемых. Тогда $r(n) = s(n)$.

Все известные доказательства тождеств Роджерса – Рамануджана используют формальные степенные ряды и весьма запутанны. Длительное время казалось, что биективных доказательств равенств $f(n) = g(n)$ и $r(n) = s(n)$ не существует. В конце концов в 1981 году биективные доказательства были предложены Адриано Гарсия и Стефеном Милном [3]. Однако построенные ими биекции очень сложны, так что доказательства из Книги еще не найдены.

Литература

[1] Andrews G. E. *The Theory of Partitions,* Encyclopedia of Mathematics and its Applications, Vol. 2, Addison-Wesley, Reading MA 1976.[Есть русский перевод: Эндрюс Г. Теория разбиений. — М., Наука, 1982.]

[2] Bressoud D., Zeilberger D. *Bijecting Euler's partitions-recurrence,* Amer. Math. Monthly, 1985, **92**, pp. 54–55.

[3] Garsia A., Milne S. *A Rogers-Ramanujan bijection,* J. Combinatorial Theory, Ser. A, 1981, **31**, pp. 289–339.

[4] Ramanujan S. *Proof of certain identities in combinatory analysis,* Proc. Cambridge Phil. Soc., 1919, **19**, pp. 214–216.

[5] Rogers L. J. *Second memoir on the expansion of certain infinite products,* Proc. London Math. Soc., 1894, **25**, pp. 318–343.

Глава 32 Дополнения до полных латинских квадратов

1	2	3	4
2	1	4	3
4	3	1	2
3	4	2	1

Латинский квадрат порядка 4

Одними из старейших комбинаторных объектов, изучение которых началось, по-видимому, еще в античные времена, являются *латинские квадраты*. Чтобы получить латинский квадрат, нужно заполнить n^2 ячеек квадратной $(n \times n)$-таблицы числами $1, 2, \ldots, n$ так, чтобы в каждой строке и в каждом столбце каждое число появлялось ровно по одному разу. Другими словами, строки и столбцы таблицы являются перестановками элементов множества $\{1, \ldots, n\}$. Назовем n *порядком* латинского квадрата.

Мы будем заниматься следующей задачей. Предположим, что некто начал заполнять ячейки таблицы числами из множества $\{1, 2, \ldots, n\}$. В некоторый момент он останавливается и просит нас заполнить оставшиеся пустые ячейки так, чтобы получить латинский квадрат. Когда это возможно? Для того, чтобы такое заполнение существовало, необходимо, чтобы любой элемент появлялся в каждой строке и в каждом столбце не более одного раза. Дадим этой ситуации название. Мы говорим о *неполном латинском квадрате* порядка n, если некоторые ячейки $(n \times n)$-таблицы заполнены числами множества $\{1, \ldots, n\}$ так, что каждое число встречается не более одного раза в каждой строке и в каждом столбце. Итак, задача состоит в следующем:

Когда неполный латинский квадрат можно дополнить до полного латинского квадрата того же порядка?

1	4	2	5	3
4	2	5	3	1
2	5	3	1	4
5	3	1	4	2
3	1	4	2	5

Циклический латинский квадрат

Рассмотрим несколько примеров. Пусть первые $n - 1$ строк заполнены, а последняя строка пустая. Тогда можно легко заполнить последнюю строку. Достаточно заметить, что в этом неполном латинском квадрате каждый элемент появляется $n - 1$ раз и, значит, отсутствует ровно в одном столбце. Поэтому, записав каждый элемент в нижней строке в том столбце, где он отсутствует, мы получим правильное заполнение квадрата.

1	2	...	n-1	
				n

Неполный латинский квадрат, который невозможно дополнить

Рассмотрим противоположный пример: пусть заполнена лишь первая строка. Тогда снова несложно дополнить квадрат до полного с помощью циклического сдвига на один шаг (например влево) при переходе к каждой следующей строке.

Итак, в первом примере дополнения определяются однозначно, а во втором имеется масса возможностей. Вообще говоря, чем меньше ячеек заполнено, тем больше свободы мы можем иметь для дополнения до полного квадрата.

Однако представленный на полях в качестве примера неполный латинский квадрат, у которого заполнены лишь n ячеек, очевидно, нельзя дополнить до полного, так как невозможно заполнить ячейку в правом верхнем углу, не нарушая условий на строки и столбцы.

Пусть в $(n \times n)$-таблице заполнено меньше n ячеек. Всегда ли можно ее дополнить до латинского квадрата?

Этот вопрос поставил Тревор Эванс в 1960 году [1], и утверждение о том, что дополнение всегда возможно, быстро стало известно как гипотеза Эванса. Конечно, для ее доказательства пытались применить индукцию, и это в конце концов привело к успеху. Опубликованное в 1981 году доказательство Богдана Сметанюка [4] дало ответ на этот вопрос и явилось прекрасным примером того, насколько тонкие индукционные рассуждения могут потребоваться. Более того, доказательство конструктивно и позволяет явно достроить латинский квадрат из любой исходной неполной конфигурации.

Прежде чем переходить к доказательству, рассмотрим внимательнее латинские квадраты вообще. Мы можем представить латинский квадрат $(3 \times n^2)$-таблицей, которую назовем *линейной таблицей* латинского квадрата. На полях изображены квадрат порядка 3 и его линейная таблица: в строках R и C стоят номера строк и столбцов, а в строке E — соответствующие элементы латинского квадрата.

1	3	2
2	1	3
3	2	1

R: 1 1 1 2 2 2 3 3 3
C: 1 2 3 1 2 3 1 2 3
E: 1 3 2 2 1 3 3 2 1

Условие, определяющее латинский квадрат, эквивалентно тому, что в любых двух строках линейной таблицы содержатся все n^2 упорядоченных пар элементов множества $\{1, 2, \ldots, n\}$ (и, следовательно, каждая такая пара встречается ровно один раз). Ясно, что можно провести произвольные замены символов в каждой строке (что соответствует перестановкам строк, столбцов или переименованию элементов) и снова получить некоторый латинский квадрат. Условие, определяющее $(3 \times n^2)$-таблицу, показывает также, что у строки элементов нет никакой специальной роли. Можно переставить строки таблицы (как целое), не нарушая условие, определяющее линейную таблицу, и получить другой латинский квадрат.

Латинские квадраты, связанные перестановкой строк линейных таблиц, называются *сопряженными*. Следующее замечание сделает доказательство прозрачным: неполный латинский квадрат соответствует неполной линейной таблице (в любых ее двух строках каждая пара элементов из $\{1, 2, \ldots, n\}$ появляется не более одного раза), и любой квадрат, сопряженный к неполному латинскому квадрату, снова является неполным латинским квадратом. В частности, неполный латинский квадрат можно дополнить до полного тогда и только тогда, когда всякий сопряженный ему можно дополнить до полного (действительно, можно дополнить сопряженный, а затем обратить перестановку трех строк линейной таблицы).

Если циклически переставить линии в предыдущем примере: $R \longrightarrow C \longrightarrow E \longrightarrow R$, то получатся следующие линейная таблица и латинский квадрат:

1	2	3
3	1	2
2	3	1

R : 1 3 2 2 1 3 3 2 1
C: 1 1 1 2 2 2 3 3 3
E: 1 2 3 1 2 3 1 2 3

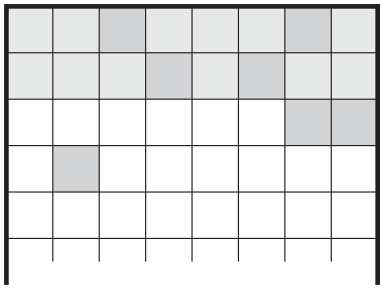
Нам потребуются два результата, принадлежащие Герберту Дж. Райзеру [3] и Чарльзу К. Линднеру [2]; они были известны еще до теоремы Сметанюка. Неполный латинский квадрат, в котором первые r строк заполнены целиком, а остальные клетки пусты, называется $(r \times n)$-*латинским прямоугольником*.

Лемма 1. *Любой $(r \times n)$-латинский прямоугольник, $r < n$, можно расширить до $((r+1) \times n)$-латинского прямоугольника и, следовательно, можно дополнить до полного латинского квадрата.*

■ **Доказательство.** Применим теорему Ф. Холла (см. гл. 27). Пусть A_j — совокупность элементов множества $\{1, 2, \ldots, n\}$, *отсутствующих* в столбце j. Допустимая $(r+1)$-я строка в точности соответствует системе различных представителей для семейства множеств $A_1, \ldots, A_n$. Поэтому для доказательства леммы мы должны проверить выполнение условия (H) теоремы Холла. Каждое множество A_j имеет размер $n-r$, каждый элемент принадлежит ровно $n-r$ множествам A_j (так как он встречается в латинском прямоугольнике r раз). Любые m множеств A_j содержат вместе $m(n-r)$ элементов и, следовательно, не меньше m различных, что означает выполнение условия (H). □

Лемма 2. *Пусть P — неполный латинский квадрат, в котором заполнено не более $n-1$ ячеек и содержится не более $\frac{n}{2}$ различных элементов. Тогда P можно дополнить до полного латинского квадрата порядка n.*

■ **Доказательство.** Сначала приведем задачу к более удобному виду. В силу указанного выше принципа сопряженности можно заменить условие «не более $\frac{n}{2}$ различных элементов» условием «элементы содержатся не более чем в $\frac{n}{2}$ строках». Далее, можно предполагать, что эти строки являются верхними строками квадрата. Итак, пусть строки с заполненными ячейками имеют номера $1, 2, \ldots, r$, причем в строке i заполнено f_i ячеек, где $r \le \frac{n}{2}$ и $\sum_{i=1}^{r} f_i \le n-1$. Перестановкой строк можно добиться выполнения условия $f_1 \ge f_2 \ge \ldots \ge f_r$. Покажем теперь, что можно шаг за шагом заполнять строки $1, \ldots, r$, пока не получится $(r \times n)$-латинский прямоугольник, который в силу леммы 1 можно расширить до латинского квадрата.



Ситуация для $n = 8$ с $\ell = 3$, $f_1 = f_2 = f_3 = 2$, $f_4 = 1$. Темные клетки были заполнены с самого начала, более светлые клетки заполнены в процессе дополнения.

Предположим, что строки $1, 2, \ldots, \ell-1$ полностью заполнены. В строке ℓ имеется f_ℓ заполненных ячеек; можно предполагать, что они находятся в конце этой строки. Текущая ситуация изображена на полях, где заштрихованы заполненные ячейки.

Строка ℓ заполняется с помощью еще одного применения теоремы Ф. Холла, но на этот раз весьма тонкого. Пусть X — множество элементов из $\{1, 2, \ldots, n\}$, *не появившихся* в строке ℓ, так что $|X| = n - f_\ell$. Для $j = 1, \ldots, n - f_\ell$ обозначим через A_j множество элементов X, *отсутствующих* в столбце j (как выше, так и ниже строки ℓ). Чтобы доказать возможность заполнения строки ℓ, мы должны проверить выполнение условия (H) для семейства $A_1, \ldots, A_{n-f_\ell}$.

Во-первых, покажем, что

$$n - f_\ell - \ell + 1 \;>\; \ell - 1 + f_{\ell+1} + \ldots + f_r. \qquad (1)$$

В случае $\ell = 1$ это очевидно. В противном случае из неравенств $\sum_{i=1}^{r} f_i < n$, $f_1 \ge \ldots \ge f_r$ и $1 < \ell \le r$ вытекает, что

$$n \;>\; \sum_{i=1}^{r} f_i \;\ge\; (\ell-1) f_{\ell-1} + f_\ell + \ldots + f_r.$$

Если $f_{\ell-1} \ge 2$, то (1) выполняется; если же $f_{\ell-1} = 1$, то неравенство (1) принимает вид $n > 2(\ell-1) + r - \ell + 1 = r + \ell - 1$, что верно, поскольку $\ell \le r \le \frac{n}{2}$.

Возьмем теперь m множеств A_j, $1 \le m \le n - f_\ell$, и пусть B — их объединение. Нам нужно показать, что $|B| \ge m$. Пусть c — число клеток с элементами из X в m столбцах, которые соответствуют множествам A_j. Выше строки ℓ таких клеток не больше $(\ell-1)m$, а ниже — не более $f_{\ell+1} + \ldots + f_r$. Следовательно,

$$c \;\le\; (\ell-1)m + f_{\ell+1} + \ldots + f_r.$$

С другой стороны, так как каждый элемент $x \in X\backslash B$ появляется в каждом из этих m столбцов, то $c \ge m(|X| - |B|)$, так что (поскольку $|X| = n - f_\ell$)

$$|B| \;\ge\; |X| - \tfrac{1}{m}c \;\ge\; n - f_\ell - (\ell-1) - \tfrac{1}{m}(f_{\ell+1} + \ldots + f_r).$$

Отсюда вытекает, что $|B| \ge m$, если

$$n - f_\ell - (\ell-1) - \tfrac{1}{m}(f_{\ell+1} + \ldots + f_r) \;>\; m - 1,$$

т. е. если

$$m(n - f_\ell - \ell + 2 - m) \quad > \quad f_{\ell+1} + \ldots + f_r. \tag{2}$$

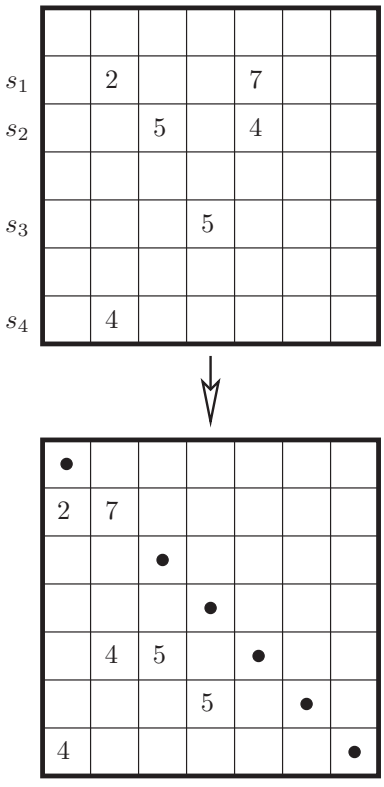
Ввиду (1) неравенство (2) справедливо для $m = 1$ и $m = n - f_\ell - \ell + 1$ и, следовательно, для всех значений m между 1 и $n - f_\ell - \ell + 1$, так как левая часть (2) — квадратичная функция от m со старшим коэффициентом -1. Остается случай $m > n - f_\ell - \ell + 1$. Так как каждый элемент $x \in X$ содержится не более чем в $\ell - 1 + f_{\ell+1} + \ldots + f_r$ строках, то количество содержащих его столбцов тоже не больше $\ell - 1 + f_{\ell+1} + \ldots + f_r$. Еще раз используя (1), мы находим, что x содержится менее чем в m столбцах и поэтому принадлежит одному из множеств A_j. Значит, в этом случае $B = X$, $|B| = n - f_\ell \ge m$, условие (Н) теоремы Холла выполняется, и доказательство завершено. □

Докажем, наконец, теорему Сметанюка.

Теорема. *Неполный латинский квадрат порядка n, в котором заполнено не более $n-1$ клеток, можно дополнить до полного латинского квадрата того же порядка.*

■ **Доказательство.** Используем индукцию по n. Случаи $n \le 2$ тривиальны. Поэтому рассмотрим неполный латинский квадрат порядка $n \ge 3$, в котором заполнено не более $n-1$ клеток. Используя те же обозначения, что и выше, будем считать, что эти клетки лежат в $r \le n-1$ разных строках с номерами $s_1, \ldots, s_r$, содержащих $f_1, \ldots, f_r > 0$ заполненных клеток, и $\sum_{i=1}^{r} f_i \le n-1$. В силу леммы 2 достаточно рассмотреть случай, когда число различных элементов больше $\frac{n}{2}$. Тогда существует элемент, появляющийся лишь один раз. Перенумерацией элементов и перестановкой строк можно добиться того, чтобы единственный раз появлялся элемент n и чтобы он находился в s_1-й строке.

Следующим шагом мы переставим строки и столбцы неполного латинского квадрата так, чтобы все заполненные клетки оказались ниже главной диагонали (состоящей из клеток вида (k,k), $1 \le k \le n$), за исключением клетки, содержащей n, которая попадет на эту диагональ. Для этого сначала переместим строку s_1 на место f_1. Переставляя столбцы, переместим все заполненные клетки этой строки влево



так, чтобы n оказался последним элементом в этой строке и лежал на диагонали. Затем переместим строку, имевшую вначале номер s_2, на место $1 + f_1 + f_2$, и опять переместим заполненные клетки насколько возможно влево. Вообще, для каждого $i = 2, \ldots, r$ переместим строку с исходным номером s_i на место $1 + f_1 + f_2 + \ldots + f_i$, а ее заполненные клетки — насколько можно влево. Ясно, что в результате мы получим желаемое расположение. На полях приведен пример с $n = 7$: строки с номерами $s_1 = 2$, $s_2 = 3$, $s_3 = 5$ и $s_4 = 7$ и числами заполненных клеток $f_1 = f_2 = 2$ и $f_3 = f_4 = 1$ перемещены на места строк 2, 5, 6 и 7, а столбцы с заполненными клетками смещены влево так, что все эти клетки (кроме клетки с 7) оказались ниже диагонали, помеченной знаками •.

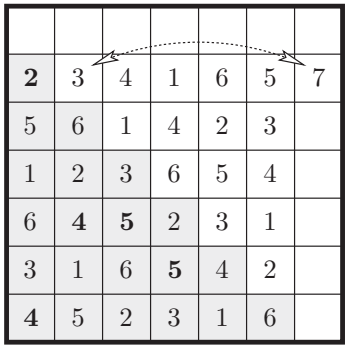
Чтобы применить метод индукции, удалим с диагонали элемент n и не будем обращать внимание на первую строку и последний столбец (не содержащие теперь заполненных клеток). Тогда мы получим неполный латинский квадрат порядка $n-1$ с не более чем $n-2$ заполненными клетками. По предположению индукции его можно дополнить до латинского квадрата порядка $n-1$. На полях изображено одно из (многих) дополнений неполного латинского квадрата в нашем примере; элементы исходного заполнения отмечены жирным шрифтом. Они уже стоят на своих местах, как и все элементы в заштрихованных клетках; остальные элементы при дальнейшем построении полного латинского квадрата порядка n могут изменять свои места.

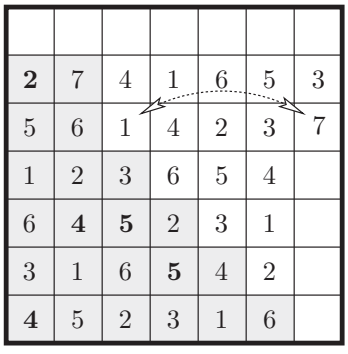
Далее мы хотим переместить элементы, стоящие на диагонали, в последний n-й столбец, а их места на диагонали занять элементами n. Однако в общем случае сделать это нельзя, так как диагональные элементы не обязаны быть различными. Поэтому будем осторожнее и последовательно, для $k = 2, 3, \ldots, n-1$ (в этом порядке), выполним следующие действия:

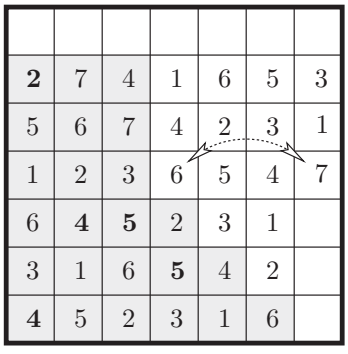
Поместим элемент n в клетку (k, n). Это даст правильный неполный латинский квадрат. Затем поменяем местами элемент x_k в диагональной клетке (k, k) и элемент n в клетке (k, n) столбца n.

Если элемент x_k еще не появлялся в последнем столбце, то работа для этого k закончена и в дальнейшем элементы k-го столбца изменяться не будут.

В нашем примере такая ситуация возникает при $k = 2$, 3 и 4, и диагональные элементы 3, 1 и 6 перемещаются в последний столбец. На следующих трех рисунках показаны производимые действия.



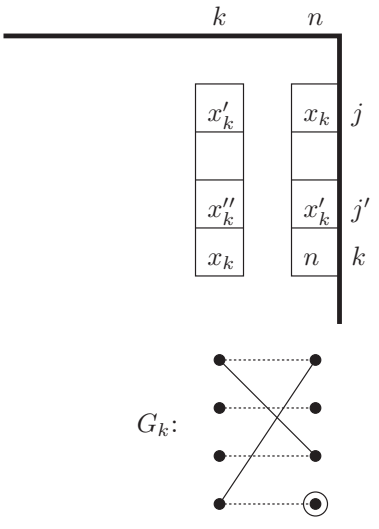




Теперь рассмотрим случай, когда элемент x_k уже содержится в последнем столбце. Тогда действуем следующим образом:

Если элемент x_k уже находится в клетке (j, n), $2 \le j < k$, то меняем местами в j-й строке элемент x_k из n-го столбца и элемент x'_k из k-го столбца. Если элемент x'_k находится в клетке (j', n), то меняем местами элементы j'-й строки, стоящие в n-м и в k-м столбцах, и т. д.

При таких операциях ни в какой строке никогда не появится двух одинаковых элементов. Покажем, что при обменах элементов k-го и n-го столбцов не может возникнуть бесконечный цикл (поэтому в конце концов каждый столбец оказывается состоящим из разных элементов). Рассмотрим двудольный граф G_k, вершины которого соответствуют тем клеткам (i, k) и (j, n), $2 \le i, j \le k$, элементы которых могут обмениваться. Вершины (i, k) и (j, n) соединены ребром, если эти клетки лежат в одной строке (т. е. $i = j$) или если эти клетки до обменов содержали одинаковые элементы (тогда $i \ne j$). На рисунке на полях ребра с $i = j$ изображены пунктирными линиями, а остальные — сплошными. Степени всех вершин в G_k равны 1 или 2. Клетка (k, n) — это вершина степени 1; с нее начинается путь, который ведет к столбцу k по горизонтальному ребру, затем, возможно, по наклонному ребру обратно к столбцу n, потом по горизонтали к столбцу k и т. д. Он заканчивается в столбце k на элементе, который не встречался в столбце n. Значит, обмены закончатся в момент, когда мы переместим в последний столбец *новый* для этого столбца элемент. Тогда работа с k-м столбцом заканчивается, и элементы в клетках (i, k) с $i \ge 2$ больше не изменяются.



В нашем примере «цепочка обменов» возникает при $k = 5$: элемент $x_5 = 3$ уже появлялся в последнем столбце, поэтому его следует обменять с элементом $x'_5 = 6$ столбца $k = 5$. Но такой элемент тоже появлялся в последнем столбце, поэтому он меняется местами с $x''_5 = 5$. Такого элемента в последнем столбце не было, и очередной цикл обменов заканчивается.

2	7	4	1	6	5	3
5	6	7	4	2	3	1
1	2	3	7	5	4	6
6	**4**	**5**	2	3	1	7
3	1	6	**5**	4	2	
4	5	2	3	1	6	

2	7	4	1	3	5	6
5	6	7	4	2	3	1
1	2	3	7	6	4	5
6	**4**	**5**	2	7	1	3
3	1	6	**5**	4	2	
4	5	2	3	1	6	

Наконец, при обменах элементов для $k = 6 = n - 1$ трудностей не возникает, и после этого в нашем примере дополнение до полного латинского квадрата проводится однозначно:

2	7	4	1	3	5	6
5	6	7	4	2	3	1
1	2	3	7	6	4	5
6	**4**	**5**	2	7	1	3
3	1	6	**5**	4	2	7
4	5	2	3	1	6	

2	7	4	1	3	5	6
5	6	7	4	2	3	1
1	2	3	7	6	4	5
6	**4**	**5**	2	7	1	3
3	1	6	**5**	4	7	2
4	5	2	3	1	6	

7	3	1	6	4	2	4
2	7	4	1	3	5	6
5	6	7	4	2	3	1
1	2	3	7	6	4	5
6	**4**	**5**	2	7	1	3
3	1	6	**5**	4	7	2
4	5	2	3	1	6	7

... как и в общем случае. После обмена элементов $(n-1)$-й строки мы помещаем элемент n в клетку (n, n), и после этого первую строку можно заполнить элементами, отсутствующими в соответствующих столбцах (см. лемму 1), что завершает доказательство.

Чтобы получить в явном виде дополнение исходного неполного латинского квадрата порядка n, нам остается провести перенумерацию элементов и перестановки строк и столбцов, обратные к сделанным на первых двух шагах доказательства. □

Литература

[1] Evans T. *Embedding incomplete Latin squares.* Amer. Math. Monthly, **67** (1960), 958–961.

[2] Lindner C. C. *On completing Latin rectangles.* Canadian Math. Bulletin, **13** (1970), 65–68.

[3] Ryser H. J. *A combinatorial theorem with an application to Latin rectangles.* Proc. Amer. Math. Soc., **2** (1951), 550–552.

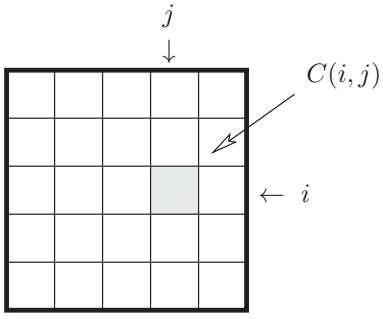
[4] Smetaniuk B. *A new construction on Latin squares. I: A proof of the Evans conjecture.* Ars Combinatoria, **11** (1981), 155–172.

Теория графов

«Четырехкрасочный географ»

Глава 33 Задача Диница

Хорошо известно, что проблема четырех красок была главной движущей силой, которая привела теорию графов к ее современному состоянию, и раскраска остается излюбленной темой многих специалистов. Здесь мы рассмотрим просто формулируемую задачу о раскраске, которую поставил Джефф Диниц в 1978 году и к которой не удавалось найти подходы, пока 15 годами позднее Фред Галвин не получил изумительно простое решение.



Рассмотрим n^2 клеток, образующих квадрат размера $(n \times n)$. Пусть (i, j) обозначает клетку на пересечении строки i и столбца j. Пусть для каждой клетки (i, j) задано множество $C(i, j)$, состоящее из n разных цветов.
Всегда ли можно закрасить все клетки (выбирая для раскраски каждой клетки (i, j) цвета из множества $C(i, j)$) так, чтобы цвета клеток в каждой строке и в каждом столбце были различными?

Вначале рассмотрим случай, когда все множества $C(i, j)$ совпадают; например, $C(i, j) = \{1, 2, \ldots, n\}$ для всех i и j. Тогда задача Диница сводится к следующей: заполнить клетки $(n \times n)$-квадрата числами $1, 2, \ldots, n$ так, чтобы числа в любой строке и в любом столбце были разными. Другими словами, раскраски с $C(i, j) = \{1, \ldots, n\}$ соответствуют латинским квадратам, о которых шла речь в предыдущей главе. Значит, в этом случае ответ на наш вопрос — «да».

Если здесь все так просто, то почему задача становится значительно сложнее в общем случае, даже когда множество $C := \bigcup_{i,j} C(i, j)$ содержит больше n цветов? Причиной сложности является то, что для раскраски произвольной клетки нельзя использовать любой цвет из C. Например, при построении латинского квадрата для первой строки, очевидно, можно выбрать произвольную перестановку цветов, но это не так в общей задаче. Сложности возникают даже в случае $n = 2$.

$\{1, 2\}$	$\{2, 3\}$
$\{1, 3\}$	$\{2, 3\}$

Пусть заданы множества цветов, указанные на рисунке. Если для раскраски первой строки выбрать цвета 1 и 2, то для обеих клеток второй строки придется выбрать цвет 3, что противоречит условию.

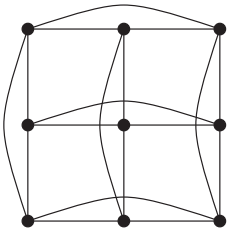
Прежде чем браться за задачу Диница, переформулируем ее на языке теории графов. Как обычно, будем рассматривать лишь графы $G = (V, E)$ без петель и кратных ребер. Пусть $\chi(G)$ — *хроматическое число* графа, т. е. наименьшее число цветов, которыми можно раскрасить его вершины так, чтобы смежные вершины получили разные цвета[1].

[1] В дальнейшем, говоря о раскраске вершин графа, авторы имеют в виду именно такие раскраски. — *Прим. перев.*

Другими словами, раскраска порождает такое разбиение множества вершин на классы (вершин одного цвета), что ребра между вершинами из одного и того же класса отсутствуют. Назовем множество $A \subseteq V$ *независимым*, если вершины из A не связаны между собой ребрами графа G. Тогда хроматическое число есть наименьшее число независимых множеств, образующих разбиение множества вершин V.

В 1976 году Визинг [5], а тремя годами позже Эрдёш, Рубин и Тейлор [1] изучали следующий вариант раскраски, который прямо приводит к задаче Диница. Пусть для каждой вершины v графа $G = (V, E)$ задано множество цветов $C(v)$. *Списочная раскраска* есть такое отображение $c : V \longrightarrow \bigcup_{v \in V} C(v)$, что $c(v) \in C(v)$ для каждого $v \in V$. Теперь легче понять определение *списочного хроматического числа* $\chi_\ell(G)$: это наименьшее такое число k, что списочная раскраска существует для *любого* списка множеств цветов $C(v)$ с $|C(v)| = k$ при всех $v \in V$. Конечно, справедливо неравенство $\chi_\ell(G) \le |V|$ (при $k > |V|$ у нас никогда не будет недостатка в цветах). Так как обычная раскраска является частным случаем списочной раскраски (когда все множества $C(v)$ одинаковы), то для любого графа G

$$\chi(G) \quad \le \quad \chi_\ell(G).$$



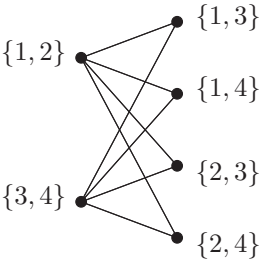
Граф S_3

Вернемся к задаче Диница и рассмотрим граф S_n, множество вершин которого состоит из n^2 клеток нашей $(n \times n)$-таблицы, причем две вершины смежны тогда и только тогда, когда они находятся в одной и той же строке или в одном и том же столбце.

Так как все n клеток одной строки попарно смежны, для раскраски требуется не менее n цветов. Далее, любой раскраске вершин S_n в n цветов соответствует латинский квадрат, а клетки, в которых размещено одно и то же число, образуют класс одного цвета. Как мы уже видели, латинские квадраты существуют, поэтому $\chi(S_n) = n$, и задачу Диница теперь можно кратко сформулировать так: верно ли, что

$$\chi_\ell(S_n) \;=\; n?$$

Можно подумать, что вообще $\chi(G) = \chi_\ell(G)$ для любого графа G, но это весьма далеко от истины. Рассмотрим, например, изображенный на полях граф $G = K_{2,4}$. Его хроматическое число равно 2, так как можно использовать при раскраске один цвет для двух вершин слева и другой — для вершин справа. Пусть теперь заданы множества цветов, указанные на рисунке. При раскраске левых вершин мы имеем четыре возможности: 1|3, 1|4, 2|3 и 2|4, но любая из этих пар является множеством цветов одной из вершин с правой стороны, так что в этом случае списочная раскраска невозможна. Следовательно, $\chi_\ell(G) \ge 3$, и читатель может получить удовольствие, доказав, что $\chi_\ell(G) = 3$ (при этом не нужно проверять все варианты!). Обобщая этот пример, нетрудно построить графы G, для которых $\chi(G) = 2$, но $\chi_\ell(G)$ сколь угодно велико! Поэтому задача о списочной раскраске не так проста, как это выглядит на первый взгляд.

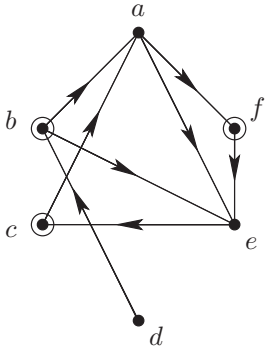


Снова обратимся к задаче Диница. Важный шаг к ее решению сделала в 1992 году Джанетт Янссен [4], доказав, что $\chi_\ell(S_n) \le n + 1$, а завершил решение Фред Галвин [3], остроумно соединив два давно известных результата. Сначала обсудим эти результаты, а затем покажем, как из них следует равенство $\chi_\ell(S_n) = n$.

Прежде всего введем несколько обозначений. Пусть v — некоторая вершина графа G, и, как и раньше, d_v обозначает *степень вершины* v. В рассматриваемом квадратном графе S_n каждая вершина имеет степень $2n-2$, так как она смежна $n-1$ другим вершинам в той же строке и в том же столбце. Для подмножества $A \subseteq V$ обозначим G_A подграф графа $G = (V, E)$, имеющий множество вершин A и содержащий все ребра графа G между вершинами из A. Назовем G_A подграфом, индуцированным множеством A, и будем говорить, что H — *индуцированный подграф* графа G, если $H = G_A$ для некоторого $A \subseteq V$.

В формулировке первого утверждения используются *ориентированные графы* (*орграфы*) $\vec{G} = (V, E)$, т. е. графы, все ребра которых имеют ориентацию[2]. Запись $e = (u, v)$ (или $u \longrightarrow v$) означает, что e — дуга с начальной вершиной u и конечной вершиной v. При этом имеет смысл говорить о *степени выхода* d_v^+ и, соответственно, о *степени входа* d_v^- вершины v: d_v^+ — число дуг с начальной вершиной v, а d_v^- — число дуг с конечной вершиной v. Очевидно, выполняется равенство $d_v^+ + d_v^- = d_v$. Запись G будет обозначать граф $\vec{G}$ без ориентации.

Следующее понятие возникло при анализе игр и будет играть решающую роль в дальнейшем обсуждении.



Определение 1. Пусть $\vec{G} = (V, E)$ — орграф. *Ядром* $K \subseteq V$ называется такое подмножество V, что

(i) K — независимое множество в G,

(ii) для каждой вершины $u \in V \backslash K$ существует дуга $u \longrightarrow v$, $v \in K$.

Рассмотрим приведенный на полях пример. Вершины $\{b, c, f\}$ образуют ядро, а индуцированный множеством $\{a, c, e\}$ подграф не имеет ядра, так как три дуги (a, e), (e, c) и (c, a) образуют цикл.

Теперь можно сформулировать первое утверждение.

Лемма 1. *Пусть $\vec{G} = (V, E)$ — орграф и для каждой вершины $v \in V$ задано множество цветов $C(v)$, мощность которого больше степени выхода: $|C(v)| \geq d_v^+ + 1$. Если каждый индуцированный подграф графа $\vec{G}$ имеет ядро, то существует списочная раскраска графа G, в которой каждой вершине $v \in V$ сопоставлен цвет из $C(v)$.*

■ **Доказательство.** Используем индукцию по $|V|$. Для $|V| = 1$ доказывать нечего. Допустим, что лемма верна для всех орграфов с числом вершин, меньшим $|V|$. Выберем цвет $c \in C = \bigcup_{v \in V} C(v)$ и положим

$$A(c) \;:=\; \{v \in V : c \in C(v)\}.$$

По условию индуцированный подграф $G_{A(c)}$ имеет ядро $K(c)$. Окрасим все вершины $v \in K(c)$ цветом c (это возможно, так как $K(c)$ — независимое множество) и удалим $K(c)$ из G, а c из C. Пусть G' — индуцированный подграф графа G на $V \backslash K(c)$ с множествами цветов $C'(v) = C(v) \backslash c$. Заметим, что для каждой вершины $v \in A(c) \backslash K(c)$ степень выхода $d'^+_v \leq d_v^+ - 1$ (в силу второго свойства ядра), поэтому $d'^+_v + 1 \leq |C'(v)|$. Это неравенство справедливо и для вершин вне $A(c)$, так как для них множества цветов $C(v)$ не изменяются. Новый граф G' содержит меньше вершин, чем G. По предположению индукции для

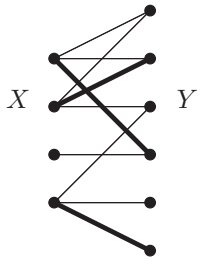
[2] Ориентированные ребра далее называются *дугами*. — *Прим. перев.*

него и для множеств $C'(v)$ существует списочная раскраска. Возвращение множества вершин $K(c)$ не нарушит правил раскраски, и тем самым индукционный шаг обоснован. □

Теперь ясно, как решать задачу Диница: достаточно найти ориентацию графа S_n со степенями выхода $d_v^+ \le n-1$ для всех v, при которой все индуцированные подграфы имеют ядра. При этом используется второй результат.

Нам снова потребуется небольшая подготовка. Вспомним (см. гл. 10), что граф $G = (X \cup Y, E)$ — *двудольный*, если множество его вершин V разбито на две части X и Y так, что каждое ребро имеет один конец в X, а другой в Y. Другими словами, двудольными являются те и только те графы, которые можно раскрасить в два цвета (один цвет для вершин из X, а второй — для вершин из Y).

Введем важное понятие «устойчивого паросочетания» (с житейской интерпретацией). *Паросочетание* M в двудольном графе $G = (X \cup Y, E)$ — это такое множество ребер, что никакие два ребра из M не имеют общих концевых вершин. Например, в графе, изображенном на полях, выделенные ребра составляют паросочетание.



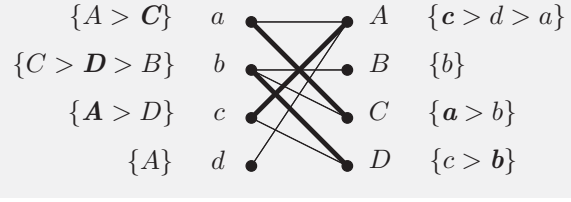
Двудольный граф с паросочетанием

Пусть X — множество парней, Y — множество девушек, а наличие ребра $uv \in E$ означает, что u и v могут пожениться. Тогда паросочетание есть коллективная свадьба, в которой каждый заключает не более одного брака. Нам потребуется более изящный (и более практичный?) вариант паросочетания, предложенный Дэвидом Гейлом и Ллойдом Шепли [2]. Ясно, что в реальной жизни лицо имеет предпочтения, и эту особенность мы добавим к нашей ситуации. Предположим, что в графе $G = (X \cup Y, E)$ для каждого $v \in X \cup Y$ задано упорядочение множества $N(v)$ вершин, смежных с v: $N(v) = \{z_1 > z_2 > \ldots > z_{d_v}\}$. Тогда z_1 — самый желанный выбор для v, за ним следует z_2, и т. д.

Определение 2. Паросочетание M в двудольном графе $G = (X \cup Y, E)$ называется *устойчивым*, если для любого ребра $uv \in E \backslash M$, где $u \in X$, $v \in Y$, либо $uy \in M$ и $y > v$ в $N(u)$, либо $xv \in M$ и $x > u$ в $N(v)$, либо выполняется и то, и другое.

В нашей интерпретации множество бракосочетаний устойчиво, если в нем отсутствуют ситуации, когда брак между $u \in N(v)$ и $v \in N(u)$ не заключен, но u предпочитает v своей жене (или не женат), а v предпочитает u своему мужу (или не замужем); естественно, такие ситуации неустойчивы.

Прежде чем доказывать наше второе утверждение, рассмотрим следующий пример.



Выделенные ребра образуют устойчивое паросочетание. В каждой строке приоритетов выбор, приводящий к устойчивому паросочетанию, напечатан жирным шрифтом.

В этом примере имеется единственное максимальное паросочетание $M = \{aC, bB, cD, dA\}$ с четырьмя ребрами, но оно не устойчиво (из-за ребра cA).

Лемма 2. *Устойчивое паросочетание всегда существует.*

■ **Доказательство.** Рассмотрим следующий алгоритм. На первом шаге все парни $u \in X$ делают предложения своим самым желанным девушкам. Если девушка получает хотя бы одно предложение, она выбирает из них наиболее желанного парня и считает его кандидатом в женихи. Оставшиеся парни отвергнуты и образуют резерв R.

На втором шаге все парни из R делают предложения своим вторым по предпочтениям девушкам. Каждая девушка сравнивает предложения (учитывая кандидата в женихи, если таковой имеется), выбирает наиболее предпочтительного парня и делает его кандидатом в женихи. Отвергнутые парни составляют новый резерв R.

После этого парни из R делают предложения своим следующим по предпочтениям девушкам, и т. д. Парень, который сделал предложение последней по его предпочтениям девушке и был отвергнут, исключается из дальнейшего рассмотрения (а также из резерва). Ясно, что через некоторое время резерв R окажется пустым, и в этот момент алгоритм заканчивает работу.

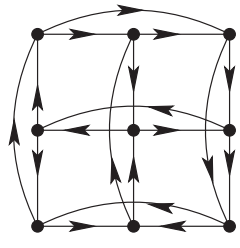
> ***Утверждение.*** *Если алгоритм завершил работу, то кандидаты в женихи вместе с выбравшими их девушками образуют устойчивое паросочетание.*

Заметим вначале, что для каждой девушки выбираемые ею кандидаты в женихи становятся (для нее) все более желанными, так как на каждом шаге она сравнивает новые предложения с кандидатом в женихи и выбирает наиболее желанного. Поэтому, если $uv \in E$, но $uv \notin M$, то либо u никогда не делал предложение v (и в этом случае u нашел лучшую супругу прежде, чем очередь дошла до v, значит, $uy \in M$, причем $y > v$ в $N(u)$), либо u делал предложение v и был отвергнут (откуда следует, что $xv \in M$, где $x > u$ в множестве $N(v)$). Но это есть как раз условие, определяющее устойчивое паросочетание. □

Соединяя вместе леммы 1 и 2, мы получим решение задачи Диница, которое нашел Галвин.

Теорема. *Для всех n справедливо равенство $\chi_\ell(S_n) = n$.*

1	2	3
3	1	2
2	3	1

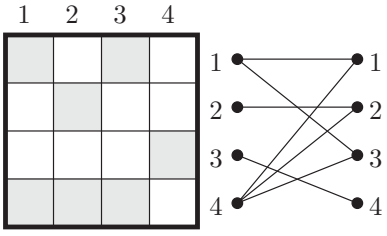


■ **Доказательство.** Как и раньше, обозначим вершины через (i, j), $1 \le i,\ j \le n$. Вершины (i, j) и (r, s) смежны тогда и только тогда, когда $i = r$ или $j = s$. Рассмотрим произвольный латинский квадрат с числами $\{1, 2, \ldots, n\}$ и обозначим $L(i, j)$ число в клетке (i, j). Далее, превратим S_n в орграф $\vec{S}_n$, ориентируя горизонтальные ребра по правилу $(i, j) \longrightarrow (i, j')$, если $L(i, j) < L(i, j')$, а вертикальные ребра по правилу $(i, j) \longrightarrow (i', j)$, если $L(i, j) > L(i', j)$. Итак, горизонтальные ребра ориентируются от меньшего элемента к большему, а вертикальные — наоборот. (На полях приведен пример для $n = 3$.)

Заметим, что $d^+_{(i,j)} = n - 1$ для всех (i, j). Действительно, если $L(i, j) = k$, то в строке i содержимое $n - k$ клеток больше k, а в столбце j содержимое $k - 1$ клеток меньше k.

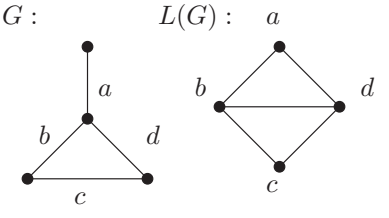
В силу леммы 1 остается показать, что каждый индуцированный подграф орграфа $\vec{S}_n$ имеет ядро. Рассмотрим подмножество клеток A.

Пусть X — множество строк L, а Y — множество его столбцов. Сопоставим A двудольный граф $G = (X \cup Y, A)$, в котором каждая пара $(i, j) \in A$ соответствует ребру ij, где $i \in X, j \in Y$. В примере на полях клетки, входящие в A, заштрихованы.



Ориентация S_n естественно порождает упорядочения в окрестностях $N(i)$ вершин графа $G = (X \cup Y, A)$: можно положить $j' > j$ в $N(i)$, $i \in X$, если $(i, j) \longrightarrow (i, j')$ в $\vec{S}_n$, и положить $i' > i$ в $N(j)$, $j \in Y$, если $(i, j) \longrightarrow (i', j)$. Согласно лемме 2 граф $G = (X \cup Y, A)$ имеет устойчивое паросочетание M. Множество M — искомое ядро подграфа $\vec{S}_n$, индуцированного множеством A. Действительно, во-первых, M — независимое множество в этом подграфе, поскольку элементы M (как ребра графа $G = (X \cup Y, A)$) не имеют общих концов i или j. Во-вторых, если $(i, j) \in A \backslash M$, то по определению устойчивого паросочетания существует либо $(i, j') \in M$ с $j' > j$, либо $(i', j) \in M$ с $i' > i$; для $\vec{S}_n$ это означает, что либо дуга $(i, j) \longrightarrow (i, j') \in M$, либо дуга $(i, j) \longrightarrow (i', j) \in M$, и доказательство закончено. □

Завершая эту главу, выйдем немного за ее пределы. Читатель мог заметить, что граф S_n возникает из двудольного с помощью простого построения. Пусть $K_{n,n}$ — полный двудольный граф с множеством вершин $X \cup Y$, $|X| = |Y| = n$, и множеством ребер $\{(u, v) : u \in X, v \in Y\}$. Рассмотрим новый граф, вершинами которого являются ребра графа $K_{n,n}$, а ребра соединяют две такие вершины тогда и только тогда, когда они (как ребра $K_{n,n}$) имеют общую вершину. Легко проверить, что он совпадает с квадратным графом S_n. Будем говорить, что S_n — *реберный граф* для $K_{n,n}$. Такое же построение для произвольного графа G дает так называемый *реберный граф* $L(G)$ графа G.



Построение реберного графа

В общем случае назовем H *реберным графом*, если $H = L(G)$ для некоторого графа G. Конечно, не всякий граф является реберным: примером является рассмотренный ранее граф $K_{2,4}$, для которого, как мы видели, $\chi(K_{2,4}) < \chi_\ell(K_{2,4})$. Но что будет, если H — реберный граф? Изменяя доказательство нашей теоремы, нетрудно показать, что $\chi(H) = \chi_\ell(H)$, если H — реберный граф *двудольного* графа. Возможно, метод можно применить при проверке главной гипотезы в этой области:

Верно ли, что $\chi(H) = \chi_\ell(H)$ для любого реберного графа H?

Об этой гипотезе известно очень мало, и задача кажется сложной, но, в конце концов, такой же казалась задача Диница 20 лет тому назад.

Литература

[1] Erdős P., Rubin A. L., Taylor H. *Choosability in graphs.* Proc. West Coast Conference on Combinatorics, Graph Theory and Computing, Congressus Numerantium, **26** (1979), 125–157.

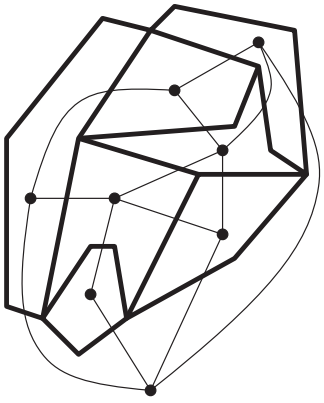
[2] Gale D., Shapley L. S. *College admissions and the stability of marriage.* Amer. Math. Monthly, **69** (1962), 9–15.

[3] Galvin F. *The list chromatic index of a bipartite multigraph.* J. Combinatorial Theory, Ser. B, **63** (1995), 153–158.

[4] Janssen J. C. M. *The Dinitz problem solved for rectangles.* Bulletin Amer. Math. Soc., **29** (1993), 243–249.

[5] Визинг В. Г. *Раскраска вершин графа в предписанные цвета.* Дискретный анализ, вып. 29, Новосибирск, 1976, с. 3–10.

Глава 34 Задача о пяти красках для плоских графов

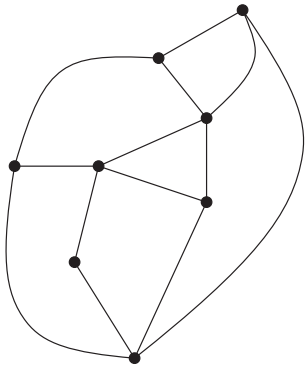


Граф, двойственный карте

Плоские графы и их раскраски интенсивно изучали с момента возникновения теории графов ввиду их связи с проблемой четырех красок. Первоначально формулировка проблемы четырех красок была такой: всегда ли можно раскрасить области плоской карты четырьмя красками так, чтобы области с общей границей (а не просто с общей точкой) получили разные цвета? Чертеж на полях показывает, что раскраска областей карты по сути дела то же самое, что и раскраска вершин плоского графа. Как в гл. 12, внутри каждой области (включая внешнюю область) разместим вершину, и каждые две вершины, лежащие в соседних областях, соединим ребром, которое пересекает их общую границу.

Получающийся граф G — *граф, двойственный карте* M, — также является плоским графом, и раскраска вершин графа G в обычном смысле есть то же самое, что раскраска областей карты M. Поэтому в дальнейшем мы будем говорить только о раскраске вершин плоских графов. Можно предполагать, что G не имеет петель и кратных ребер, так как они не существенны для раскраски.

В длительной и трудной истории поисков решения проблемы четырех красок многие были близки к цели, и появившиеся в конце концов доказательство Аппеля – Хейкена 1976 года и недавнее доказательство Робертсона, Сандерса, Сеймора и Томаса 1997 года [4], оказались сочетанием очень старых идей (восходящих к XIX веку) и вычислительных возможностей самых современных компьютеров. Двадцать пять лет спустя после первого доказательства ситуация по существу остается той же самой: существует построенное компьютером и проверяемое с помощью компьютера доказательство, построенное Гонтье [3], но доказательства из Книги пока не видно.



Этот плоский граф имеет 8 вершин, 13 ребер и 7 областей.

Поэтому будем скромнее и выясним, существует ли красивое доказательство того, что каждый плоский граф можно раскрасить пятью красками. Эта теорема о пяти красках была доказана Хивудом[1] еще в конце XIX века. Основным инструментом в его доказательстве (а также в теореме о четырех красках) была формула Эйлера (см. гл. 12). Ясно, что при раскраске графа G можно предположить, что G связен, так как связные компоненты можно раскрашивать по отдельности. Плоский граф делит плоскость на некоторое множество R областей, включая внешнюю область. Формула Эйлера утверждает, что для любого плоского связного графа $G = (V, E)$ справедливо равенство

$$|V| - |E| + |R| \;=\; 2.$$

В качестве подготовки посмотрим, как можно с помощью формулы Эйлера доказать, что шести цветов достаточно для раскраски любого

[1] Доказательство теоремы о пяти красках можно найти, например, в [9*]. — *Прим. перев.*

плоского графа G. Применим индукцию по числу вершин n. Для малых значений n (в частности, для $n \le 6$) это очевидно.

Согласно части (A) Предложения на с. 85 граф G имеет вершину v, степень которой не больше пяти. Удалим v и все ребра, инцидентные v. Полученный граф $G' = G \backslash v$ тоже плоский и имеет $n-1$ вершин. Согласно предположению индукции его можно раскрасить шестью цветами. Так как v имеет в G не более пяти соседей, эти соседи окрашены в G' не более чем пятью цветами. Поэтому любую 6-раскраску[2] G' можно продолжить до 6-раскраски G, приписав вершине v цвет, не использованный для ее соседей при раскраске G'. Таким образом, граф G можно раскрасить шестью красками.

Далее рассмотрим для плоских графов списочное хроматическое число, обсуждавшееся в главе о задаче Диница. Ясно, что наш метод 6-раскраски применим также для списков цветов (нам опять всегда хватит цветов), так что неравенство $\chi_\ell(G) \le 6$ справедливо для любого плоского графа G. Эрдёш, Рубин и Тейлор в 1979 году [2] предположили, что списочное хроматическое число каждого плоского графа не больше 5, и что, кроме того, существуют плоские графы G, для которых $\chi_\ell(G) > 4$. Они были правы в обоих случаях. Маргит Войгт [7] первая построила пример плоского графа G с $\chi_\ell(G) = 5$ (ее пример имел 238 вершин) и почти одновременно Карстен Томассен [6] дал действительно ошеломляющее доказательство гипотезы Эрдёша, Рубина и Тейлора. Его доказательство — впечатляющий пример того, что можно сделать, если найти правильное предположение индукции. Оно вообще не использует формулу Эйлера!

Теорема. *Списочное хроматическое число каждого плоского графа G не больше 5:*

$$\chi_\ell(G) \le 5.$$

■ **Доказательство.** Вначале заметим, что добавление ребер не может уменьшить хроматическое число. Другими словами, если H — подграф графа G, то обязательно $\chi_\ell(H) \le \chi_\ell(G)$. Поэтому можно предполагать, что плоский граф G связен и что все его конечные грани являются треугольниками. Назовем такие графы *почти триангулированными*. Из справедливости теоремы для почти триангулированных плоских графов следует, что она верна для всех плоских графов.

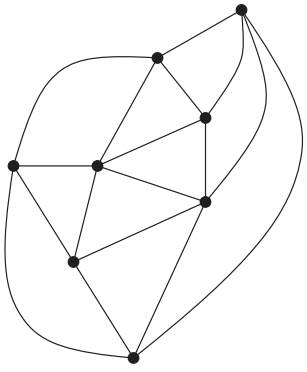
Идея доказательства состоит в том, чтобы вывести теорему из более сильного утверждения (которое можно доказать методом индукции).

Пусть $G = (V, E)$ — почти триангулированный граф и B — цикл, ограничивающий внешнюю область. Пусть множества цветов $C(v)$, $v \in V$, удовлетворяют следующим условиям:

(1) *Две смежные вершины x, y цикла B уже окрашены в (разные) цвета α и β.*

(2) *$|C(v)| \ge 3$ для всех других вершин v на B.*

(3) *$|C(v)| \ge 5$ для всех внутренних вершин.*

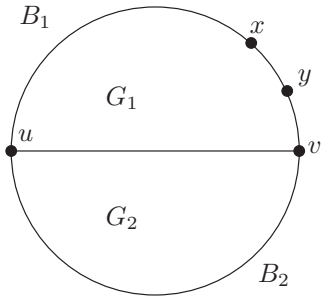


Почти триангулированный граф

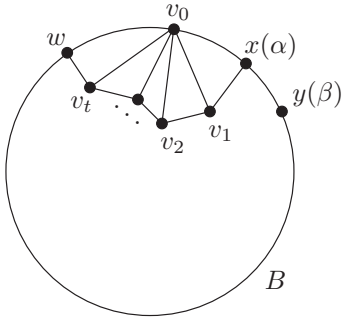
[2] Т. е. раскраску шестью цветами. — *Прим. перев.*

Тогда раскраску x, y можно продолжить до правильной раскраски графа G, выбирая цвета из списков. В частности, $\chi_\ell(G) \le 5$.

Для $|V| = 3$ это очевидно, так как для единственной не окрашенной вершины v по условию $|C(v)| \ge 3$, так что имеется не использованный цвет. Далее воспользуемся индукцией.



Случай 1: Допустим, что B имеет хорду, т. е. ребро, не лежащее на цикле B, которое соединяет вершины $u, v \in B$ и разбивает его на части B_1 и B_2, $x, y \in B_1$. Подграф G_1, ограниченный циклом $B_1 \cup \{uv\}$, содержит x, y, u и v и является почти триангулированным. В силу предположения индукции G_1 можно раскрасить, выбирая цвета из списков $C(v)$, $v \in G_1$. Допустим, что при этой раскраске вершины u и v получили цвета γ и δ. Рассмотрим теперь второй подграф G_2 с границей $B_2 \cup \{u, v\}$. Рассматривая u, v как уже раскрашенные, мы находим, что для G_2 предположение индукции тоже выполняется. Поэтому G_2 можно раскрасить, выбирая цвета из списков $C(v)$, $v \in G_2$. Значит, G можно раскрасить, выбирая цвета из списков $C(v)$.



Случай 2: Допустим, что цикл B не имеет хорд. Пусть v_0 — вершина цикла B, отличная от y и смежная с окрашенной в цвет α вершиной x, и пусть $x, v_1, \ldots, v_t, w$ — все соседи v_0. Так как граф G почти триангулирован, мы имеем ситуацию, показанную на чертеже.

Построим почти триангулированный граф $G' = G \backslash v_0$, удалив из G вершину v_0 и все ребра, исходящие из v_0. Этот граф G' имеет в качестве внешней границы $B' = (B \backslash v_0) \cup \{v_1, \ldots, v_t\}$. Согласно условию (2) имеем $|C(v_0)| \ge 3$, так что в $C(v_0)$ существуют два цвета γ, δ, отличные от α. Построим списки цветов для вершин графа G', заменяя каждое из множеств цветов $C(v_i)$ на $C(v_i) \backslash \{\gamma, \delta\}$ и не изменяя множества цветов для всех остальных вершин. Тогда граф G' будет удовлетворять всем условиям и поэтому в силу индукции его можно правильно раскрасить. Выбрав для v_0 цвет γ или δ, отличный от цвета w, мы продолжим эту раскраску с графа G' на весь граф G. □

Итак, теорема о списочном хроматическом числе доказана, но история на этом не кончается. Более сильная гипотеза утверждает, что списочное хроматическое число плоского графа G не более чем на единицу превышает обычное хроматическое число:

Верно ли, что $\chi_\ell(G) \le \chi(G) + 1$ для каждого плоского графа G ?

Поскольку согласно теореме о четырех красках $\chi(G) \le 4$, существуют три возможности:

Случай I: $\chi(G) = 2 \implies \chi_\ell(G) \le 3$.

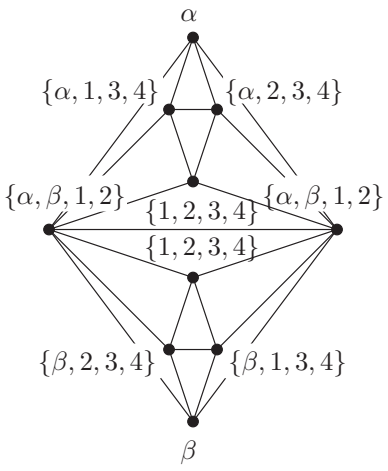
Случай II: $\chi(G) = 3 \implies \chi_\ell(G) \le 4$.

Случай III: $\chi(G) = 4 \implies \chi_\ell(G) \le 5$.

Результат Томассена обосновал случай III, а случай I был доказан с помощью остроумного (и значительно более сложного) рассуждения Алоном и Тарси [1]. Более того, существуют плоские графы G, для которых $\chi(G) = 2$ и $\chi_\ell(G) = 3$, например, граф $K_{2,4}$ из главы о задаче Диница.

А что известно о случае II? Здесь гипотеза не подтвердилась: это впервые продемонстрировала Маргит Войгт для графа, который ранее построил Шай Гутнер. Его граф, имеющий 130 вершин, получается следующим образом. Вначале возьмем «двойной октаэдр» (см.

рисунок на полях), который, понятно, раскрашивается тремя красками. Положим $\alpha \in \{5,6,7,8\}$ и $\beta \in \{9,10,11,12\}$ и рассмотрим списки цветов, указанные на рисунке. Проверьте самостоятельно, что для них списочной раскраски не существует. Затем возьмем 16 экземпляров этого графа и отождествим у них все верхние и нижние вершины. Это даст граф с $16 \cdot 8 + 2 = 130$ вершинами, который тоже является плоским и 3-раскрашиваемым. Припишем цвета $\{5,6,7,8\}$ верхней и цвета $\{9,10,11,12\}$ нижней вершинам, а внутренним вершинам 16 графов — списки, соответствующие 16 парам (α,β), $\alpha \in \{5,6,7,8\}$, $\beta \in \{9,10,11,12\}$. При любом выборе цветов верхней и нижней вершин один из подграфов будет иметь вид, указанный на рисунке, и поэтому списочная раскраска большого графа невозможна.



Модифицировав другой пример Гутнера, Войгт и Вирт [8] построили даже меньший плоский граф с 75 вершинами и $\chi = 3$, $\chi_\ell = 5$, для которого, кроме того, число 5-цветных списков минимально. Последний рекорд — граф с 63 вершинами.

Литература

[1] Alon N., Tarsi M. *Colorings and orientations of graphs.* Combinatorica, **12** (1992), 125–134.

[2] Erdős P., Rubin A. L., Taylor H. *Choosability in graphs.* Proc. West Coast Conference on Combinatorics, Graph Theory and Computing, Congressus Numerantium, **26** (1979), 125–157.

[3] Gonthier G. *Formal proof — the Four-Color Theorem.* Notices of the AMS, **55**(11) (2008), 1382–1393.

[4] Gutner S. *The complexity of planar graph choosability.* Discrete Math., **159** (1996), 119–130.

[5] Robertson N., Sanders D. P., Seymour P., Thomas R. *The four-colour theorem.* J. Combinatorial Theory, Ser. B, **70** (1997), 2–44.

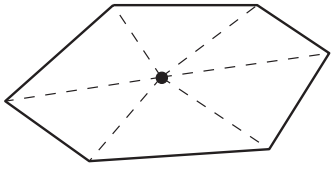
[6] Thomassen C. *Every planar graph is* 5*-choosable.* J. Combinatorial Theory, Ser. B, **62** (1994), 180–181.

[7] Voigt M. *List colorings of planar graphs.* Discrete Math., **120** (1993), 215–219.

[8] Voigt M., Wirth B. *On* 3*-colorable non-*4*-choosable planar graphs.* J. Graph Theory, **24** (1997), 233–235.

[9*] Емеличев В. А., Мельников О. И., Сарванов В. И., Тышкевич Р. И. *Лекции по теории графов.* М., Наука, 1990.

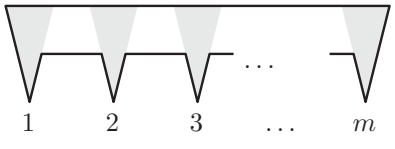
Глава 35 Как охранять музей



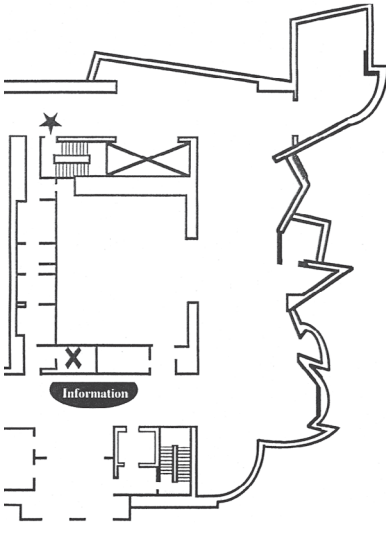
Выпуклый выставочный зал

Следующую занятную задачу поставил в 1973 г. Виктор Кли. Предположим, что директор музея хочет, чтобы каждая точка музея постоянно наблюдалась охранником. Охранники располагаются в стационарных пунктах, но могут поворачиваться. Сколько охранников необходимо иметь?

Представим себе стены музея в виде многоугольника с n сторонами. Конечно, если многоугольник выпуклый, то достаточно иметь одного охранника, и его можно разместить в любой точке музея. Но в общем случае стены музея могут иметь форму любого замкнутого многоугольника.



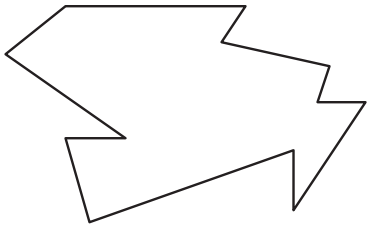
Рассмотрим представленный на полях музей с $n = 3m$ стенами, который имеет вид пилы. Легко видеть, что здесь требуется по меньшей мере $m = \frac{n}{3}$ охранников. Действительно, имеется n стен. Теперь заметим, что точку 1 может наблюдать охранник, располагающийся в затемненном треугольнике, и то же замечание относится к точкам $2, 3, \ldots, m$. Так как эти треугольники не пересекаются, то нужно иметь не менее m охранников. Отсекая одну или две стены в конце, мы заключаем, что для любого n имеется музей с n стенами, для охраны которого требуется $\lfloor \frac{n}{3} \rfloor$ охранников.



Реальная схема художественной галереи...

Следующее предложение утверждает, что этот случай является наихудшим.

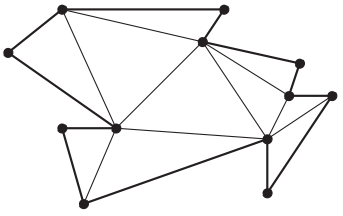
Теорема. *Для любого музея с n стенами достаточно иметь $\lfloor \frac{n}{3} \rfloor$ охранников.*



Музей с $n = 12$ стенами

Впервые эту «теорему о художественной галерее» доказал Вашек Чватал [1], использовавший тонкие рассуждения. Но здесь приведено поистине красивое доказательство, принадлежащее Стиву Фиску [2].

■ **Доказательство.** Прежде всего проведем $n - 3$ непересекающихся диагоналей, соединяющих углы стен, пока внутренность музея не будет триангулирована. Например, в музее, изображенном на полях, мы можем провести 9 диагоналей, чтобы выполнить триангуляцию. Не существенно, какую триангуляцию мы выбрали: любая из них годится. Теперь представим себе новую фигуру как плоский граф, углы стен — как вершины, а стены и диагонали — как ребра.



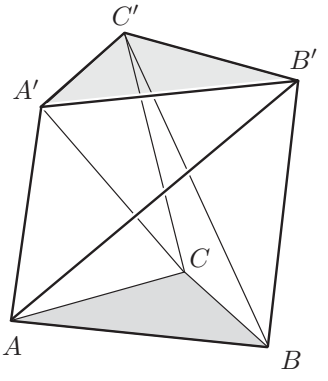
Триангуляция музея

Утверждение. *Этот граф является 3-раскрашиваемым.*

Для $n = 3$ доказывать нечего. Далее воспользуемся индукцией и для $n > 3$ выберем любые две вершины u и v, связанные диагональю. Эта диагональ разбивает граф на два меньших триангулированных графа, каждый из которых содержит ребро uv. В силу предположения индукции можно каждую часть раскрасить в три цвета, и в обеих раскрасках выбрать цвет 1 для u и цвет 2 для v. Склеивая раскраски вместе, получаем 3-раскраску всего графа.

Остальное просто. Так как имеется n вершин, то по крайней мере один цветовой класс (например, вершины, раскрашенные в цвет 1) содержит не более $\lfloor \frac{n}{3} \rfloor$ вершин, и в них мы поместим охранников. Учитывая, что каждый треугольник имеет вершину, раскрашенную в цвет 1, мы приходим к заключению, что каждый треугольник охраняется и, следовательно, то же верно для всего музея. □

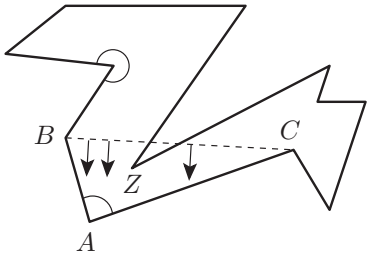
Вдумчивый читатель мог заметить одно тонкое место в нашем рассуждении. Всегда ли существует триангуляция? Вероятно, первая реакция каждого есть: «Очевидно, да!». Действительно, она существует, но это не совсем очевидно, и естественное обобщение на три измерения (разбиение на тетраэдры) на самом деле не верно! Это можно увидеть, рассматривая *многогранник Шенхардта*, изображенный на полях. Он получается из трехгранной призмы вращением верхнего треугольника в его плоскости так, что каждая четырехугольная грань разбивается на два треугольника, образующих вогнутый участок границы многогранника. Попробуйте разбить этот многогранник на тетраэдры! Вы заметите, что любой тетраэдр, который содержит нижний треугольник, должен содержать также одну из трех верхних вершин. Но такой тетраэдр не будет содержаться в многограннике Шенхардта. Поэтому не существует разбиения без дополнительной вершины.



Многогранник Шенхардта: внутренние двугранные углы при ребрах AB', BC' и CA' больше 180°.

Для доказательства того, что триангуляция плоского невыпуклого многоугольника существует, используем индукцию по числу вершин n. Для $n = 3$ многоугольник является треугольником, и доказывать нечего. Пусть $n \geq 4$. Чтобы воспользоваться предположением индукции,

нам достаточно провести *одну* диагональ, которая разобьет многоугольник P на две меньшие части так, что триангуляция многоугольника получится объединением триангуляций частей.

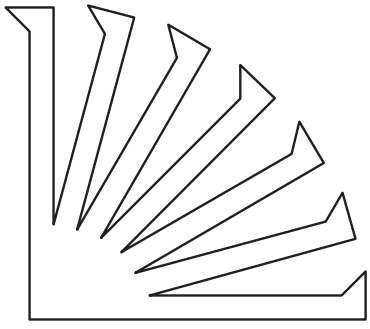


Назовем вершину A *выпуклой*, если внутренний угол при этой вершине меньше $180°$. Так как сумма внутренних углов P равна $(n-2)180°$, то выпуклая вершина A должна существовать. Более того, должны существовать по крайней мере три таких вершины. По существу это следует из принципа Дирихле. Или можно рассмотреть выпуклую оболочку многоугольника и заметить, что все ее вершины являются выпуклыми также и для исходного многоугольника P.

Теперь рассмотрим две соседние с A вершины B и C. Если отрезок BC целиком лежит в P, то он является искомой диагональю. В противном случае треугольник ABC содержит другие вершины многоугольника P. Будем параллельно перемещать отрезок BC в направлении к вершине A до тех пор, пока на нем не окажется последняя лежащая в ABC вершина многоугольника P. Отрезок AZ целиком лежит внутри P и является искомой диагональю.

Существует много вариантов теоремы о художественной галерее. Например, можно охранять только те стены, на которых висят картины, или размещать всю охрану в вершинах. Очень изящный (нерешенный) вариант формулируется следующим образом.

> *Пусть каждый охранник может патрулировать одну стену музея и, перемещаясь вдоль своей стены, он видит все, что можно рассмотреть хотя бы из одной точки этой стены. Сколько «стенных охранников» необходимо для охраны любого музея с n стенами?*



Готфрид Туссан построил пример изображенного на полях музея, который показывает, что может потребоваться $\lfloor \frac{n}{4} \rfloor$ охранников.

Этот многоугольник имеет 28 сторон (в общем случае $4m$ сторон), и читателю предлагается проверить, что необходимо иметь m стенных охранников. Предполагается, что (за исключением некоторых малых значений n) это число также и достаточно, но доказательства, не говоря уже о доказательстве из Книги, еще не найдено.

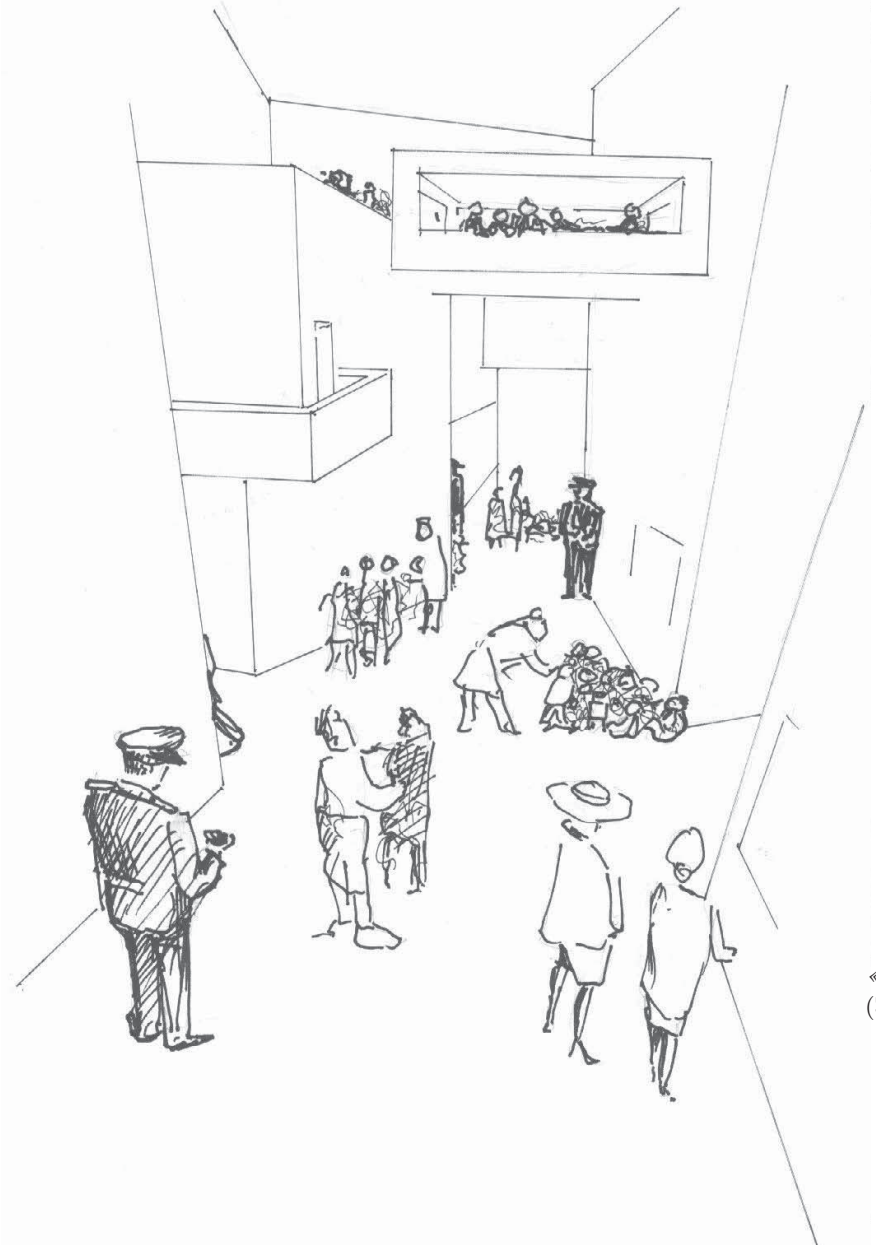
Литература

[1] Chvátal V. *A combinatorial theorem in plane geometry.* J. Combinatorial Theory, Ser. B, **18** (1975), 39–41.

[2] Fisk S. *A short proof of Chvátal's watchman theorem.* J. Combinatorial Theory, Ser. B, **24** (1978), 374.

[3] O'Rourke J. *Art Gallery Theorems and Algorithms.* Oxford University Press, 1987.

[4] Schönhardt E. *Über die Zerlegung von Dreieckspolyedern in Tetraeder.* Math. Annalen, **98** (1928), 309–312.



«Музейные охранники»
(Задача о трехмерной галерее)

Глава 36 Теорема Турана о графах

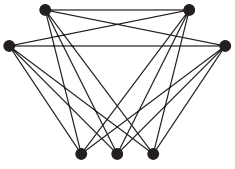
Пауль Туран

Одним из фундаментальных результатов теории графов является теорема Турана 1941-го года, которая положила начало теории экстремальных графов. Теорема Турана переоткрывалась много раз и имеет различные доказательства. Мы обсудим пять доказательств; пусть читатель решает, которое из них достойно Книги.

Введем несколько обозначений. Рассмотрим простой граф G с множеством вершин $V = \{v_1, \ldots, v_n\}$ и множеством ребер E. Если v_i и v_j — соседи, то будем писать $v_iv_j \in E$. Полный граф с p вершинами обозначается K_p. Подграф графа G, совпадающий с K_p, называется *p-кликой* в графе G .

Пауль Туран поставил следующую задачу.

> *Пусть G — простой граф, не содержащий p-клик. Какое наибольшее число ребер может иметь G?*


Граф $K_{2,2,3}$

Легко построить примеры простых графов без p-клик, разбивая V на $p-1$ попарно не пересекающихся подмножеств $V = V_1 \cup \ldots \cup V_{p-1}$, $|V_i| = n_i$, $n = n_1 + \ldots + n_{p-1}$, и соединяя две вершины ребром тогда и только тогда, когда они принадлежат различным множествам V_i, V_j. Обозначим полученный граф $K_{n_1,\ldots,n_{p-1}}$; он имеет $\sum_{i<j} n_in_j$ ребер. Среди всех таких графов с данным n максимальное число ребер имеет граф, у которого числа n_i максимально близки, т. е. $|n_i - n_j| \le 1$ для всех i, j. Действительно, если $n_1 \ge n_2 + 2$, то, переместив одну вершину из V_1 в V_2, мы получим граф, имеющий на $(n_1-1)(n_2+1)-n_1n_2 = n_1-n_2-1 \ge 1$ ребер больше, чем в $K_{n_1,n_2,\ldots,n_{p-1}}$. Графы, для которых $|n_i - n_j| \le 1$, назовем *графами Турана.*

Если $p-1$ делит (нацело) n, то мы можем положить $n_i = \frac{n}{p-1}$ для всех i; граф с такими n_i имеет

$$\binom{p-1}{2}\Big(\frac{n}{p-1}\Big)^2 \;=\; \Big(1-\frac{1}{p-1}\Big)\frac{n^2}{2}$$

ребер. Теорема Турана утверждает, что это число — оценка сверху для числа ребер *произвольного* графа с n вершинами, не имеющего p-клик.

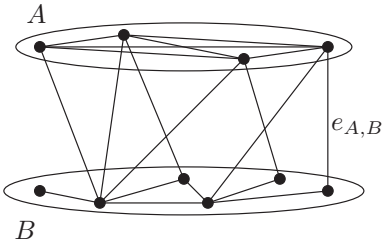
Теорема. *Если граф $G = (V, E)$ с n вершинами не имеет p-клик, $p \ge 2$, то*

$$|E| \;\le\; \Big(1-\frac{1}{p-1}\Big)\frac{n^2}{2}\,. \tag{1}$$

Для $p = 2$ это утверждение тривиально. В первом интересном случае $p = 3$ теорема утверждает, что граф с n вершинами, не имеющий треугольников, содержит не более $\frac{n^2}{4}$ ребер. Доказательства в этом частном случае были известны до Турана. Два изящных доказательства, использующие неравенства, приведены в гл. 18.

Перейдем к общему случаю. Два первых доказательства используют индукцию и принадлежат Турану и Эрдёшу, соответственно.

■ **Первое доказательство.** Воспользуемся индукцией по n. При $n < p$ неравенство (1) легко проверяется. Пусть G — граф с множеством вершин $V = \{v_1, \ldots, v_n\}$ без p-клик, имеющий максимальное число ребер, и $n \geq p$. Конечно, G имеет $(p-1)$-клики, так как в противном случае можно было бы добавить ребра. Пусть A — одна из $(p-1)$-клик; положим $B := V \backslash A$. Клика A имеет $\binom{p-1}{2}$ ребер; оценим число e_B ребер в B и число $e_{A,B}$ ребер между A и B. По предположению индукции $e_B \leq \frac{1}{2}\,(1 - \frac{1}{p-1})(n-p+1)^2$. Так как G не имеет p-клик, то каждая вершина $v_j \in B$ смежна не более чем с $p-2$ вершинами из A; значит, $e_{A,B} \leq (p-2)(n-p+1)$. Поэтому

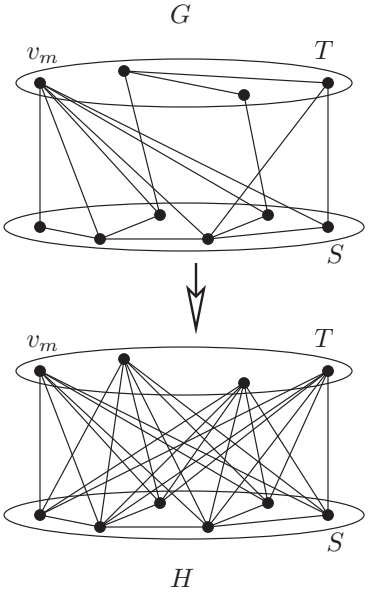


$$|E| \leq \binom{p-1}{2} + \frac{1}{2}\Big(1 - \frac{1}{p-1}\Big)(n-p+1)^2 + (p-2)(n-p+1)\,.$$

Правая часть этого неравенства в точности равна $(1 - \frac{1}{p-1})\frac{n^2}{2}$. □

■ **Второе доказательство.** Это доказательство использует структуру графов Турана и индукцию по числу вершин n. При $n < p$ теорема верна. Допустим, что теорема верна, если число вершин графа меньше n, и G — граф с множеством вершин $V = \{v_1, \ldots, v_n\}$. Пусть d_j — степень вершины v_j, а $v_m \in V$ — вершина максимальной степени $d_m = \max_{1 \leq j \leq n} d_j$. Множество соседей v_m обозначим S, $|S| = d_m$, и положим $T := V \backslash S$. Так как G не имеет p-клик и v_m смежна всем вершинам из S, то S не может содержать $(p-1)$-клик.

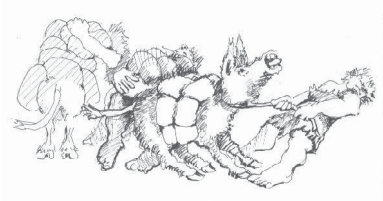
Построим теперь новый граф H с множеством вершин V (см. рисунок). Граф H совпадает с G на множестве S; множество его ребер $E(H)$ содержит все ребра, соединяющие S и T, и не содержит ребер, соединяющих вершины из T. Поэтому T — независимое множество в H, и мы приходим к выводу, что H тоже не имеет p-клик. Пусть d'_j — степень v_j в H. Если $v_j \in S$, то $d'_j \geq d_j$ по построению H, а если $v_j \in T$, то $d'_j = |S| = d_m \geq d_j$ вследствие выбора v_m. Значит, $|E(H)| \geq |E|$, т. е. среди графов на V с максимальным числом ребер должен быть граф вида H. В силу предположения индукции подграф графа G с множеством вершин S имеет не больше ребер, чем некоторый граф $K_{n_1,\ldots,n_{p-2}}$ на множестве S. Поэтому $|E| \leq |E(H)| \leq E(K_{n_1,\ldots,n_{p-1}})$, где $n_{p-1} = |T|$. Отсюда следует (1). □



Следующие два совершенно разные доказательства используют сведение к экстремальным задачам и идеи из теории вероятностей. Одно из них принадлежит Моцкину и Штраусу [4], другое — Алону и Спенсеру [2].

■ **Третье доказательство.** Рассмотрим *вероятностное распределение* $\boldsymbol{w} = (w_1, \ldots, w_n)$ на вершинах, т. е. сопоставим вершинам значения (веса) $w_i \geq 0$, $\sum_{i=1}^{n} w_i = 1$. Найдем максимальное значение функции

$$f(\boldsymbol{w}) \;=\; \sum_{v_i v_j \in E} w_i w_j.$$



«Перемещение весов»

Предположим, что $\boldsymbol{w}$ — произвольное распределение, v_i, v_j — пара не смежных вершин с положительными весами w_i, w_j. Пусть s_i — сумма весов всех вершин, смежных с v_i, и аналогично для v_j определена сумма s_j. Можно считать, что $s_i \ge s_j$. Теперь переместим вес из v_j в v_i, т. е. новый вес v_i будет $w_i + w_j$, а вес v_j уменьшается до 0. Для нового распределения $\boldsymbol{w}'$

$$f(\boldsymbol{w}') \;=\; f(\boldsymbol{w}) + w_j s_i - w_j s_j \;\ge\; f(\boldsymbol{w}).$$

Будем повторять такие операции (сокращая на каждом шаге число вершин с положительным весом на единицу) до тех пор, пока не останется несмежных вершин с положительными весами. Таким образом, при оптимальном распределении ненулевые веса сосредоточиваются на некоторой клике, например на k-клике. Если теперь, скажем, $w_1 > w_2 > 0$, то выберем такое ε, что $0 < \varepsilon < w_1 - w_2$, и заменим w_1 на $w_1 - \varepsilon$, а w_2 на $w_2 + \varepsilon$. Для нового распределения $\boldsymbol{w}'$ выполняется неравенство $f(\boldsymbol{w}') = f(\boldsymbol{w}) + \varepsilon(w_1 - w_2) - \varepsilon^2 > f(\boldsymbol{w})$; значит, в множестве распределений, сосредоточенных на k-кликах, максимальное значение f достигается, если $w_i = \frac{1}{k}$ для вершин клики и $w_i = 0$ для других вершин. Так как k-клика имеет $\frac{k(k-1)}{2}$ ребер, то

$$f(\boldsymbol{w}) \;=\; \frac{k(k-1)}{2}\frac{1}{k^2} \;=\; \frac{1}{2}\Big(1 - \frac{1}{k}\Big).$$

Это выражение возрастает при росте k, поэтому оно максимально при $k = p - 1$ (так как G не имеет p-клик). Таким образом, мы получаем, что для *любого* распределения $\boldsymbol{w}$ на графе без p-клик

$$f(\boldsymbol{w}) \;\le\; \frac{1}{2}\Big(1 - \frac{1}{p-1}\Big).$$

В частности, это неравенство справедливо для *равновероятного* распределения, когда $w_i = \frac{1}{n}$ при всех i. Значит,

$$\frac{|E|}{n^2} \;=\; f\Big(\Big(\frac{1}{n}, \ldots, \frac{1}{n}\Big)\Big) \;\le\; \frac{1}{2}\Big(1 - \frac{1}{p-1}\Big),$$

что есть в точности (1). □

■ **Четвертое доказательство.** На этот раз воспользуемся некоторыми понятиями из теории вероятностей. Пусть G — произвольный граф с множеством вершин $V = \{v_1, \ldots, v_n\}$. Обозначим степень вершины v_i через d_i, а число вершин в наибольшей клике (оно называется *кликовым числом* графа G) обозначим $\omega(G)$.

Утверждение. *Справедливо неравенство* $\omega(G) \ge \sum_{i=1}^{n} \frac{1}{n - d_i}$.

Пусть $\pi = (\pi(1), \pi(2), \ldots, \pi(n))$ — случайная перестановка, имеющая равномерное распределение на совокупности всех $n!$ перестановок множества $\{1, \ldots, n\}$. Построим по π множество $C_\pi \subseteq V$, включая $v_{\pi(i)}$ в C_π

тогда и только тогда, когда $v_{\pi(i)}$ смежна всем $v_{\pi(j)}$ $(j < i)$. По построению C_π — клика в G. Пусть $X = |C_\pi|$ — соответствующая случайная величина. Тогда $X = \sum_{i=1}^{n} X_i$, где X_i — индикаторная случайная величина, соответствующая вершине $v_{\pi(i)}$, т. е. $X_i = 1$ при $v_{\pi(i)} \in C_\pi$ и $X_i = 0$ при $v_{\pi(i)} \notin C_\pi$. Заметим, что $v_{\pi(i)}$ находится в множестве C_π, построенном по перестановке π, тогда и только тогда, когда $v_{\pi(i)}$ появляется в перестановке *раньше* $n - 1 - d_{\pi(i)}$ вершин, не смежных с $v_{\pi(i)}$, другими словами, если $v_{\pi(i)}$ появляется *первой* из множества, состоящего из $v_{\pi(i)}$ и $n - 1 - d_{\pi(i)}$ вершин, не смежных с $v_{\pi(i)}$. Вероятность этого события равна $\frac{1}{n-d_{\pi(i)}}$, так что $EX_i = \frac{1}{n-d_{\pi(i)}}$.

Поэтому в силу линейности математического ожидания (см. приложение к гл. 15 на с. 103) мы получаем

$$E(|C_\pi|) \;=\; EX \;=\; \sum_{i=1}^{n} EX_i \;=\; \sum_{i=1}^{n} \frac{1}{n - d_{\pi(i)}} = \sum_{i=1}^{n} \frac{1}{n - d_i}\,.$$

Отсюда следует, что должна быть клика по меньшей мере такого размера, а в этом и состоит наше утверждение.

Чтобы получить из утверждения теорему Турана, воспользуемся неравенством Коши – Буняковского – Шварца из гл. 18:

$$\Big(\sum_{i=1}^{n} a_i b_i\Big)^2 \;\le\; \Big(\sum_{i=1}^{n} a_i^2\Big)\Big(\sum_{n=1}^{n} b_i^2\Big).$$

Положим $a_i = \sqrt{n - d_i}$, $b_i = \frac{1}{\sqrt{n-d_i}}$. Тогда $a_i b_i = 1$, и поэтому

$$n^2 \;\le\; \Big(\sum_{i=1}^{n}(n - d_i)\Big)\Big(\sum_{i=1}^{n} \frac{1}{n - d_i}\Big) \;\le\; \omega(G)\sum_{i=1}^{n}(n - d_i). \qquad (2)$$

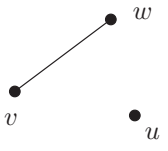
Теперь воспользуемся условием теоремы Турана, согласно которому $\omega(G) \le p - 1$. Учитывая также равенство $\sum_{i=1}^{n} d_i = 2|E|$ из гл. 25 о двойном счете, приведем неравенство (2) к виду

$$n^2 \;\le\; (p - 1)(n^2 - 2|E|),$$

который эквивалентен неравенству Турана. □

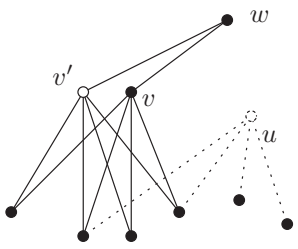
Наконец, перейдем к последнему доказательству, которое, возможно, красивее остальных. Его происхождение не ясно; нам его сообщил Стефан Брандт, а он услышал доказательство в Обервольфахе. Видимо, оно является «фольклором» теории графов. Из него в одну строку следует, что граф Турана является единственным примером графа с максимальным числом ребер. Заметим, что из первого и второго доказательств также вытекает это более сильное утверждение.

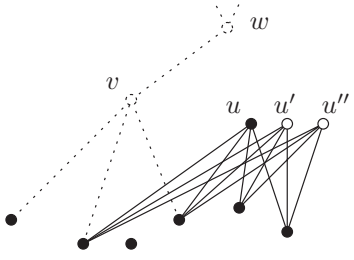
■ **Пятое доказательство.** Пусть G — граф с n вершинами без p-клик, имеющий максимальное число ребер.



Утверждение. *Граф G не имеет таких вершин u, v, w, что $vw \in E$, но $uv \notin E$ и $uw \notin E$.*

Предположим обратное и рассмотрим следующие два случая (далее степень вершины u обозначается $d(u)$. — *Прим. ред.*).





Случай 1: $d(u) < d(v)$ или $d(u) < d(w)$.
Для определенности предположим, что $d(u) < d(v)$. Продублируем v, т. е. введем новую вершину v', которая имеет точно тех же соседей, что и v (но vv' ребром не является), удалим (вместе с $d(u)$ инцидентными ей ребрами) u, а остальные ребра и вершины сохраним без изменений.

Новый граф G' тоже не имеет p-клик, а число его ребер есть

$$|E(G')| \;=\; |E(G)| + d(v) - d(u) \;>\; |E(G)|,$$

но это противоречит тому, что G имеет максимальное число ребер.

Случай 2: $d(u) \geq d(v)$ и $d(u) \geq d(w)$.
Аналогично предыдущему дважды продублируем u и удалим v и w, как показано на полях. Новый граф G', как и прежде, не имеет p-клик, и мы получаем

$$|E(G')| \;=\; |E(G)| + 2d(u) - (d(v) + d(w) - 1) \;>\; |E(G)|,$$

где -1 появляется потому, что ребро vw учитывается как в $d(v)$, так и в $d(w)$. Следовательно, мы опять приходим к противоречию.

Как нетрудно проверить, доказанное утверждение означает, что для графов без p-клик, имеющих максимальное число ребер, формула

$$u \sim v \iff uv \notin E(G)$$

определяет отношение эквивалентности (все ребра в G соединяют только вершины из разных классов эквивалентности. — *Прим. ред.*). Значит, G является полным многодольным графом: $G = K_{n_1,\ldots,n_{p-1}}$, и доказательство закончено. □

Литература

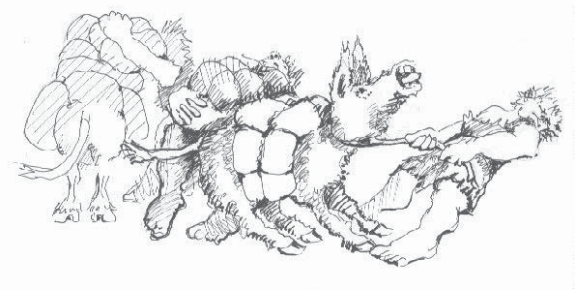
[1] Aigner M. *Turán's graph theorem.* Amer. Math. Monthly, **102** (1995), 808–816.

[2] Alon N., Spencer J. *The Probabilistic Method.* Wiley Interscience, 1992. [Имеется русский перевод 2-го английского издания 2000 г.: Алон Н., Спенсер Дж. *Вероятностный метод.* М., Бином, 2011.]

[3] Erdős P. *On the graph theorem of Turán.* Math. Fiz. Lapok, **21** (1970), 249–251 (на венгерском языке).

[4] Motzkin T. S., Straus E. G. *Maxima for graphs and a new proof of a theorem of Turán.* Canad. J. Math., **17** (1965), 533–540.

[5] Turán P. *On an extremal problem in graph theory.* Math. Fiz. Lapok, **48** (1941), 436–452.



«Перемещение больших весов»

Связь без ошибок

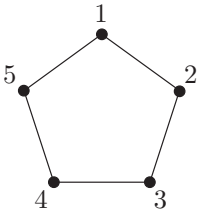
Глава 37

В 1956 году основоположник теории информации Клод Шеннон поставил следующий очень интересный вопрос:

> *Предположим, что мы хотим передать сообщение адресату по каналу связи, в котором возможны искажения символов. Какова максимальная скорость передачи, при которой адресат может без ошибок восстановить первоначальное сообщение?*

Клод Шеннон

Рассмотрим, как именно Шеннон понимал термины «канал связи» и «скорость передачи». Пусть задано множество символов V (алфавит); сообщение есть последовательность символов из V. В качестве модели канала связи выберем граф $G = (V, E)$, где V — множество символов, а E — множество ребер, соединяющих пары близких символов, т. е. символов, которые могут переходить друг в друга при передаче сообщения. Например, в модели обычного разговора по телефону мы свяжем ребром символы Б и П, поскольку адресат может их перепутать. Будем говорить, что G — *граф помех*.



Важную роль в наших рассуждениях будет играть цикл длины 5 (5-цикл) C_5. В этом примере адресат может перепутать 1 и 2, но не 1 и 3, и т. д. В идеале хотелось бы использовать при передаче все 5 символов, но так как мы хотим, чтобы сообщение передавалось без ошибок, то — при передаче отдельных символов — следует использовать не более одного знака из каждой пары знаков, которые можно перепутать. Поэтому в случае 5-цикла можно пользоваться только двумя различными символами (любыми двумя, не связанными ребром в C_5). На языке теории информации это означает, что для 5-цикла при этом достигается скорость передачи информации $\log_2 2 = 1$ (вместо максимально возможной $\log_2 5 \approx 2.32$). Ясно, что в модели с произвольным графом помех $G = (V, E)$ лучшее, что можно сделать, — это передавать символы из наибольшего независимого множества M. Тогда скорость передачи информации при передаче отдельных символов будет равна $\log_2 \alpha(G)$, где $\alpha(G) = |M|$ — *число независимости* графа G.

Посмотрим, нельзя ли увеличить скорость передачи информации, используя вместо отдельных символов составленные из них цепочки. Допустим, что мы хотим передавать цепочки длины 2. Цепочки u_1u_2 и v_1v_2 можно перепутать в одном из следующих трех случаев:

- $u_1 = v_1$ и u_2 можно перепутать с v_2,
- $u_2 = v_2$ и u_1 можно перепутать с v_1,
- $u_1 \neq v_1$ можно перепутать и $u_2 \neq v_2$ можно перепутать.

В терминах теории графов это равнозначно рассмотрению *произведения*[1] $G_1 \times G_2$ двух графов $G_1 = (V_1, E_1)$ и $G_2 = (V_2, E_2)$. Граф $G_1 \times G_2$ имеет множество вершин $V_1 \times V_2 = \{(u_1, u_2) : u_1 \in V_1, u_2 \in V_2\}$, и вершины $(u_1, u_2) \neq (v_1, v_2)$ соединяются ребром тогда и только тогда, когда $u_i = v_i$ или $u_i v_i \in E_i$ для каждого $i = 1, 2$. Графом помех для цепочек длины 2 поэтому является $G^2 = G \times G$, т. е. произведение графа помех G для одного символа на себя. Тогда скорость передачи информации цепочками длины 2 *на символ* определяется формулой

$$\frac{\log_2 \alpha(G^2)}{2} \quad = \quad \log_2 \sqrt{\alpha(G^2)}.$$

Конечно, мы можем использовать цепочки любой длины n. Для них n-й граф помех $G^n = G \times G \times \ldots \times G$ имеет множество вершин $V^n = \{(u_1, \ldots, u_n) : u_i \in V\}$, и вершины $(u_1, \ldots, u_n) \neq (v_1, \ldots v_n)$ связываются ребром, если для каждого i либо $u_i = v_i$, либо $u_i v_i \in E$. Скорость передачи информации на один символ для передачи цепочками длины n равна

$$\frac{\log_2 \alpha(G^n)}{n} \quad = \quad \log_2 \sqrt[n]{\alpha(G^n)}.$$

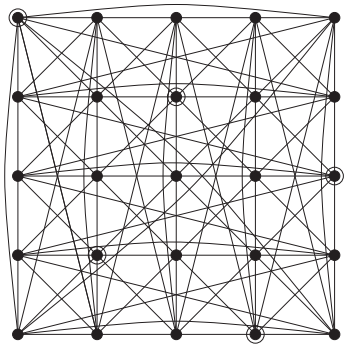
Что можно сказать о числе $\alpha(G^n)$? Вот первое наблюдение. Пусть $U \subseteq V$ — наибольшее независимое множество в G и $|U| = \alpha$. Ясно, что совокупность α^n вершин графа G^n вида $(u_1, \ldots, u_n)$, где $u_i \in U$ для всех i, образует независимое множество в G^n. Следовательно,

$$\alpha(G^n) \geq \alpha(G)^n$$

и поэтому

$$\sqrt[n]{\alpha(G^n)} \geq \alpha(G).$$

Это означает, что мы не уменьшим скорость передачи информции, используя длинные цепочки вместо отдельных символов. В этом, кстати, и состоит основная идея теории кодирования: кодируя сообщения более длинными цепочками, мы можем сделать безошибочную передачу сообщений более эффективной.



Граф $C_5 \times C_5$

Пренебрегая логарифмом, мы приходим к основополагающему определению Шеннона. *Безошибочная пропускная способность*[2] графа G задается соотношением

$$\Theta(G) \ := \ \sup_{n \geq 1} \sqrt[n]{\alpha(G^n)},$$

и задача Шеннона состоит в вычислении $\Theta(G)$, в частности, $\Theta(C_5)$.

Рассмотрим теперь цикл C_5. Мы уже знаем, что $\alpha(C_5) = 2 \leq \Theta(C_5)$. Используя приведенное выше изображение 5-цикла или изображенное на полях произведение $C_5 \times C_5$, легко проверить, что $\{(1,1), (2,3), (3,5), (4,2), (5,4)\}$ — независимое множество вершин в ${C_5}^2$. Поэтому $\alpha({C_5}^2) \geq 5$. Так как независимое множество может содержать

[1] Это определение отличается от определения произведения графов, содержащегося, например, в книге Ф. Харари [5*], с. 36. — *Прим. перев.*

[2] Используется также термин «шенноновская емкость графа» (см. перевод статьи Л. Ловаса [3]). — *Прим. перев.*

не более двух вершин из любых двух соседних строк, то $\alpha({C_5}^2) = 5$. Таким образом, с помощью строк длины 2 мы увеличили нижнюю оценку пропускной способности C_5 до $\Theta(C_5) \geq \sqrt{5}$.

До сих пор у нас не было верхних оценок пропускной способности. Чтобы получить такие оценки, снова воспользуемся исходными идеями Шеннона. Во-первых, нам потребуется двойственное определение независимого множества. Напомним, что подмножество $C \subseteq V$ — *клика*, если любые две вершины C связаны ребром. Таким образом, отдельные вершины образуют тривиальные клики размера 1, ребра являются кликами размера 2, треугольники — кликами размера 3, и т. д. Обозначим через $\mathcal{C}$ множество клик графа G. Рассмотрим произвольное распределение вероятностей $\boldsymbol{x} = (x_v : v \in V)$ на множестве вершин, т. е. $x_v \geq 0$ и $\sum_{v\in V} x_v = 1$. Каждому распределению $\boldsymbol{x}$ сопоставим «максимальную вероятность клик»

$$\lambda(\boldsymbol{x}) \;=\; \max_{C\in\mathcal{C}} \sum_{v\in C} x_v,$$

и, наконец, положим

$$\lambda(G) \;=\; \min_{\boldsymbol{x}} \lambda(\boldsymbol{x}) \;=\; \min_{\boldsymbol{x}} \max_{C\in\mathcal{C}} \sum_{v\in C} x_v.$$

Корректнее было бы вместо min использовать inf, но, поскольку функция $\lambda(\boldsymbol{x})$ непрерывна на компактном множестве всех распределений, минимум существует.

Пусть теперь $U \subseteq V$ — независимое множество максимального размера $\alpha(G) = \alpha$. Свяжем с U распределение $\boldsymbol{x}_U = (x_v : v \in V)$, положив $x_v = \frac{1}{\alpha}$ при $v \in U$ и $x_v = 0$ в противном случае. Так как любая клика содержит не более одной вершины из U, то $\lambda(\boldsymbol{x}_U) = \frac{1}{\alpha}$, и по определению $\lambda(G)$

$$\lambda(G) \leq \frac{1}{\alpha(G)}, \qquad \text{или} \qquad \alpha(G) \leq \lambda(G)^{-1}.$$

Как заметил Шеннон, величина $\lambda(G)^{-1}$ является верхней оценкой для всех $\sqrt[n]{\alpha(G^n)}$ и поэтому также и для $\Theta(G)$. Чтобы доказать это, достаточно показать, что для графов G, H справедливо равенство

$$\lambda(G \times H) \;=\; \lambda(G)\lambda(H), \tag{1}$$

так как из него вытекает соотношение $\lambda(G^n) = \lambda(G)^n$, в силу которого

$$\begin{aligned} \alpha(G^n) &\leq \lambda(G^n)^{-1} = \lambda(G)^{-n}, \\ \sqrt[n]{\alpha(G^n)} &\leq \lambda(G)^{-1}. \end{aligned}$$

Для доказательства (1) воспользуемся теоремой двойственности из линейного программирования (см. [1]):

$$\lambda(G) \;=\; \min_{\boldsymbol{x}} \max_{C\in\mathcal{C}} \sum_{v\in C} x_v \;=\; \max_{\boldsymbol{y}} \min_{v\in V} \sum_{C\ni v} y_C, \tag{2}$$

где максимум в правой части берется по всем вероятностным распределениям $\boldsymbol{y} = (y_C : C \in \mathcal{C})$ на $\mathcal{C}$.

Рассмотрим граф $G \times H$, и пусть $\boldsymbol{x}$ и $\boldsymbol{x}'$ — распределения, на которых достигаются минимумы: $\lambda(\boldsymbol{x}) = \lambda(G)$, $\lambda(\boldsymbol{x}') = \lambda(H)$. Поставим в

соответствие каждой вершине (u,v) графа $G\times H$ значение $z_{(u,v)} = x_u x'_v$. Так как $\sum_{(u,v)} z_{(u,v)} = \sum_u x_u \sum_v x'_v = 1$, то $\{z_{(u,v)}\}$ — распределение. Далее заметим, что максимальные клики в графе $G \times H$ имеют вид $C \times D = \{(u,v) : u \in C,\, v \in D\}$, где C и D — клики в G и H соответственно. Отсюда по определению $\lambda(G \times H)$ находим

$$\begin{aligned}\lambda(G\times H) \;\le\; \lambda(\boldsymbol{z}) \;&=\; \max_{C\times D} \sum_{(u,v)\in C\times D} z_{(u,v)} \\ &=\; \max_{C\times D} \sum_{u\in C} x_u \sum_{v\in D} x'_v \;=\; \lambda(G)\lambda(H).\end{aligned}$$

Тем же способом (с помощью двойственного выражения для $\lambda(G)$ в (2)) доказывается обратное неравенство $\lambda(G \times H) \ge \lambda(G)\lambda(H)$. В итоге мы можем утверждать: для любого графа G

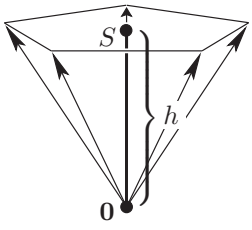
$$\Theta(G) \;\le\; \lambda(G)^{-1}.$$

Применим полученные результаты к 5-циклу и вообще к m-циклу C_m. Используя равномерное распределение $(\frac{1}{m}, \ldots, \frac{1}{m})$ на вершинах, получаем: $\lambda(C_m) \le \frac{2}{m}$, так как каждая клика в C_m содержит не более двух вершин. Аналогично, сопоставляя число $\frac{1}{m}$ ребрам и число 0 вершинам, с помощью двойственного выражения в (2) получаем, что $\lambda(C_m) \ge \frac{2}{m}$. Значит, $\lambda(C_m) = \frac{2}{m}$, и поэтому для всех m

$$\Theta(C_m) \;\le\; \frac{m}{2}.$$

Далее, понятно, что если m четно, то $\alpha(C_m) = \frac{m}{2}$ и поэтому $\Theta(C_m) = \frac{m}{2}$. Если m нечетно, то $\alpha(C_m) = \frac{m-1}{2}$. При $m = 3$ цикл C_3 является кликой, и то же верно для каждой его степени ${C_3}^n$, откуда следует, что $\alpha(C_3) = \Theta(C_3) = 1$. Итак, первый интересный случай — это 5-цикл, о котором мы пока знаем, что

$$\sqrt{5} \;\le\; \Theta(C_5) \;\le\; \frac{5}{2}. \tag{3}$$



«Зонт Ловаса»

Используя линейное программирование (и ряд других идей), Шеннон вычислил пропускную способность многих графов, в частности, всех графов с числом вершин не более пяти, за исключением цикла C_5, для которого он не смог продвинуться дальше оценок (3). Такое положение сохранялось более 20 лет, пока Ласло Ловас с помощью удивительно простого приема не показал, что в действительности $\Theta(C_5) = \sqrt{5}$. Комбинаторная задача, которая казалась очень трудной, получила неожиданное и изящное решение.

Главная новая идея Ловаса состояла в том, чтобы представить вершины графа v действительными векторами длины 1, сопоставляя любым двум не смежным вершинам ортогональные векторы. Будем говорить, что такое множество векторов — *ортонормальное представление* графа G. Такое представление всегда существует: достаточно взять единичные векторы $(1,0,\ldots,0)^T$, $(0,1,0,\ldots,0)^T$, $\ldots$, $(0,0,\ldots,1)^T$ размерности $m = |V|$.

Для графа C_5 можно построить ортонормальное представление в $\mathbb{R}^3$, рассматривая «зонт» с пятью спицами $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_5$ единичной длины.

Теперь будем раскрывать зонт (считая верхушку зонта началом координат $\mathbf{0}$) до тех пор, пока углы между любыми двумя не соседними спицами не станут равными $90°$.

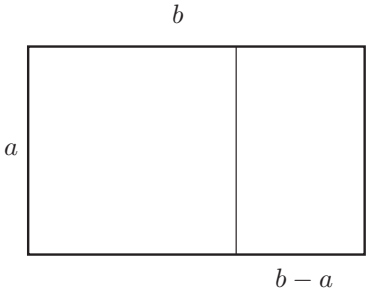
Ловас показал, что высота этого зонта h, т. е. расстояние между $\mathbf{0}$ и S, дает оценку

$$\Theta(C_5) \;\le\; \frac{1}{h^2}. \tag{4}$$

Простое вычисление (см. вставку) показывает, что $h^2 = \frac{1}{\sqrt{5}}$. Отсюда следует, что $\Theta(C_5) \le \sqrt{5}$, и, значит, $\Theta(C_5) = \sqrt{5}$.

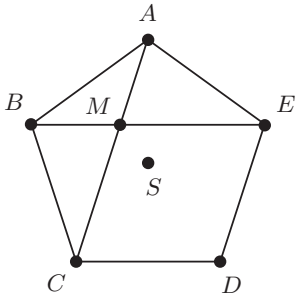
Пятиугольники и золотое сечение

Считается, что форма прямоугольника эстетически оптимальна, если после отсечения от него квадрата остающийся прямоугольник подобен исходному. Длины сторон a, b такого прямоугольника удовлетворяют условию $\frac{b}{a} = \frac{a}{b-a}$. Полагая $\tau := \frac{b}{a}$, получаем $\tau = \frac{1}{\tau-1}$, или $\tau^2 - \tau - 1 = 0$. Решение этого квадратного уравнения дает *золотое сечение* $\tau = \frac{1+\sqrt{5}}{2} \approx 1.6180$.



Рассмотрим теперь правильный пятиугольник со стороной длины a, пусть d — длина его диагоналей. Еще Евклиду было известно (Книга XIII,8), что $\frac{d}{a} = \tau$ и что точка пересечения двух диагоналей делит их в золотом сечении.

Приведем принадлежащее Евклиду и достойное Книги доказательство этого факта. Так как сумма всех углов пятиугольника равна 3π, то углы при его вершинах равны $\frac{3\pi}{5}$. Отсюда следует, что $\sphericalangle ABE = \frac{\pi}{5}$, так как ABE — равнобедренный треугольник. В свою очередь, отсюда вытекает, что $\sphericalangle AMB = \frac{3\pi}{5}$, и, значит, треугольники ABC и AMB подобны. Четырехугольник $CMED$ — ромб, так как его противоположные стороны параллельны, поэтому $|MC| = a$ и, следовательно, $|AM| = d-a$. Используя подобие треугольников ABC и AMB, находим



$$\frac{d}{a} = \frac{|AC|}{|AB|} = \frac{|AB|}{|AM|} = \frac{a}{d-a} = \frac{|MC|}{|MA|} = \tau.$$

Это еще не все. Попробуйте доказать, что $s^2 = \frac{d^2}{\tau+2}$, где s — расстояние от любой вершины пятиугольника до его центра (заметьте, что BS пересекает диагональ AC под прямым углом и делит ее пополам).

В завершение этого экскурса в геометрию рассмотрим зонт, концы спиц которого образуют правильный пятиугольник. Поскольку не являющиеся соседними спицы зонта (длины 1) перпендикулярны, из теоремы Пифагора получаем, что $d = \sqrt{2}$ и поэтому $s^2 = \frac{2}{\tau+2} = \frac{4}{\sqrt{5}+5}$. Далее, снова применяя теорему Пифагора, приходим к искомой формуле для высоты $h = |OS|$:

$$h^2 \;=\; 1 - s^2 \;=\; \frac{1+\sqrt{5}}{\sqrt{5}+5} \;=\; \frac{1}{\sqrt{5}}.$$

Посмотрим, как Ловас доказал неравенство (4). (На самом деле он получил значительно более общий результат.) Пусть

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = x_1 y_1 + \ldots + x_s y_s$$

— обычное скалярное произведение двух векторов $\boldsymbol{x} = (x_1, \ldots, x_s)$, $\boldsymbol{y} = (y_1, \ldots, y_s)$ в $\mathbb{R}^s$. Тогда $|\boldsymbol{x}|^2 = \langle \boldsymbol{x}, \boldsymbol{x} \rangle = x_1^2 + \ldots + x_s^2$ — это квадрат длины $|\boldsymbol{x}|$ вектора $\boldsymbol{x}$, и угол γ между $\boldsymbol{x}$ и $\boldsymbol{y}$ определяется равенством

$$\cos\gamma \;=\; \frac{\langle \boldsymbol{x}, \boldsymbol{y} \rangle}{|\boldsymbol{x}||\boldsymbol{y}|}\,.$$

Следовательно, $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0$ тогда и только тогда, когда $\boldsymbol{x}$ и $\boldsymbol{y}$ ортогональны.

Теперь займемся доказательством верхней оценки «$\Theta(G) \le \sigma_T^{-1}$» для шенноновской пропускной способности любого графа G, имеющего особенно «хорошее» ортонормальное представление. Пусть $T = \{\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(m)}\}$ — ортонормальное представление графа G в $\mathbb{R}^s$, где вектор $\boldsymbol{v}^{(i)}$ соответствует вершине v_i. Предположим, кроме того, что все векторы $\boldsymbol{v}^{(i)}$ образуют *один и тот же* угол ($\neq 90°$) с вектором $\boldsymbol{u} := \frac{1}{m}(\boldsymbol{v}^{(1)} + \ldots + \boldsymbol{v}^{(m)})$, т. е. что скалярное произведение

$$\langle \boldsymbol{v}^{(i)}, \boldsymbol{u} \rangle \;=\; \sigma_{_T}$$

для всех i принимает одно и то же значение $\sigma_{_T} \neq 0$. Назовем это значение $\sigma_{_T}$ *константой* представления T. Для зонта Ловаса, представляющего цикл C_5, условие $\langle \boldsymbol{v}^{(i)}, \boldsymbol{u} \rangle = \sigma_{_T}$, где $\boldsymbol{u} = \vec{OS}$, разумеется, выполняется.

Дальнейшие рассуждения разбиваются на три шага.

(A) Рассмотрим вероятностное распределение $\boldsymbol{x} = (x_1, \ldots, x_m)$ на множестве V; положим

$$\mu(\boldsymbol{x}) \;\;:=\;\; |x_1 \boldsymbol{v}^{(1)} + \ldots + x_m \boldsymbol{v}^{(m)}|^2$$

и

$$\mu_{_T}(G) \;\;:=\;\; \inf_{\boldsymbol{x}} \mu(\boldsymbol{x}).$$

Пусть U — наибольшее независимое множество графа G и $|U| = \alpha$; положим $\boldsymbol{x}_U = (x_1, \ldots, x_m)$, где $x_i = \frac{1}{\alpha}$ при $v_i \in U$ и $x_i = 0$ в противном случае. Так как все векторы $\boldsymbol{v}^{(i)}$ имеют единичную длину и $\langle \boldsymbol{v}^{(i)}, \boldsymbol{v}^{(j)} \rangle = 0$ для любых двух не смежных вершин, то

$$\mu_{_T}(G) \;\le\; \mu(\boldsymbol{x}_U) \;=\; \Big| \sum_{i=1}^{m} x_i \boldsymbol{v}^{(i)} \Big|^2 \;=\; \sum_{i=1}^{m} x_i^2 = \alpha \frac{1}{\alpha^2} = \frac{1}{\alpha}\,.$$

Таким образом, $\mu_{_T}(G) \le \alpha^{-1}$ и поэтому

$$\alpha(G) \;\le\; \frac{1}{\mu_{_T}(G)}\,.$$

(B) Теперь вычислим $\mu_{_T}(G)$. Нам потребуется неравенство Коши – Буняковского – Шварца

$$\langle \boldsymbol{a}, \boldsymbol{b} \rangle^2 \;\le\; |\boldsymbol{a}|^2\, |\boldsymbol{b}|^2$$

для векторов $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{R}^s$. Применяя его к векторам $\boldsymbol{a} = x_1\boldsymbol{v}^{(1)} + \ldots + x_m\boldsymbol{v}^{(m)}$ и $\boldsymbol{b} = \boldsymbol{u}$, получаем

$$\langle x_1\boldsymbol{v}^{(1)} + \ldots + x_m\boldsymbol{v}^{(m)}, \boldsymbol{u}\rangle^2 \;\leq\; \mu(\boldsymbol{x})\,|\boldsymbol{u}|^2. \tag{5}$$

Согласно нашему предположению $\langle \boldsymbol{v}^{(i)}, \boldsymbol{u}\rangle = \sigma_{_T}$ для всех i, значит,

$$\langle x_1\boldsymbol{v}^{(1)} + \ldots + x_m\boldsymbol{v}^{(m)}, \boldsymbol{u}\rangle \;=\; (x_1 + \ldots + x_m)\,\sigma_{_T} \;=\; \sigma_{_T}$$

для *любого* распределения $\boldsymbol{x}$. В частности, для равномерного распределения $(\frac{1}{m}, \ldots, \frac{1}{m})$ последнее равенство принимает вид $|\boldsymbol{u}|^2 = \sigma_{_T}$. Поэтому неравенство (5) сводится к

$$\sigma_{_T}^2 \;\leq\; \mu(\boldsymbol{x})\,\sigma_{_T}, \qquad \text{или} \qquad \mu_{_T}(G) \;\geq\; \sigma_{_T}.$$

С другой стороны, для $\boldsymbol{x} = (\frac{1}{m}, \ldots, \frac{1}{m})$ получаем

$$\mu_{_T}(G) \;\leq\; \mu(\boldsymbol{x}) \;=\; |\tfrac{1}{m}(\boldsymbol{v}^{(1)} + \ldots + \boldsymbol{v}^{(m)})|^2 \;=\; |\boldsymbol{u}|^2 \;=\; \sigma_{_T},$$

т. е. мы доказали, что

$$\mu_{_T}(G) \;=\; \sigma_{_T}. \tag{6}$$

Таким образом, неравенство

$$\alpha(G) \;\leq\; \frac{1}{\sigma_{_T}} \tag{7}$$

доказано для *любого* ортонормального представления T графа G с константой $\sigma_{_T}$.

«Зонт с пятью спицами»

(C) Чтобы распространить это неравенство на $\Theta(G)$, будем действовать аналогично предыдущему. Снова рассмотрим произведение $G \times H$ двух графов. Пусть G и H имеют ортонормальные представления R и S в $\mathbb{R}^r$ и $\mathbb{R}^s$ с константами $\sigma_{_R}$ и $\sigma_{_S}$ соответственно. Пусть $\boldsymbol{v} = (v_1, \ldots, v_r)$ — вектор из R, а $\boldsymbol{w} = (w_1, \ldots, w_s)$ — вектор из S. Вершине $(\boldsymbol{v}, \boldsymbol{w})$ произведения $G \times H$ сопоставим вектор

$$\boldsymbol{v}\boldsymbol{w}^T := (v_1w_1, \ldots, v_1w_s, v_2w_1, \ldots, v_2w_s, \ldots, v_rw_1, \ldots, v_rw_s) \in \mathbb{R}^{rs}.$$

Несложно проверить, что $R \times S := \{\boldsymbol{v}\boldsymbol{w}^T : \boldsymbol{v} \in R, \boldsymbol{w} \in S\}$ есть ортонормальное представление графа $G \times H$ с константой $\sigma_{_R}\sigma_{_S}$. Теперь, учитывая (6), получаем

$$\mu_{_{R\times S}}(G \times H) \;\;=\;\; \mu_{_R}(G)\mu_{_S}(H).$$

Для графа $G^n = G \times \ldots \times G$ и представления T с константой $\sigma_{_T}$ это означает, что

$$\mu_{_{T^n}}(G^n) \;=\; \mu_{_T}(G)^n \;=\; \sigma_{_T}^n,$$

а отсюда и из (7) следуют неравенства

$$\alpha(G^n) \;\leq\; \sigma_{_T}^{-n}, \qquad \sqrt[n]{\alpha(G^n)} \;\leq\; \sigma_{_T}^{-1}.$$

Собирая вместе все эти замечания, мы завершаем доказательство Ловаса:

Теорема. *Если* $T = \{\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(m)}\}$ *— ортонормальное представление графа* G *с константой* σ_T*, то*

$$\Theta(G) \;\leq\; \frac{1}{\sigma_T}\,. \tag{8}$$

Для зонта Ловаса имеем $\boldsymbol{u} = (0, 0, h)^T$, где $h = \frac{1}{\sqrt[4]{5}}$, и поэтому $\sigma = \langle \boldsymbol{v}^{(i)}, \boldsymbol{u}\rangle = h^2 = \frac{1}{\sqrt{5}}$, откуда $\Theta(C_5) \leq \sqrt{5}$. Тем самым задача Шеннона решена.

Продолжим наше обсуждение. Неравенство (8) показывает, что чем больше константа σ_T представления графа G, тем лучше получается оценка для $\Theta(G)$. Опишем метод построения ортонормального представления *произвольного* графа G. Графу $G = (V, E)$ сопоставляется *матрица смежности* $A = (a_{ij})$, которая определяется следующим образом. Пусть $V = \{v_1, \ldots, v_m\}$; положим

$$a_{ij} \;:=\; \begin{cases} 1, & \text{если } \; v_i v_j \in E, \\ 0 & \text{в противном случае.} \end{cases}$$

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Матрица смежности для 5-цикла C_5

Матрица A — действительная, симметричная, с нулями на главной диагонали.

Далее нам потребуются два результата из линейной алгебры. Во-первых, матрица A, будучи симметричной, имеет m действительных собственных чисел $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_m$ (некоторые из них могут совпадать), и сумма собственных чисел равна сумме диагональных элементов матрицы A, т. е. 0. Поэтому наименьшее собственное число должно быть отрицательным (кроме тривиального случая, когда граф G не имеет ребер).

Пусть $p = |\lambda_m| = -\lambda_m$ — абсолютная величина наименьшего собственного числа. Рассмотрим матрицу

$$M \;:=\; I \;+\; \frac{1}{p}\,A,$$

где I — единичная $(m \times m)$-матрица. Матрица M имеет собственные числа

$$1 + \frac{\lambda_1}{p} \geq 1 + \frac{\lambda_2}{p} \geq \ldots \geq 1 + \frac{\lambda_m}{p} = 0.$$

Теперь приведем второй результат (теорему линейной алгебры о главных осях): если $M = (m_{ij})$ — действительная симметричная матрица, все собственные числа которой неотрицательны, то существуют такие векторы $\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(m)} \in \mathbb{R}^s$, где $s = \operatorname{rank}(M)$, что

$$m_{ij} \;=\; \langle \boldsymbol{v}^{(i)}, \boldsymbol{v}^{(j)}\rangle \qquad (1 \leq i, j \leq m).$$

В частности, для матрицы $M = I + \frac{1}{p}\,A$ получаем

$$\langle \boldsymbol{v}^{(i)}, \boldsymbol{v}^{(i)}\rangle \;=\; m_{ii} = 1 \qquad \text{для всех } i$$

и

$$\langle \boldsymbol{v}^{(i)}, \boldsymbol{v}^{(j)} \rangle \;=\; \frac{1}{p}\, a_{ij} \qquad \text{при} \qquad i \neq j.$$

Так как $a_{ij} = 0$ всякий раз, когда $v_i v_j \notin E$, то векторы $\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(m)}$ образуют искомое ортонормальное представление графа G.

Наконец, применим эту конструкцию к m-циклам C_m с нечетными $m \geq 5$. Нетрудно проверить, что $p = |\lambda_{\min}| = 2\cos\frac{\pi}{m}$ (см. вставку). Каждая строка матрицы смежности содержит два единичных элемента, поэтому сумма элементов каждой строки матрицы M равна $1 + \frac{2}{p}$. Для представления $\{\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(m)}\}$ это означает, что

$$\langle \boldsymbol{v}^{(i)}, \boldsymbol{v}^{(1)} + \ldots + \boldsymbol{v}^{(m)} \rangle \;=\; 1 + \frac{2}{p} \;=\; 1 + \frac{1}{\cos\frac{\pi}{m}}\,;$$

следовательно, для всех i

$$\langle \boldsymbol{v}^{(i)}, \boldsymbol{u} \rangle \;=\; \frac{1}{m}(1 + (\cos\tfrac{\pi}{m})^{-1}) \;=\; \sigma.$$

Собственные числа для цикла C_m

Рассмотрим матрицу смежности A цикла C_m. Чтобы найти ее собственные числа (и собственные векторы), используем корни m-й степени из единицы. Они образуют последовательность $1, \zeta, \zeta^2, \ldots, \zeta^{m-1}$, где $\zeta = e^{\frac{2\pi i}{m}}$ (см. вставку на с. 43).
Пусть $\lambda = \zeta^k$ — один из этих корней. Тогда $(1, \lambda, \lambda^2, \ldots, \lambda^{m-1})^T$ — собственный вектор матрицы A с собственным числом $\lambda + \lambda^{-1}$. Действительно, по определению A находим

$$A \begin{pmatrix} 1 \\ \lambda \\ \lambda^2 \\ \vdots \\ \lambda^{m-1} \end{pmatrix} = \begin{pmatrix} \lambda & + & \lambda^{m-1} \\ \lambda^2 & + & 1 \\ \lambda^3 & + & \lambda \\ & \vdots & \\ 1 & + & \lambda^{m-2} \end{pmatrix} = (\lambda + \lambda^{-1}) \begin{pmatrix} 1 \\ \lambda \\ \lambda^2 \\ \vdots \\ \lambda^{m-1} \end{pmatrix}.$$

Так как векторы $(1, \lambda, \ldots, \lambda^{m-1})$ при разных λ линейно независимы (их координаты образуют так называемую матрицу Вандермонда), то для нечетных m величины

$$\begin{aligned} \zeta^k + \zeta^{-k} \;&=\; [(\cos(2k\pi/m) + i\sin(2k\pi/m)] \\ &\quad + [\cos(2k\pi/m) - i\sin(2k\pi/m)] \\ &=\; 2\cos(2k\pi/m) \qquad (0 \leq k \leq \tfrac{m-1}{2}) \end{aligned}$$

суть все собственные числа матрицы A. Далее, на отрезке $[0, \pi]$ косинус убывает, и поэтому

$$2\cos\Big(\frac{(m-1)\pi}{m}\Big) \;=\; -2\cos\frac{\pi}{m}$$

— наименьшее собственное число матрицы A.

Поэтому, применяя основной результат — оценку (8), — находим, что

$$\Theta(C_m) \;\le\; \frac{m}{1+(\cos\frac{\pi}{m})^{-1}} \qquad \text{(для нечетных } m \ge 5\text{)}. \tag{9}$$

Заметим, что, поскольку $\cos\frac{\pi}{m} < 1$, неравенство (9) лучше найденной ранее оценки $\Theta(C_m) \le \frac{m}{2}$. Заметим еще, что $\cos\frac{\pi}{5} = \frac{\tau}{2}$, где $\tau = \frac{\sqrt{5}+1}{2}$ — золотое сечение. Значит, для $m = 5$ снова получаем

$$\Theta(C_5) \le \frac{5}{1+\frac{4}{\sqrt{5}+1}} = \frac{5(\sqrt{5}+1)}{5+\sqrt{5}} = \sqrt{5}.$$

Определяемое этой конструкцией ортонормальное представление, конечно, совпадает с «зонтом Ловаса».

Например, для $m = 7$ мы знаем лишь, что $\sqrt[4]{108} \le \Theta(C_7) \le \frac{7}{1+(\cos\frac{\pi}{7})^{-1}}$, или $3.2237 \le \Theta(C_7) \le 3.3177$.

А что она дает для C_7, C_9 и других циклов нечетных длин? Рассматривая $\alpha(C_m^2)$, $\alpha(C_m^3)$ и другие малые степени, можно улучшать нижнюю оценку $\frac{m-1}{2} \le \Theta(C_m)$, но ни для одного нечетного $m \ge 7$ наилучшие известные нижние оценки не совпадают с верхней оценкой из неравенства (8). Таким образом, через двадцать лет после того, как Ловас нашел изумительное доказательство равенства $\Theta(C_5) = \sqrt{5}$, эти задачи остаются открытыми и считаются очень трудными[3], т. е. ситуация та же, что и раньше.

Литература

[1] Chvátal V. *Linear Programming,* Freeman, New York 1983.

[2] Haemers W. *Eigenvalue methods,* в: «Packing and Covering in Combinatorics» (A. Schrijver, ed.), Math. Centre Tracts, **106**, 1979, pp. 15–38.

[3] Lovász L. *On the Shannon capacity of a graph,* IEEE Trans. Information Theory, **25**, 1979, pp. 1–7. [Русский перевод: Ловас Л. О шенноновской емкости графа. — Киберн. сб., 1983, вып. **19**, с. 5–22.]

[4] Shannon C. E. *The zero-error capacity of a noisy channel,* IRE Trans. Information Theory, **3**, 1956, pp. 3–15. [Русский перевод: Шеннон К. Пропускная способность канала с шумом при нулевой ошибке. В кн. Шеннон К. Работы по теории информации и кибернетике. — М., ИЛ, 1963, с. 464–487.]

[5*] Харари Ф. *Теория графов.* М., Мир, 1973.

[6*] Schrijver A.A. *Comparison of the Delsarte and Lovász bounds.* IEEE Trans. Inform. Theory, **IT-25**, 1979, № 4, pp. 425–429. [Русский перевод: Схрейвер А. Сравнение границ Дельсарта и Ловаса. — Киберн. сб., 1983, вып. **19**, с. 23–34.]

[7*] MacEliece R.J., Rodemich E.R., Rumsey H.C. *The Lovász bound and some generalizations.* J. Comb., Inform. and System Sci., 1978, **3**, № 3, pp. 134–152. [Русский перевод: Мак-Элис Р., Родемич Е., Рамсей Г. Граница Ловаса и некоторые обобщения. — Киберн. сб., 1983, вып. **19**, с. 35–55.]

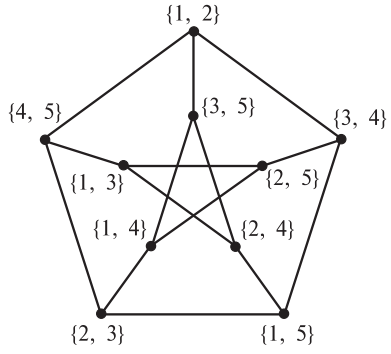
[3] Обсуждение результатов Л.Ловаса можно найти, например, в работах [6*], [7*]. — *Прим. перев.*

Хроматическое число графов Кнезера

Глава 38

В 1955 году теоретико-числовик Мартин Кнезер [5] предложил безобидную на первый взгляд задачу, которая стала одной из важных проблем в теории графов, пока 23 года спустя Ласло Ловас [6] не нашел ее блестящее и совершенно неожиданное решение с использованием «теоремы Борсука–Улама» из топологии.

В математике часто случается, что вскоре после решения давно стоявшей задачи появляется еще одно, более короткое. Так было и в этом случае. Через несколько недель Имре Барани [1] показал, что комбинация теоремы Борсука–Улама с другим известным результатом позволяет элегантно доказать гипотезу Кнезера. Затем в 2002 г. студент-выпускник Джошуа Грин еще больше упростил рассуждения Барани, и мы приводим здесь его вариант доказательства.



Известный *граф Петерсена* является графом Кнезера $K(5,2)$.

Но начнем с начала. Для целых $n > k \geq 1$ рассмотрим граф $K(n,k)$, который теперь называется *графом Кнезера*. Множество его вершин $V(n,k)$ есть семейство k-подмножеств множества $\{1,\ldots,n\}$, так что $|V(n,k)| = \binom{n}{k}$. Два таких k-множества A и B *смежны*, если они не пересекаются: $A \cap B = \varnothing$.

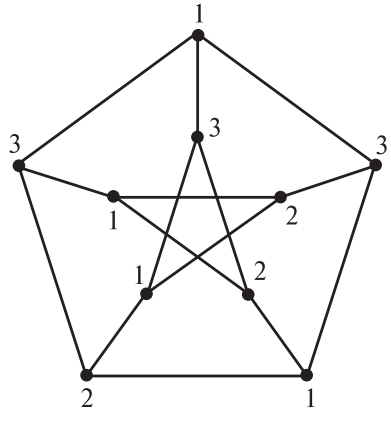
Если $n < 2k$, то каждые два подмножества пересекаются, и этот случай не интересен: $K(n,k)$ не имеет ребер. Поэтому далее будем предполагать, что $n \geq 2k$.

Графы Кнезера устанавливают интересную связь между теорией графов и конечными множествами. Например, *число независимости* графа $\alpha(K(n,k))$ равно максимальному числу попарно не пересекающихся k-подмножеств n-множества. Его значение дает теорема Эрдёша–Ко–Радо из главы 27: $\alpha(K(n,k)) = \binom{n-1}{k-1}$.

Можно изучать и другие интересные характеристики этого семейства графов, а Кнезер выбрал наиболее сложную: *хроматическое число* $\chi(K(n,k))$. Напомним, что в предыдущих главах m-цветной раскраской множества V вершин графа G называлось такое отображение $c : V \to \{1,\ldots,m\}$, которое смежным вершинам сопоставляет разные цвета. Хроматическое число $\chi(G)$ определяется как минимальное число цветов, достаточное для раскраски V. Другими словами, мы хотим представить множество вершин V как объединение минимально возможного числа попарно не пересекающихся *цветовых классов*: $V = V_1 \sqcup \ldots \sqcup V_{\chi(G)}$, так что между вершинами каждого из множеств V_i ребер нет[1].

Для графов $K(n,k)$ раскраске соответствует разбиение $V(n,k) = V_1 \sqcup \ldots \sqcup V_\chi$, в котором каждое V_i является семейством *пересекающихся* k-множеств. Поскольку мы предполагаем, что $n \geq 2k$, постольку положим $n = 2k + d,\ k \geq 1,\ d \geq 0$.

Отсюда следует, что $\chi(K(n,k)) \geq \frac{|V|}{\alpha} = \frac{\binom{n}{k}}{\binom{n-1}{k-1}} = \frac{n}{k}$.



3-раскраска графа Петерсена.

[1] Символ $\sqcup$ обозначает объединение попарно не пересекающихся множеств. — *Прим. ред.*

Существует простая раскраска графа $K(n,k)$ в $d+2$ цветов: V_i для каждого $i=1,2,\dots,d+1$ состоит из всех k-множеств с минимальным элементом i, а V_{d+2} состоит из k-подмножеств множества $\{d+2, d+3,\dots,2k+d\}$. Так как число элементов последнего множества равно $2k-1$, все k-подмножества из V_{d+2} попарно пересекаются, и им можно сопоставить цвет $d+2$. Таким образом, $\chi(K(2k+d,k)) \le d+2$, и Кнезер предложил доказать, что на самом деле левая и правая части равны.

Гипотеза Кнезера. *Имеет место равенство*

$$\chi(K(2k+d,d)) = d+2.$$

Скорее всего, у каждого первая попытка доказательства будет связана с индукцией по k и d. Действительно, базу индукции — случаи $k=1$ и $d=0,1$ — проверить несложно, однако не ясно, как сделать шаг индукции от k к $k+1$ (или от d к $d+1$). Поэтому вместо индукции мы переформулируем гипотезу в виде задачи о существовании.

Если $d=0$, то ребра в $K(2k,k)$ не имеют общих вершин. Поэтому $\chi(K(2k,k))=2$ в соответствии с гипотезой.

Если семейство k-подмножеств множества $\{1,2,\dots,2k+d\}$ разбито на $d+1$ не пересекающихся классов: $V(n,k) = V_1 \sqcup \dots \sqcup V_{d+1}$, то хотя бы один класс V_i содержит пару A, B не пересекающихся k-подмножеств.

Замечательная догадка Ловаса состояла в том, что (топологическим) центром проблемы является известная теорема о d-мерной единичной сфере S^d в $\mathbb{R}^{d+1}$: $S^d = \{x \in \mathbb{R}^{d+1} : |x| = 1\}$.

Теорема Борсука–Улама. *Для любого непрерывного отображения $f : S^d \to \mathbb{R}$ из d-сферы в d-мерное пространство существуют точки–антиподы $x^*, -x^*$, которые отображаются в одну и ту же точку: $f(x^*) = f(-x^*)$.*

Этот результат — один из краеугольных камней топологии. Впервые он был опубликован в знаменитой статье Борсука [2] в 1933 году. Мы даем набросок его доказательства в приложении к главе; полное доказательство можно найти в разделе 2.2 прекрасной книги Матушека «Применения теоремы Борсука–Улама» [8], само название которой демонстрирует мощь и значение теоремы. Имеется много эквивалентных формулировок, подтверждающих центральное место теоремы. Мы будем использовать ее вариант, который восходит к книге Л. А. Люстерника и Л. Г. Шнирельмана [7], вышедшей в 1930 году, т. е. раньше статьи Борсука.

Теорема. *Если d-сфера S^d покрыта $d+1$ множествами*

$$S^d = U_1 \bigcup \dots \bigcup U_d \bigcup U_{d+1}$$

так, что каждое из первых d множеств $U_1,\dots,U_d$ либо открыто, либо замкнуто, то одно из $d+1$ множеств содержит пару точек-антиподов.

Случай, когда все $d+1$ множеств замкнуты, рассмотрели Люстерник и Шнирельман. Случай, когда все $d+1$ множеств открыты, столь же не сложен и тоже называется теоремой Люстерника–Шнирельмана. Грин [4] догадался, что теорема справедлива и тогда, когда каждое из $d+1$ множеств *либо открыто, либо замкнуто*. Как мы увидим, для U_{d+1} не нужны даже эти условия. Для доказательства гипотезы Кнезера нам достаточно лишь, чтобы $U_1, \ldots, U_d$ были открытыми.

■ **Доказательство теоремы Люстерника–Шнирельмана с использованием теоремы Борсука–Улама.** Пусть дано покрытие $S^d = U_1 \cup \cdots \cup U_d \cup U_{d+1}$ с указанным порядком множеств. Предположим, что ни в одном из множеств U_i нет точек-антиподов. Определим отображение $f : S^d \to \mathbb{R}$, положив

$$f(x) = (d(x, U_1), d(x, U_2), \ldots, d(x, U_d)).$$

Здесь $d(x, U_i)$ обозначает расстояние от точки x до U_i. Так как расстояние d — непрерывная функция, то и отображение f непрерывно. Тогда по теореме Борсука–Улама существуют точки–антиподы $x^*, -x^*$, для которых $f(x^*) = f(-x^*)$. Поскольку U_{d+1} не содержит антиподов, мы получаем, что по крайней мере одна из точек x^* или $-x^*$ должна содержаться в одном из остальных множеств U_i, например, в множестве U_k ($k \le d$). Заменяя, если это необходимо, x^* на $-x^*$, мы можем считать, что $x^* \in U_k$. В частности, отсюда следует равенство $d(x^*, U_k) = 0$, а из условия $f(x^*) = f(-x^*)$ следует, что $d(-x^*, U_k) = 0$.

Если U_k замкнуто, то из равенства $d(-x^*, U_k) = 0$ следует, что $-x^* \in U_k$, и мы приходим к противоречию в связи с наличием в U_k пары точек–антиподов.

Если U_k открыто, то из $d(-x^*, U_k) = 0$ вытекает, что $-x^*$ содержится в замыкании $\bar{U}_k$ множества U_k. В свою очередь, множество $\bar{U}_k$ содержится в $S^d \setminus (-U_k)$, так как $S^d \setminus (-U_k)$ — замкнутое подмножество S_d, содержащее U_k. Следовательно, $-x^*$ содержится в $S^d \setminus (-U_k)$. Тогда $-x^*$ не может содержаться в $-U_k$, а x^* не может принадлежать U_k. Получено противоречие. □

Замыкание U_k — наименьшее замкнутое множество, содержащее U_k (пересечение всех замкнутых множеств, содержащих U_k).

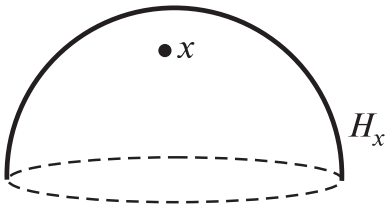
В качестве второй компоненты доказательства Имре Барани использовал еще одну теорему существования для сферы S^d.

Теорема Гейла. *Существует такое расположение $2k+d$ точек на сфере S^d, что каждая открытая полусфера содержит не менее k из этих точек.*

Дэвид Гейл открыл свою теорему в 1956 году в связи с многогранными политопами. Он предложил сложное индуктивное доказательство, но сегодня, используя накопленные знания, мы можем легко построить такое множество и доказать, что оно обладает нужным свойством.

С помощью этих результатов можно получить короткое решение задачи Кнезера, но, как показал Грин, можно добиться большего, даже не используя теорему Гейла. Достаточно взять любые $2k+d$ точек на сфере S^{d+1} в *общем положении*; последнее означает, что никакой набор из $d+2$ точек не содержится в гиперплоскости, проходящей через центр сферы. Ясно, что при $d \ge 0$ такие расположения существуют.

■ **Доказательство гипотезы Кнезера.** В качестве исходного множества возьмем $n = 2k+d$ точек в общем положении на сфере S^{d+1}.



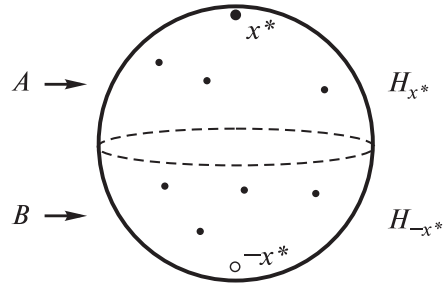
Открытая полусфера в S^2.

Пусть множество $V(n,k)$ всех k-подмножеств этого множества разбито на $d+1$ классов: $V(n,k) = V_1 \sqcup \ldots \sqcup V_{d+1}$. Мы должны найти пару не пересекающихся k-подмножеств A и B, принадлежащих одному и тому же классу V_i.

Для $i = 1, \ldots, d+1$ положим

$$O_i = \{x \in S^{d+1} : \text{открытая полусфера } H_x \text{ с полюсом } x \text{ содержит } k\text{-множество из } V_i\}.$$

Ясно, что каждое O_i — открытое множество. Кроме того, открытые множества O_i и замкнутое множество $C = S^{d+1} \setminus (O_1 \cup \ldots \cup O_{d+1})$ покрывают S^{d+1}. По теореме Люстерника–Шнирельмана одно из этих множеств содержит точки–антиподы x^* и $-x^*$. Этим множеством не может быть C! В самом деле, если бы x^* и $-x^*$ принадлежали C, то по определению множеств O_i каждая из полусфер H_{x^*} и H_{-x^*} содержала бы менее k точек. Это означает, что на экваторе $\bar{H}_{x^*} \cap \bar{H}_{-x^*}$ относительно северного полюса x^*, т. е. на гиперплоскости, проходящей через центр сферы, находится не менее $d+2$ точек. Но этого не может быть, так как точки находятся в общем положении. Значит, некоторое множество O_i содержит пару $x^*, -x^*$, а тогда существуют такие k-множества A и B (оба из класса V_i), что $A \subseteq H_{x^*}$ и $B \subseteq H_{-x^*}$.



Но так как полусферы H_{x^*} и H_{-x^*} *открыты*, то они не пересекаются; и это завершает доказательство. □

Читатель может усомниться в необходимости таких изощренных результатов, как теорема Борсука–Улама, для доказательства утверждений о конечных множествах. Действительно, недавно Юрий Матушек [9] нашел красивое комбинаторное доказательство гипотезы Кнезера, но при детальном анализе видно, что оно тоже имеет топологический характер (хотя и дискретный).

Приложение: Набросок доказательства теоремы Борсука–Улама

При каждом *общем* отображении (называемым также отображением *общего положения*) из компактного d-мерного пространства в d-мерное пространство любая точка образа имеет лишь конечное число прообразов[2]. Естественно ожидать, что при общем отображении из $(d+1)$-мерного пространства в d-мерное каждая точка образа имеет 1-мерный

[2]Указанное свойство — не определение, а лишь одно из свойств «общих» отображений. Как видно из дальнейшего, «общее» отображение не может быть контрпримером ни к какой достаточно общей теореме. — *Прим. ред.*

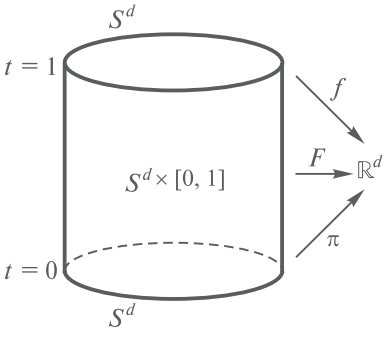
прообраз, т. е. совокупность кривых. Довольно легко доказывается, что любое гладкое или кусочно-линейное отображение можно преобразовать в близкое общее отображение.

Идея доказательства теоремы Борсука–Улама состоит в том, чтобы показать, что у каждого общего отображения $S^d \to \mathbb{R}^d$ существует нечетное (в частности, конечное и ненулевое) число пар антиподов с совпадающими образами. Если бы отображение f не имело ни одной такой пары антиподов, то существовали бы сколь угодно близкие к f общие отображения $\tilde{f}$, не имеющие антиподов с совпадающими образами.

Рассмотрим теперь проекцию $\pi : S^d \to \mathbb{R}^d$, которая попросту удаляет последнюю координату. Это отображение отождествляет «северный полюс» e_{d+1} d-сферы с ее «южным полюсом» $-e_{d+1}$. Для произвольного отображения $f : S^d \to \mathbb{R}^d$ построим непрерывное преобразование отображения π в f, т. е. построим интерполяцию этих двух отображений (например, линейную). Тогда мы получим такое непрерывное отображение

$$F : S^d \times [0,1] \to \mathbb{R}^d,$$

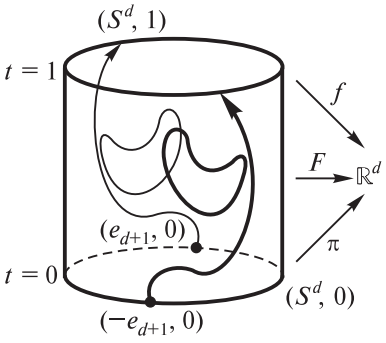
что $F(x,0) = \pi(x)$ и $F(x,1) = f(x)$ для всех $x \in S^d$. (Такое отображение называется *гомотопией*.)



Теперь аккуратным возмущением[3] преобразуем F в общее отображение $\tilde{F} = S^d \times [0,1] \to \mathbb{R}^d$, которое по-прежнему можно предполагать гладким или кусочно-линейным на мелкой триангуляции $S^d \times [0,1]$. Если это возмущение «достаточно мало» и проведено аккуратно, то возмущенный вариант проекции $\tilde{\pi}(x) := \tilde{F}(x,0)$ будет по-прежнему сопоставлять один и тот же образ точкам-антиподам $\pm e_{d+1}$ и только им. Если $\tilde{F}$ окажется достаточно общим, то множество точек в $S^d \times [0,1]$, определенное соотношением

$$M := \{(x,t) \in S^d \times [0,1] : \tilde{F}(-x,t) = \tilde{F}(x,t)\},$$

согласно теореме о неявных функциях (ее вариантам для гладких и кусочно-гладких функций) образует совокупность (не пересекающихся — *прим.ред.*) путей и замкнутых кривых. Ясно, что эта совокупность *симметрична*, т. е. $(-x,t) \in M$ тогда и только тогда, когда $(x,t) \in M$.



Пути в M могут иметь концевые точки лишь на границе множества $S^d \times [0,1]$, т. е. при $t = 0$ и $t = 1$. Однако концами путей при $t = 0$ являются только точки $(\pm e_{d+1}, 0)$, и два пути, начинающиеся в этих двух точках, являются симметричными копиями друг друга. Эти пути не пересекаются и могут оканчиваться лишь при $t = 1$. Значит, существуют решения уравнения $\tilde{F}(-x,t) = \tilde{F}(x,t)$ при $t = 1$ и, следовательно, решения уравнения $f(-x) = f(x)$.

Литература

[1] Bárány I. *A short proof of Kneser's conjecture.* J. Combinatorial Theory, Ser. B, **25**, 1978, pp. 325–326.

[2] Borsuk K. *Drei Sätze über die n-dimensionale Sphäre.* Fundamenta Math., **20**, 1933, pp. 177–190.

[3] В частности, сохраняющим равенство $F(e_{d+1},0) = F(-e_{d+1},0)$, см. ниже. — *Прим. ред.*

[3] Gale D. *Neighboring vertices on a convex polyhedron.* В сб. Linear Inequalities and Related Systems (ред. H. W. Kuhn, A. W. Tucker). Princeton University Press, Princeton, 1956, 255–263. [Имеется перевод: Д. Гейл. *Соседние вершины на выпуклом многограннике.* В кн.: Линейные неравенства и смежные вопросы, Москва, ИЛ, 1959.]

[4] Green J. E. *A new proof of Kneser's conjecture.* American Math. Monthly, **109** (2002), pp. 918–920.

[5] Kneser M. *Aufgabe 360.* Jahresbericht der Deutschen Mathematiker Vereinigung, **58** (1955), p. 27.

[6] Lovász L. *Kneser's conjecture, chromatic number and homotopy.* J. Combinatorial Theory, Ser. B, **25** (1978), pp. 319–324.

[7] Люстерник Л. А., Шнирельман Л. Г. *Топологические методы в вариационных задачах.* Москва, Госиздат, 1930.

[8] Matoušek J. *Using the Borsuk-Ulam Theorem. Lectures on Topological Methods in Combinatorics and Geometry* . Universitext, Springer-Verlag, Berlin, 2003 [Второе исправленное и дополненное издание: Springer-Verlag, Berlin, 2008.]

[9] Matoušek J. *A combinatorial proof of Kneser's conjecture.* Combinatorica, **24** (2004), pp. 163–170.

О друзьях и политиках

Глава 39

Неизвестно, кто первый поставил следующую задачу или кто придал ей социальный оттенок. Вот она:

> *Пусть в некоторой группе людей каждая пара лиц имеет ровно одного общего друга. Верно ли, что тогда есть человек («политик»), который является другом каждого?*

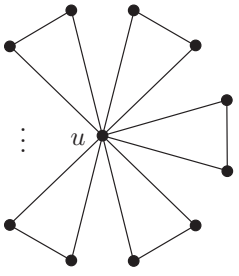
«Улыбка политика»

На математическом жаргоне эта задача называется *теоремой о друзьях*.

Сначала перефразируем задачу в терминах графов. Интерпретируя людей как множество вершин V, соединим две вершины ребром, если соответствующие лица являются друзьями. Мы неявно предполагаем, что дружба всегда является двусторонней, т. е. что если u — друг v, то v — также друг u, и кроме того, никто не является своим собственным другом. Тогда утверждение принимает следующий вид.

Теорема. *Пусть G — конечный граф, в котором любые две вершины имеют ровно одного общего соседа. Тогда в G существует вершина, смежная всем другим вершинам.*

Заметим, что конечные графы с этим свойством существуют; см. рисунок на полях, где u — политик. Более того, эти «графы-мельницы» оказываются к тому же единственными графами с указанными свойствами. В самом деле, нетрудно проверить, что при наличии политика возможны только такие графы-мельницы.

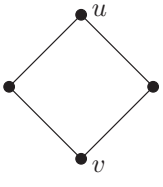


Граф-мельница

Удивительно, что теорема о друзьях не верна для бесконечных графов! Для индуктивного построения контрпримера можно начать, например, с 5-цикла и каждый раз добавлять в граф общих соседей для всех пар вершин, которые их до сих пор не имели. Это приводит к (счетному) бесконечному графу без политика.

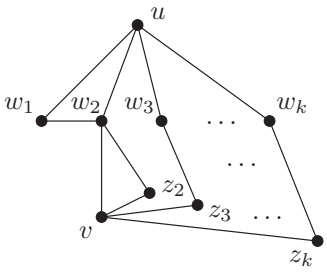
Существует несколько доказательств теоремы о друзьях, но первое доказательство, предложенное Паулем Эрдёшем, Альфредом Реньи и Верой Сос [1], все еще является наиболее изысканным.

■ **Доказательство.** Предположим, что утверждение не верно и что граф G является контрпримером, т. е. что в G нет вершины, смежной всем другим вершинам. Мы придем к противоречию в два шага. Первая часть доказательства является комбинаторной, а вторая основана на линейной алгебре.



(1) Как и раньше, будем через $d(u)$ обозначать степень вершины u. Покажем, что G — *регулярный граф*, т. е. что $d(u) = d(v)$ для всех $u, v \in V$.

Заметим вначале, что из условия теоремы следует отсутствие в G циклов длины 4. Назовем это C_4*-условием*.



Прежде всего докажем, что любые две *несмежные* вершины u и v имеют одинаковую степень: $d(u) = d(v)$. Предположим, что $d(u) = k$ и $w_1, \ldots, w_k$ — соседи u. Только одна из вершин w_i, например, w_2, смежна v, и w_2 смежна ровно одной из других вершин w_i, например, вершине w_1, так что мы имеем ситуацию, которая представлена на полях. Вершина v имеет с w_1 общего соседа w_2, а с w_i $(i \geq 2)$ — общего соседа z_i $(i \geq 2)$. Согласно C_4-условию, все эти z_i должны быть различны, и мы заключаем, что $d(v) \geq k = d(u)$; поэтому в силу симметрии $d(u) = d(v) = k$.

Чтобы завершить доказательство утверждения **(1)**, заметим, что любая вершина, отличная от w_2, не смежна либо с u, либо с v, и, следовательно, согласно тому, что мы уже доказали, имеет степень k. Но так как хотя бы одна из них не смежна с w_2, то степень w_2 тоже равна k, и поэтому G является k-регулярным.

Суммируя степени всех k соседей u, мы получаем k^2. Учитывая, что каждая вершина графа G (кроме u) имеет с u ровно одного общего соседа, мы подсчитали каждую вершину один раз (за исключением u, которая считалась k раз). Поэтому общее число вершин графа G есть

$$n \;=\; k^2 - k + 1. \tag{1}$$

(2) Оставшаяся часть доказательства — прекрасное применение некоторых стандартных теорем линейной алгебры. Заметим вначале, что k должно быть больше двух, так как при $k \leq 2$ в силу (1) имеются лишь две возможности: $G = K_1$ или $G = K_3$, и обе соответствуют тривиальным графам-мельницам. Рассмотрим матрицу смежности $A = (a_{ij})$ графа G, определенную на с. 258. Согласно первой части доказательства каждая строка матрицы A содержит ровно k единиц, и по условию теоремы для любых двух строк имеется ровно один столбец, в котором они обе содержат единицы. Далее, главная диагональ матрицы A состоит из нулей. Поэтому

$$A^2 \;=\; \begin{pmatrix} k & 1 & \ldots & 1 \\ 1 & k & & 1 \\ \vdots & & \ddots & \vdots \\ 1 & \ldots & 1 & k \end{pmatrix} \;=\; (k-1)\,I + J\,,$$

где I — единичная матрица, а в матрице J все элементы равны 1. (Дальнейшие рассуждения почти дословно повторяют конец п. 5 гл. 25. — *Прим. ред.*) Матрица J имеет такие собственные значения: n (кратности 1) и 0 (кратности $n-1$). Поэтому A^2 имеет собственные значения $k - 1 + n = k^2$ (кратности 1) и $k - 1$ (кратности $n - 1$).

Учитывая, что неотрицательная матрица A симметрична и, следовательно, диагонализуема, мы приходим к выводу, что A имеет собственные значения k (кратности 1) и $\pm\sqrt{k-1}$. Допустим, что r ее собственных значений равны $\sqrt{k-1}$, а s равны $-\sqrt{k-1}$, причем $r + s = n - 1$. Теперь мы почти у цели. Так как сумма собственных значений матрицы A равна следу (который равен нулю), мы находим:

$$k + r\sqrt{k-1} - s\sqrt{k-1} \;=\; 0;$$

значит, $r \neq s$ и

$$\sqrt{k-1} \;=\; \frac{k}{s-r}\,.$$

Далее, если квадратный корень $\sqrt{m}$ из натурального числа рационален, то он является целым! (Элегантное доказательство этого дал Дедекинд в 1858 году. Пусть n_0 — наименьшее натуральное число, для которого $n_0\sqrt{m} \in \mathbb{N}$. Если $\sqrt{m} \notin \mathbb{N}$, то существует такое $\ell \in \mathbb{N}$, что $0 < \sqrt{m} - \ell < 1$. Полагая $n_1 := n_0(\sqrt{m} - \ell)$, находим, что $n_1 \in \mathbb{N}$ и, кроме того, $n_1\sqrt{m} = n_0(\sqrt{m} - \ell)\sqrt{m} = n_0 m - \ell(n_0\sqrt{m}) \in \mathbb{N}$. Так как $n_1 < n_0$, то это противоречит выбору n_0.)

Возвращаясь к нашему уравнению, положим $h = \sqrt{k-1} \in \mathbb{N}$; тогда

$$h(s-r) \;=\; k \;=\; h^2 + 1.$$

Так как h делит h^2+1 и h^2, то h должно равняться единице, и поэтому $k = 2$. Но эту возможность мы уже исключили. Итак, мы пришли к противоречию, и доказательство закончено. □

Однако, это еще не все. Переформулируем нашу теорему следующим образом. Пусть граф G обладает следующим свойством: между любыми двумя его вершинами существует ровно один путь длины 2. Ясно, что это — эквивалентная формулировка условия теоремы. Наша теорема означает, что все такие графы являются графами-мельницами. Но что будет, если рассматривать пути, длины которых больше 2? Согласно гипотезе Антона Коцига [2] такая ситуация невозможна.

Гипотеза Коцига. *Пусть $\ell > 2$. Тогда не существует конечных графов, между любыми двумя вершинами которых имеется ровно один путь длины ℓ.*

Сам Коциг проверил эту гипотезу для $\ell \leq 8$. В [3] его гипотеза доказана для $\ell = 20$, и А.Косточка недавно сообщил, что к настоящему времени он проверил ее для всех $\ell \leq 33$. В общем случае, однако, представляется, что доказательство находится вне пределов досягаемости...

Литература

[1] Erdős P., Rényi A., Sós V. *On a problem of graph theory.* Studia Sci. Math., **1** (1966), 215–235.

[2] Kotzig A. *Regularly k-path connected graphs.* Congressus Numerantium, **40** (1983), 137–141.

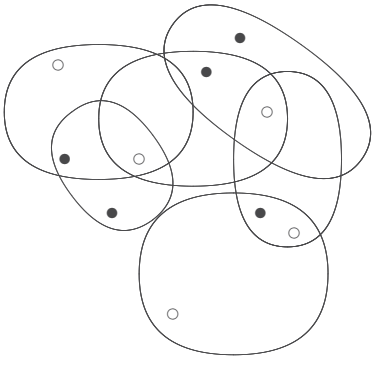
[3] Kostochka A. *The nonexistence of certain generalized friendship graphs.* In: «Combinatorics» (Eger, 1987), Colloq. Math. Soc. János Bolyai, **52**, North-Holland, Amsterdam 1988, 341–356.

Глава 40 Вероятность (иногда) упрощает перечисление

Как начали мы эту книгу с первой статьи Пауля Эрдёша, так и завершим ее обсуждением того, что, возможно, будет считаться его наиболее ценным наследием: введенного им (совместно с Альфредом Реньи) *вероятностного метода*. В простейшем виде он состоит в следующем:

> *Пусть для заданного множества объектов вероятность того, что объект не обладает некоторым свойством, меньше* 1. *Тогда должен существовать объект, обладающий этим свойством.*

Таким образом, мы получаем теорему о *существовании*. Часто бывает, что найти этот объект очень трудно, но известно, что он существует. Мы приведем здесь три примера (в порядке возрастания сложности) применения вероятностного метода Эрдёшем, а завершим главу особенно элегантным недавним применением.



2-раскрашиваемое семейство 3-множеств

В качестве разминки рассмотрим семейство $\mathcal{F}$ подмножеств A_i конечного основного множества X, имеющих один и тот же объем $d \geq 2$. Семейство $\mathcal{F}$ назовем 2-*раскрашиваемым*, если существует такая раскраска X в два цвета, что в каждом множестве A_i есть элементы обоих цветов. Очевидно, что не для каждого семейства такая окраска существует. Например, рассмотрим *все* d-элементные подмножества множества X, состоящего из $(2d-1)$ элементов. Тогда при любой раскраске X в два цвета найдутся d одинаково окрашенных элементов. С другой стороны, столь же ясно, что каждое подсемейство 2-раскрашиваемого семейства d-элементных множеств само 2-раскрашиваемо. Поэтому представляет интерес *наименьшее* число $m = m(d)$, для которого существует семейство из m множеств, не являющееся 2-раскрашиваемым. Иначе говоря, $m(d)$ — наибольшее такое число, что *каждое* семейство, содержащее меньше $m(d)$ множеств, 2-раскрашиваемо.

Теорема 1. *Каждое семейство, содержащее не более* 2^{d-1} *множеств из* d *элементов,* 2*-раскрашиваемо, т. е.* $m(d) > 2^{d-1}$.

■ **Доказательство.** Пусть $\mathcal{F}$ — семейство, состоящее не более чем из 2^{d-1} множеств по d элементов в каждом. Раскрасим элементы множества X случайным образом в два цвета, считая все раскраски равновероятными. Для каждого множества $A \in \mathcal{F}$ обозначим через E_A событие «все элементы множества A окрашены одинаково». Так как существует ровно две таких раскраски, то

$$\mathrm{Prob}(E_A) \;=\; \left(\tfrac{1}{2}\right)^{d-1},$$

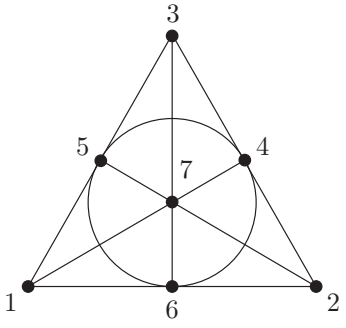
и, следовательно, при $m = |\mathcal{F}| \leq 2^{d-1}$ (заметим, что пересечения собы-

тий E_A не пустые) справедливо неравенство

$$\mathrm{Prob}\left(\bigcup_{A\in\mathcal{F}} E_A\right) \;<\; \sum_{A\in\mathcal{F}} \mathrm{Prob}(E_A) \;=\; m\,(\tfrac{1}{2})^{d-1} \;\le\; 1.$$

Значит, существует 2-раскраска X без одноцветных множеств в $\mathcal{F}$, а это и есть условие 2-раскрашиваемости. □

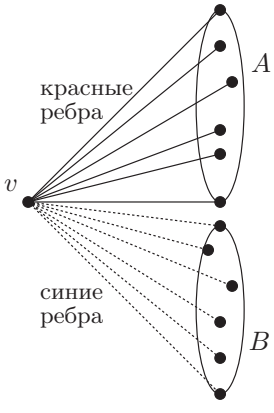
Верхняя оценка для $m(d)$, приближенно равная $d^2 2^d$, также была получена Эрдёшем с помощью вероятностного метода, но на этот раз множества выбирались случайно, а раскраска фиксировалась. Точно известны лишь два первых значения: $m(2) = 3$, $m(3) = 7$. Конечно, значение $m(2) = 3$ реализуется графом K_3, а конфигурация Фано показывает, что $m(3) \le 7$. В этом случае $\mathcal{F}$ состоит из семи 3-элементных подмножеств изображенной на полях фигуры (включая лежащее на окружности множество $\{4, 5, 6\}$). В качестве развлечения читатель может доказать, что для раскраски $\mathcal{F}$ нужны три краски. Доказательство того, что все семейства из шести 3-элементных множеств 2-раскрашиваемы (и поэтому $m(3) = 7$), требует больше усилий.



Наш следующий пример является классическим в области, связанной с числами Рамсея. Рассмотрим полный граф K_N с N вершинами. Скажем, что K_N обладает свойством (m, n), если при любой раскраске ребер графа K_N в красный и синий цвета найдется полный подграф с m вершинами, все ребра которого красные, или полный подграф с n вершинами, все ребра которого синие. Ясно, что если K_N обладает свойством (m, n), то тем же свойством обладает каждый граф K_s, если $s \ge N$. Как и в первом примере, нас интересует *наименьшее* число N (если оно существует) с указанным свойством; это число и есть *число Рамсея* $R(m, n)$.

Вначале заметим, что всегда выполняется равенство $R(m, 2) = m$, так как либо все ребра графа K_m являются красными, либо существует синее ребро, т. е. синий подграф K_2. В силу симметрии $R(2, n) = n$. Далее, допустим, что $R(m-1, n)$ и $R(m, n-1)$ существуют. Докажем, что тогда существует и $R(m, n)$ и

$$R(m, n) \;\le\; R(m-1, n) \;+\; R(m, n-1). \qquad (1)$$



Положим $N = R(m-1, n) + R(m, n-1)$ и рассмотрим произвольную красно-синюю раскраску графа K_N. Для некоторой вершины v обозначим через A множество вершин, соединенных с v красным ребром, и через B множество вершин, соединенных с v синим ребром.

Так как $|A| + |B| = N - 1$, то либо $|A| \ge R(m-1, n)$, либо $|B| \ge R(m, n-1)$. Пусть $|A| \ge R(m-1, n)$ (другой случай рассматривается аналогично). Тогда по определению $R(m-1, n)$ либо в A существует подмножество A_R объема $m-1$, все вершины которого соединены красными ребрами и которое вместе с v образует красный граф K_m, либо существует подмножество A_B объема n, все вершины которого соединены синими ребрами. Следовательно, K_N обладает (m, n)-свойством, и неравенство (1) доказано.

Объединяя (1), начальные значения $R(m, 2) = m$, $R(2, n) = n$ и учитывая известную рекуррентную формулу для биномиальных коэффи-

циентов, получаем

$$R(m,n) \;\le\; \binom{m+n-2}{m-1},$$

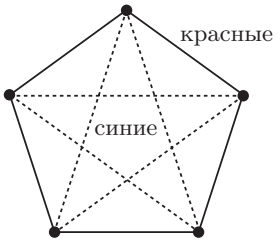
и, в частности

$$R(k,k) \;\le\; \binom{2k-2}{k-1} \;=\; \binom{2k-3}{k-1} \;+\; \binom{2k-3}{k-2} \;\le\; 2^{2k-3}. \qquad (2)$$

Нас интересует прежде всего нижняя оценка для $R(k,k)$. Это сводится к нахождению по возможности наибольшего значения $N < R(k,k)$, при котором *существует* раскраска ребер, не порождающая ни красных, ни синих графов K_k. Именно здесь применяется вероятностный метод.

Теорема 2. *Для чисел Рамсея при всех $k \ge 2$ справедлива оценка снизу*

$$R(k,k) \;\ge\; 2^{\frac{k}{2}}.$$



■ **Доказательство.** Имеем $R(2,2) = 2$. Из (2) следует оценка $R(3,3) \le 6$, и изображенный на полях окрашенный пятиугольник показывает, что $R(3,3) = 6$.

Далее будем считать, что $k \ge 4$. Пусть $N < 2^{\frac{k}{2}}$. Рассмотрим все красно-синие раскраски, и будем раскрашивать ребра независимо друг от друга в красный и синий цвета с вероятностью $\frac{1}{2}$. Тогда все раскраски имеют одинаковую вероятность $2^{-\binom{N}{2}}$. Пусть A — множество, содержащее k вершин. Вероятность события $A_{\scriptscriptstyle R} = \{$все вершины из A соединены красными ребрами$\}$ равна $2^{-\binom{k}{2}}$. Значит, вероятность $p_{\scriptscriptstyle R}$ того, что *существует* k-элементное множество вершин, все ребра между которыми — красные, оценивается так:

$$p_{\scriptscriptstyle R} \;=\; \mathrm{Prob}\left(\bigcup_{|A|=k} A_{\scriptscriptstyle R}\right) \;\le\; \sum_{|A|=k} \mathrm{Prob}(A_{\scriptscriptstyle R}) \;=\; \binom{N}{k} 2^{-\binom{k}{2}}.$$

Теперь, учитывая, что $N < 2^{\frac{k}{2}}$ и $k \ge 4$, и используя неравенство $\binom{N}{k} \le \frac{N^k}{2^{k-1}}$ при $k \ge 2$ (см. с. 21), получаем

$$\binom{N}{k} 2^{-\binom{k}{2}} \;\le\; \frac{N^k}{2^{k-1}} 2^{-\binom{k}{2}} \;<\; 2^{\frac{k^2}{2}-\binom{k}{2}-k+1} \;=\; 2^{-\frac{k}{2}+1} \le \frac{1}{2}.$$

Таким образом, $p_{\scriptscriptstyle R} < \frac{1}{2}$, и в силу симметрии $p_{\scriptscriptstyle B} < \frac{1}{2}$, где $p_{\scriptscriptstyle B}$ — вероятность того, что все ребра, соединяющие некоторые k вершин, окрашены в синий цвет. Значит, $p_{\scriptscriptstyle R} + p_{\scriptscriptstyle B} < 1$, если $N < 2^{\frac{k}{2}}$, так что *должна* существовать раскраска без красных и синих графов K_k. Это означает, что K_N не обладает свойством (k,k). □

Конечно, разница между нижней и верхней оценками для $R(k,k)$ довольно велика. Однако, несмотря на простоту этого Доказательства из Книги, в течение более 50 лет после результата Эрдёша не удается найти оценку снизу для произвольного k с лучшим показателем степени. Именно, никому пока не удалось получить нижнюю оценку вида

$R(k,k) > 2^{(\frac{1}{2}+\varepsilon)k}$ или верхнюю оценку вида $R(k,k) < 2^{(2-\varepsilon)k}$ с фиксированным $\varepsilon > 0$.

Наш третий результат — еще одна превосходная иллюстрация вероятностного метода. Рассмотрим граф G с n вершинами, и пусть $\chi(G)$ — его хроматическое число[1]. Если $\chi(G)$ велико, т. е. если для раскраски графа требуется много цветов, то можно подумать, что G содержит большой полный подграф. Однако это далеко от истины. В сороковых годах Бланш Декарт [10*] построила графы с произвольно большими хроматическими числами, не имеющие треугольников (т. е. каждый цикл в них имеет длину не меньше 4), и аналогичные графы построили другие авторы.

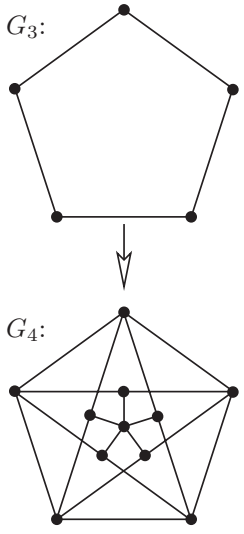
Графы с большими хроматическими числами, не имеющие треугольников

Построим последовательность $G_3, G_4, \ldots$ графов без 3-циклов, для которых

$$\chi(G_n) \;=\; n.$$

Начнем с $G_3 = C_5$, т. е. с 5-цикла; тогда $\chi(G_3) = 3$. Допустим, что мы уже построили граф G_n с множеством вершин V. Новый граф G_{n+1} имеет множество вершин $V \cup V' \cup \{z\}$, где вершины $v' \in V'$ взаимно однозначно соответствуют вершинам $v \in V$, а z — единственная другая вершина. Ребра G_{n+1} разбиваются на три класса: а) все ребра графа G_n, б) ребра, соединяющие каждую вершину v' с соседями соответствующей вершины v в G_n, в) ребра, соединяющие z со всеми вершинами $v' \in V'$. Таким образом из $G_3 = C_5$ мы получаем в качестве G_4 так называемый *граф Мыцельского*.

Ясно, что G_{n+1} не имеет треугольников. Чтобы доказать, что $\chi(G_{n+1}) = n+1$, используем индукцию по n. Допустим, что $\chi(G_{n+1}) = n$. Любая n-раскраска G_{n+1} порождает n-раскраску графа G_n. Рассмотрим класс C вершин G_n, окрашенных каким-то одним цветом. Должна существовать вершина $v \in C$, смежная по крайней мере одной вершине каждого другого цветового класса (в противном случае можно было бы раскрасить вершины из C остальными $n-1$ цветами, а это значило бы, что $\chi(G_n) \le n-1$). Но тогда v' (вершина в V', соответствующая v) в рассматриваемой n-раскраске G_{n+1} должна быть окрашена в тот же самый цвет, что и v. Поэтому для раскраски вершин из V' используются все n красок, и для окраски z требуется новая краска, что противоречит предположению $\chi(G_{n+1}) = n$.



Построение графа Мыцельского

Однако в этих примерах было много циклов длины 4. Можно ли добиться большего? Существуют ли графы без циклов малых длин, имеющие сколь угодно большие хроматические числа? Да, существуют! Для краткости формулировок назовем длину кратчайшего цикла в G *обхватом* $\gamma(G)$ графа G. Справедлива следующая теорема, впервые доказанная Паулем Эрдёшем.

[1] См. гл. 33. — *Прим. перев.*

Теорема 3. *Для каждого $k \geq 2$ существует граф G с хроматическим числом $\chi(G) > k$ и обхватом $\gamma(G) > k$.*

Метод доказательства аналогичен использованному в предыдущих случаях. Мы рассмотрим некоторое вероятностное пространство на графах и покажем, что вероятность события $\chi(G) \leq k$ меньше $\frac{1}{2}$ и что вероятность события $\gamma(G) \leq k$ тоже меньше $\frac{1}{2}$. Поэтому должен существовать граф с указанными свойствами.

■ **Доказательство.** Пусть $V = \{v_1, v_2, \ldots, v_n\}$ — множество вершин и p — фиксированное число между 0 и 1, точное значение которого будет выбрано позднее. Наше вероятностное пространство $\mathcal{G}(n,p)$ состоит из всех графов с множеством вершин V. Вероятность появления графа определяется следующим условием: каждое ребро независимо от остальных ребер присутствует в графе с вероятностью p и отсутствует с вероятностью $1-p$. Другими словами, для каждого ребра проводится испытание Бернулли с вероятностью успеха p. Например, вероятность $\mathrm{Prob}(K_n)$ появления полного графа есть $\mathrm{Prob}(K_n) = p^{\binom{n}{2}}$. В общем случае для графа H с множеством вершин V и ровно m ребрами $\mathrm{Prob}(H) = p^m(1-p)^{\binom{n}{2}-m}$.

Рассмотрим сначала хроматическое число $\chi(G)$. Обозначим через $\alpha = \alpha(G)$ *число независимости* графа G, т. е. объем наибольшего независимого множества вершин графа G. Так как при правильной раскраске $\chi = \chi(G)$ цветами все множества одинаково окрашенных вершин являются независимыми (следовательно, их объемы не больше α), мы заключаем, что $\chi\alpha \geq n$. Значит, если α мало по сравнению с n, то χ должно быть большим, что нам и нужно.

Пусть r — целое число, $2 \leq r \leq n$. Вероятность того, что фиксированное множество из r элементов V независимо, есть $(1-p)^{\binom{r}{2}}$, и с помощью тех же рассуждений, что в теореме 2, мы получаем оценки

$$\begin{aligned}\mathrm{Prob}(\alpha \geq r) \;&\leq\; \binom{n}{r}(1-p)^{\binom{r}{2}} \\ &\leq\; n^r(1-p)^{\binom{r}{2}} \;=\; \Bigl(n(1-p)^{\frac{r-1}{2}}\Bigr)^r \;\leq\; \Bigl(ne^{-p(r-1)/2}\Bigr)^r,\end{aligned}$$

поскольку $1-p \leq e^{-p}$ при всех p.

Для любого фиксированного $k > 0$ положим $p := n^{-\frac{k}{k+1}}$ и покажем, что для достаточно больших n

$$\mathrm{Prob}\Bigl(\alpha \geq \frac{n}{2k}\Bigr) \;<\; \frac{1}{2}\,. \tag{3}$$

В самом деле, так как $n^{\frac{1}{k+1}}$ растет быстрее, чем $\log n$, то $n^{\frac{1}{k+1}} \geq 6k\log n$ при достаточно больших n, поэтому $p \geq 6k\frac{\log n}{n}$. При $r := \lceil \frac{n}{2k} \rceil$ это дает $pr \geq 3\log n$, в силу чего

$$ne^{-p(r-1)/2} \;=\; ne^{-\frac{pr}{2}}e^{\frac{p}{2}} \;\leq\; ne^{-\frac{3}{2}\log n}e^{\frac{1}{2}} \;=\; n^{-\frac{1}{2}}e^{\frac{1}{2}} \;=\; \bigl(\tfrac{e}{n}\bigr)^{\frac{1}{2}},$$

и последнее выражение стремится к 0, когда $n \to \infty$. Значит, существует такое $n_1 < \infty$, что (3) выполняется для всех $n \geq n_1$.

Теперь рассмотрим параметр $\gamma(G)$. Мы хотим показать, что для данного k не может существовать слишком много циклов длины не больше k. Пусть $3 \le i \le k$ и $A \subseteq V$ — фиксированное i-элементное множество. Число возможных i-циклов на A, очевидно, равно числу полноцикловых перестановок[2] A, деленному на 2 (поскольку цикл можно проходить в любом из двух направлений), и равно поэтому $\frac{(i-1)!}{2}$. Значит, общее число возможных i-циклов равно $\binom{n}{i}\frac{(i-1)!}{2}$, и каждый такой цикл C появляется с вероятностью p^i. Пусть X — случайная величина, равная количеству циклов в графе G длины не больше k. Чтобы оценить X, воспользуемся двумя простыми, но замечательными приемами. Первый – это линейность математического ожидания, а второй — неравенство Маркова для неотрицательных случайных величин, согласно которому

$$\mathrm{Prob}(X \ge a) \ \le \ \frac{EX}{a},$$

где EX — математическое ожидание X. Эти приемы были описаны в приложении к главе 15.

Обозначим через X_C индикатор цикла C; пусть i — длина C. Иначе говоря, мы полагаем $X_C = 1$ или 0 в зависимости от того, присутствует цикл C в графе или нет; следовательно, $EX_C = p^i$. Так как X равно числу всех циклов длины не более k, то $X = \sum X_C$, и в силу линейности математического ожидания

$$EX \ = \ \sum_{i=3}^{k} \binom{n}{i} \frac{(i-1)!}{2} p^i \ \le \ \frac{1}{2}\sum_{i=3}^{k} n^i p^i \ \le \ \frac{1}{2}(k-2)n^k p^k,$$

где последнее неравенство справедливо в силу того, что $np = n^{\frac{1}{k+1}} \ge 1$. Применяя теперь неравенство Маркова с $a = \frac{n}{2}$, получаем

$$\mathrm{Prob}(X \ge \tfrac{n}{2}) \le \frac{EX}{n/2} \le \ (k-2)\frac{(np)^k}{n} \ = \ (k-2)n^{-\frac{1}{k+1}}.$$

Поскольку правая часть стремится к 0, когда n стремится к бесконечности, постольку существует такое $n_2 < \infty$, что $p(X \ge \frac{n}{2}) < \frac{1}{2}$ при $n \ge n_2$.

Теперь мы почти у финиша. Наши рассуждения показали, что при $n \ge \max(n_1, n_2)$ существует граф H с n вершинами, у которого $\alpha(H) < \frac{n}{2k}$ и число циклов длины не больше k меньше $\frac{n}{2}$. Удалим по одной вершине в каждом из этих циклов и обозначим через G полученный граф. Тогда для графа G справедлива оценка $\gamma(G) > k$. Так как G содержит больше $\frac{n}{2}$ вершин и $\alpha(G) \le \alpha(H) < \frac{n}{2k}$, то

$$\chi(G) \ \ge \ \frac{n/2}{\alpha(G)} \ \ge \ \frac{n}{2\alpha(H)} \ > \ \frac{n}{n/k} \ = \ k,$$

и доказательство закончено. □

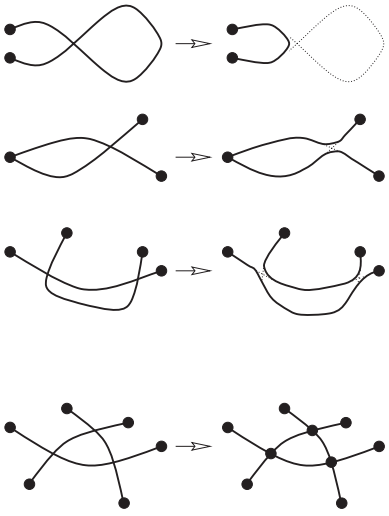
Известны явные конструкции графов с большим обхватом и очень большими хроматическими числами. (Напротив, не известны способы построения красно-синих раскрасок без больших одноцветных клик, которые согласно теореме 2 существуют.) Поражает, что доказательство

[2] То есть перестановок, содержащих единственный цикл длины i. — *Прим. перев.*

Эрдёша обосновывает существование относительно небольших графов с большими хроматическими числами и обхватами.

В завершение нашей экскурсии по вероятностному миру мы обсудим важный результат из геометрической теории графов (который снова возвращает нас к Паулю Эрдёшу); ошеломляющее Доказательство из Книги этого результата просто опьяняет.

Рассмотрим простой граф $G = G(V, E)$ с n вершинами и m ребрами. Мы хотим уложить G на плоскости так же, как укладывали планарные графы. В гл. 12 в качестве следствия из формулы Эйлера было показано, что простой планарный граф имеет не более $3n - 6$ ребер. Значит, если m больше $3n - 6$, то ребра при укладке графа на плоскость должны пересекаться. Поэтому естественно определить *число скрещиваний* $\mathrm{cr}(G)$ как наименьшее число пересечений ребер среди всех укладок G на плоскость (причем пересечения более двух ребер в одной точке не допускаются). Следовательно, $\mathrm{cr}(G) = 0$ тогда и только тогда, когда G — планарный граф.



Для такой минимальной укладки выполняются три условия:

- ребро не может пересекать само себя;
- не могут пересекаться ребра с общей концевой вершиной;
- никакие два ребра не пересекаются дважды.

Действительно, в каждом из этих случаев можно (с помощью операций, указанных на рисунках) построить другую укладку того же самого графа с меньшим числом скрещиваний. Поэтому далее мы будем предполагать, что указанные условия выполняются для любой укладки.

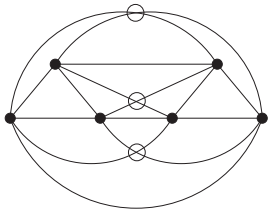
Пусть граф G уложен на плоскость с $\mathrm{cr}(G)$ скрещиваниями. Нетрудно получить для числа скрещиваний оценку снизу. Для этого рассмотрим граф H, вершинами которого являются все вершины G и все точки пересечений ребер, а ребрами — ребра G, не имеющие пересечений, и все части ребер графа G, на которые их разделили точки пересечений.

Построенный граф H — плоский и простой (это следует из трех наших условий!). Число вершин в H равно $n + \mathrm{cr}(G)$, а число ребер есть $m + 2\mathrm{cr}(G)$, так как каждая новая вершина имеет степень 4. Используя оценку числа ребер плоского графа, мы находим, что

$$m + 2\,\mathrm{cr}(G) \quad \leq \quad 3(n + \mathrm{cr}(G)) - 6,$$

то есть

$$\mathrm{cr}(G) \quad \geq \quad m - 3n + 6. \tag{4}$$



Например, для полного графа K_6 получаем

$$\mathrm{cr}(K_6) \geq 15 - 18 + 6 = 3,$$

и укладка K_6 с ровно тремя пересечениями действительно существует (см. рисунок на полях).

Оценка (4) достаточно хороша, когда m линейно связано с n, но если m значительно больше n, то картина меняется, и к этому случаю относится наша теорема.

Теорема 4. *Пусть G — простой граф с n вершинами и m ребрами, причем $m \geq 4n$. Тогда*

$$\mathrm{cr}(G) \;\geq\; \frac{1}{64}\frac{m^3}{n^2}\,.$$

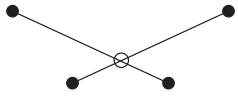
История этого утверждения, называемого *леммой о скрещиваниях*, довольно интересна. Как гипотезу его высказали Эрдёш и Гай в 1973 году [6] (с константой c вместо коэффициента $\frac{1}{64}$). Первые доказательства получили Лейтон в 1982 году [8] (с $\frac{1}{100}$ вместо $\frac{1}{64}$) и независимо Аджтай, Чватал, Ньюбери и Семереди [1]. Лемма о скрещиваниях оставалась малоизвестной (многие долго считали ее гипотезой даже после появления первоначальных доказательств), пока Ласло Секей [9] не продемонстрировал ее полезность в блестящей статье, применив ее к ряду экстремальных геометрических задач, казавшихся очень трудными. Приведенное ниже доказательство возникло при переписке по электронной почте между Бернардом Чазеллом, Мишей Шариром и Эмо Велзл, и оно, несомненно, принадлежит Книге.

■ **Доказательство.** Рассмотрим минимальную укладку графа G. Пусть p — число между 0 и 1 (выберем его позже). Построим случайный подграф G_p графа G, включая в него каждую вершину графа G независимо от остальных с вероятностью p.

Пусть n_p, m_p, X_p — случайные величины, равные числам вершин, ребер и скрещиваний в G_p соответственно. Так как $\mathrm{cr}(G) - m + 3n \geq 0$ для любого графа G в силу (4), то и для математического ожидания имеем

$$E(X_p - m_p + 3n_p) \geq 0.$$

Вычислим теперь математические ожидания $E(n_p)$, $E(m_p)$ и $E(X_p)$. Ясно, что $E(n_p) = pn$ и $E(m_p) = p^2 m$, поскольку ребро появляется в G_p тогда и только тогда, когда этот граф содержит оба его конца. Наконец, $E(X_p) = p^4 \mathrm{cr}(G)$, ибо пересечение ребер в G_p возникает тогда и только тогда, когда все четыре (разные!) конца ребер входят в G_p.



Поэтому в силу линейности математического ожидания

$$0 \leq E(X_p) - E(m_p) + 3E(n_p) = p^4 \mathrm{cr}(G) - p^2 m + 3pn,$$

что дает

$$\mathrm{cr}(G) \geq \frac{p^2 m - 3pn}{p^4} = \frac{m}{p^2} - \frac{3n}{p^3}. \qquad (5)$$

Теперь наступил решающий момент доказательства. Полагая $p := \frac{4n}{m}$ (согласно условию теоремы дробь не превосходит 1), приводим оценку (5) к виду

$$\mathrm{cr}(G) \geq \frac{1}{64}\left[\frac{4m}{(n/m)^2} - \frac{3n}{(n/m)^3}\right] = \frac{1}{64}\frac{m^3}{n^2},$$

и теорема доказана. □

Это доказательство доставило бы удовольствие Паулю Эрдёшу.

Литература

[1] Ajtai M., Chvátal V., Newborn M., Szemerédi E. *Crossing-free subgraphs.* Annals of Discrete Math., **12** (1982), 9–12.

[2] Alon N., Spencer J. *The Probabilistic Method.* Third edition, Wiley-Interscience, 2008. [См. примечание к [2] в гл. 36.]

[3] Erdős P. *Some remarks on the theory of graphs.* Bulletin Amer. Math. Soc., **53** (1947), 292–294.

[4] Erdős P. *Graph theory and probability.* Canadian J. Math., **11** (1959), 34–38.

[5] Erdős P. *On a combinatorial problem. I.* Nordisk Math. Tidskrift, **11** (1963), 5–10.

[6] Erdős P., Guy R. K. *Crossing number problems.* Amer. Math. Monthly, **80** (1973), 52–58.

[7] Erdős P., Rényi A. *On the evolution of random graphs.* Magyar Tud. Akad. Mat. Kut. Int. Közl., **5** (1960), 17–61.

[8] Leighton T. *Complexity Issues in VLSI.* MIT Press, Cambridge MA, 1983.

[9] Székely L. A. *Crossing numbers and hard Erdős problems in discrete geometry.* Combinatorics, Probability, and Computing, **6** (1997), 353–358.

[10*] Descartes B. *Solution to advanced problem № 4526.* Amer. Math. Monthly, **61** (1954), p. 352.


26.2.98

Об иллюстрациях

Мы благодарим Карла Хайнриха Хофманна из Дармштадта за предоставленную нам возможность иллюстрировать эту книгу его восхитительными оригинальными рисунками. Спасибо!

Правильные многогранники на с. 84 и выкройку нежесткого многогранника на с. 93 нарисовал Вольфганг А.Ф.Рупперт из Вены. Юрген Рихтер-Геберт (из Мюнхена) предоставил две иллюстрации для с. 86, а Рональд Воцлав создал прекрасную постскриптовскую графику для с. 144–145. На с. 242 изображен Вейсмановский музей искусств в Миннеаполисе, построенный по проекту Франка Гехри. Фотография его западного фасада сделана Крисом Фаустом. На плане изображена Галерея речных видов Долли Фитерман, находящаяся за западным фасадом.

Портреты Бертрана, Кантора, Эрдёша, Эйлера, Ферма, Герглотца, Эрмита, Гильберта, Пойа, Литтлвуда и Сильвестра публикуются по разрешению фотоархива Института математических исследований в Обервольфахе. (Мы крайне признательны Аннет Диш!)

Портрет Гаусса на с. 32 был опубликован в Astronomische Nachrichten в 1828 году и предоставлен Википедией; автор этой литографии — Зигфрид Детлев Бендиксен.

Изображение Эрмита взято из первого тома собрания его трудов.

Портрет Эйзенштейна приводится с любезного разрешения профессора Карин Райх из коллекции портретов Математического Общества Гамбурга.

Марки с портретами Бюффона, Чебышёва, Эйлера и Рамануджана взяты с веб-сайта математических марок http://jeff560.tripod.com Джеффа Миллера с его великодушного согласия.

Фотография Клода Шеннона предоставлена Музеем Массачусетского технологического института и воспроизводится с его согласия.

Портрет Кэли взят из «Фотоальбома Вейерштрасса» (под редакцией Рейнхарда Беллинга, издательство Vieweg, 1994), с согласия Библиотеки Искусств при Государственном музее прусской культуры в Берлине.

Портрет Коши воспроизведен с разрешения Собрания Парижской Политехнической Школы. Изображение Ферма взято из книги Стефана Хилдебрандта и Энтони Тромба «Экономная Вселенная. Образы и формы естественного мира», Springer-Verlag, Нью-Йорк, 1996.

Портрет Эрнста Витта взят из Journal für die Reine und Angewandte Mathematik, том 426 (1992 г.) с разрешения издательства Walter de Gruyter. Он был сделан около 1941 года.

Фотография Карола Борсука была сделана в 1967 году Айзеком Намиокой и воспроизводится с его согласия.

Мы благодарны доктору Петеру Шпернеру из Брауншвейга за портрет его отца, а также Вере Сос за фотографию Пауля Турана.

Благодарим Н. Алона за портрет А. Нилли!

Предметный указатель

Оглавление

Минимальные системные требования определяются соответствующими требованиями программы Adobe Reader версии не ниже 11-й для операционных систем Windows, Mac OS, Android, iOS, Windows Phone и BlackBerry; экран 10″

Научно-популярное электронное издание

Айгнер Мартин
Циглер Гюнтер

ДОКАЗАТЕЛЬСТВА ИЗ КНИГИ

Лучшие доказательства со времен Евклида до наших дней

Ведущий редактор *М. С. Стригунова*
Редактор *А. С. Попов*
Художественный редактор *Н. А. Новак*
Технический редактор *Е. В. Денюкова*
Оригинал-макет подготовлен *И. А. Зубковым, А. М. Зубковым* в пакете LaTeX 2_ε

Подписано к использованию 01.11.14.

Издательство «БИНОМ. Лаборатория знаний»
125167, Москва, проезд Аэропорта, д. 3
Телефон: (499) 157-5272
e-mail: binom@Lbz.ru, http://www.Lbz.ru

В книге приведены красивые и изящные доказательства многих результатов. Среди них:

- Бесконечность множества простых чисел
- Представление чисел в виде суммы двух квадратов
- Третья проблема Гильберта
- Теорема Коши о жесткости
- Гипотеза Борсука
- Теорема Пойа о многочленах
- Задача Бюффона об игле
- Формула Кэли для числа деревьев
- Задача Диница
- Задача о пяти красках для плоских графов
- Теорема Турана для графов

Мартин Айгнер и Гюнтер Циглер, основываясь на предложениях и рекомендациях Пауля Эрдёша, собрали много замечательных и удивительных результатов из различных областей математики (теории чисел, геометрии, анализа, комбинаторики, теории графов) и сумели с блеском изложить их полные, но краткие доказательства, которые используют неожиданные сочетания разнородных идей. Текст удачно дополняют со вкусом подобранные и специально для этой книги сделанные рисунки.

Цель «Доказательств из Книги» – не столько изложить какие-то части математических теорий, сколько предоставить читателю возможность насладиться изяществом математических рассуждений и почувствовать единство областей математики, кажущихся далекими друг от друга.

Из предисловия редактора перевода