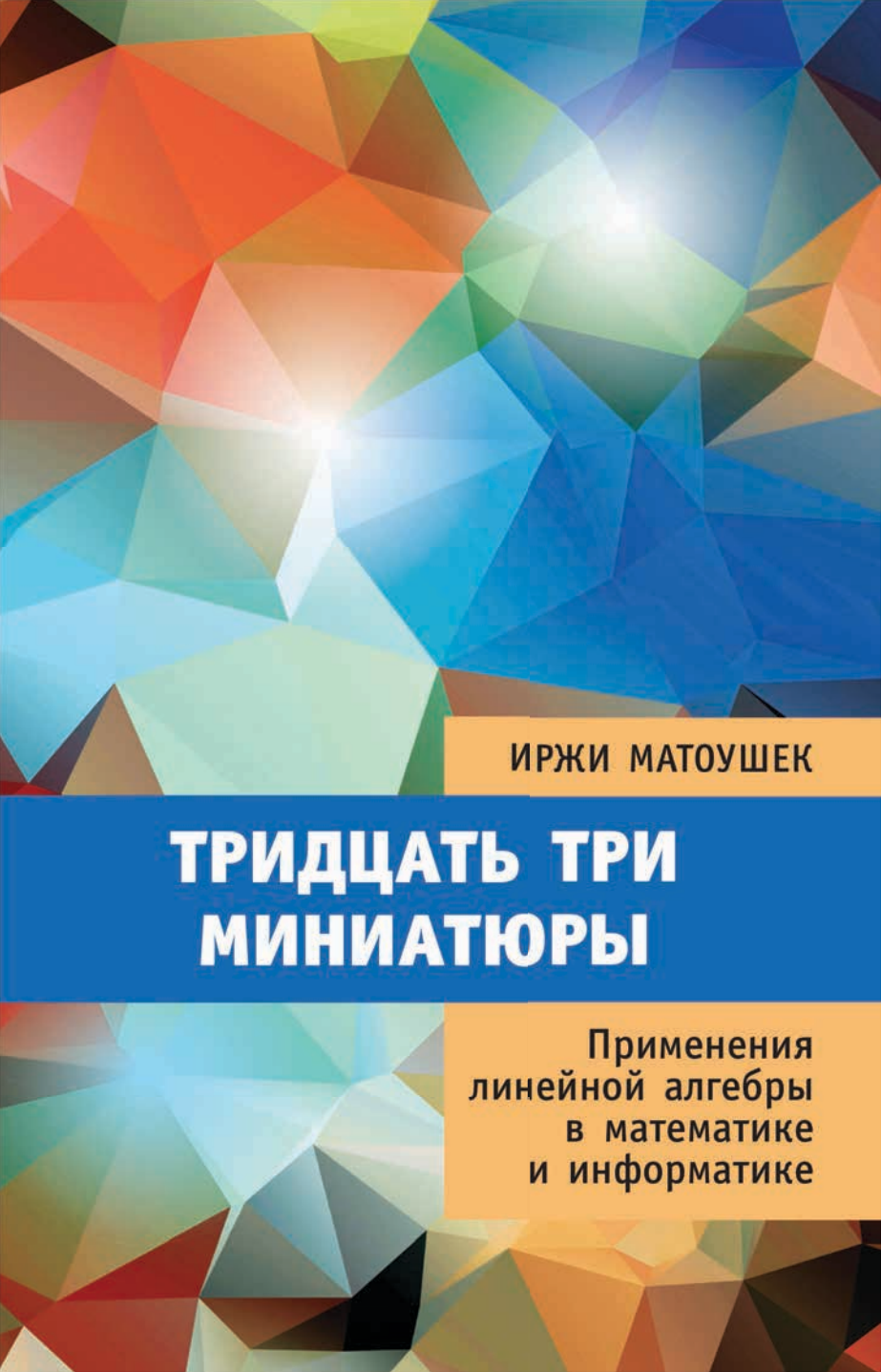

ИРЖИ МАТОУШЕК
ТРИДЦАТЬ ТРИ МИНИАТЮРЫ
Применения линейной алгебры в математике и информатике

Иржи Матоушек

Тридцать три миниатюры

Применения линейной алгебры в математике и информатике

Перевод с английского Б. Р. Френкина

Электронное издание

Москва
Издательство МЦНМО
2021

УДК 512.64
ББК 22.143
М34

Матоушек И.
Тридцать три миниатюры.
Применения линейной алгебры в математике и информатике.
Перевод с англ. Б. Р. Френкина.
Электронное издание.
М.: МЦНМО, 2021.
168 с.
ISBN 978-5-4439-3617-8

В книге собраны примеры остроумного применения линейной алгебры в различных областях математики — в основном в комбинаторике, геометрии и теории алгоритмов. Каждый раздел посвящён одному существенному результату, его мотивировке и доказательству. Для понимания требуется лишь некоторое знакомство с линейной алгеброй.

Книга содержит немало признанных математических жемчужин, в том числе коды Хэмминга, матричную теорему о деревьях, границу Ловаса для ёмкости Шеннона и контрпример к гипотезе Борсука. Представлены и менее известные, но не менее замечательные результаты; среди них быстрая проверка ассоциативности, лемма Штейница об упорядочении векторов, теорема о невозрастающих целочисленных разбиениях и применение внешнего произведения при рассмотрении пар множеств.

Сравнительно простые результаты из первых миниатюр дают богатый материал, заставляющий оживить в памяти вузовский курс линейной алгебры. Более трудные разделы можно использовать в курсе линейно-алгебраических методов для аспирантов.

Подготовлено на основе книги:
Матоушек И. Тридцать три миниатюры. Применения линейной алгебры в математике и информатике / Перевод с англ. Б. Р. Френкина. — М.: МЦНМО, 2021. — 168 с. — ISBN 978-5-4439-1617-0
Научно-популярное издание

6+

Издательство Московского центра
непрерывного математического образования
119002, Москва, Большой Власьевский пер., 11,
тел. (499)241-08-04.
http://www.mccme.ru

ISBN 978-5-4439-3617-8

Оглавление

Предисловие

Несколько лет назад я стал собирать примеры удачного применения линейной алгебры, и вот перед вами получившаяся коллекция. Эти примеры в основном принадлежат к главным сферам моих научных интересов — комбинаторике, геометрии и информатике. Большинство из них математические — относятся к доказательству теорем, но некоторые посвящены разумным способам вычислений, т. е. алгоритмам. Появление методов линейной алгебры часто оказывается неожиданным.

В некоторый момент я стал называть примеры из этой коллекции «миниатюрами». Потом я решил, что название «миниатюра» подходит, если полное изложение результата, с предварительными сведениями и всем прочим, занимает не больше четырёх печатных страниц (формата A4). Это правило абсолютно произвольно, как и многие другие правила, но в нём есть рациональное зерно — а именно, такой объём обычно без труда излагается за 90 минут (стандартная продолжительность лекции в университетах, где мне случалось преподавать). Разумеется, есть и отступления от этого правила, например шестистраничные миниатюры, которые я не смог заставить себя исключить.

Очевидно, коллекцию можно расширять до бесконечности, но я счёл, что тридцать три — достаточно удачное число, чтобы на нём остановиться.

Изложение предназначено в основном для лекторов (мне приходилось преподавать почти всё, что сюда включено), а также для студентов, которым интересны красивые математические идеи, даже если они требуют определённых размышлений. Надеюсь, что материал получился готовым для изучения, а подробности, предоставленные читателю, действительно не содержат каверз.

У читателя предполагается знание основ линейной алгебры, а также некоторое знакомство с многочленами и с терминологией геометрии и теории графов. Уровень трудности разных разделов различен, и в целом я их упорядочил, начиная от самых, по моему мнению, доступных и переходя к более трудным.

Я хотел сделать каждый раздел в основном независимым от других. При хорошей вузовской подготовке можно, например, начать

с раздела 24. Такой подход противоположен обычному построению учебника математики, где материал излагается последовательно и если надо понять что-то на странице 123, то обычно надо понять предыдущие 122 страницы или, если повезёт, подходящие 38.

Разумеется, «антиучебниковое» построение иногда приводит к скучным повторениям и, что, может быть, ещё более важно, накладывает ограничения на возможную степень освоения материала. С другой стороны, я верю, что здесь есть и преимущества: я бросил читать несколько учебников задолго до страницы 123, осознав, что между короткими, как правило, периодами чтения я не мог удержать в памяти ключевые определения (имеющие маленьких детей поймут, о чём я говорю).

Прочитав несколько разделов, читатель может усмотреть одинаковые схемы в некоторых доказательствах. Их можно долго обсуждать, но я решил исключить всякие общие рассуждения о линейно-алгебраических методах.

В этом тексте нет ничего оригинального, и некоторые примеры достаточно хорошо известны и появлялись во многих публикациях (а иногда и в других моих книгах). Ниже перечислено несколько основных источников. Я добавил также ссылки на исходные публикации, когда смог их найти. Однако я свёл исторические замечания к минимуму и уделил лишь ограниченное внимание происхождению обсуждаемых идей. (Приношу извинения авторам, чьи работы упомянуты в недостаточной степени или совсем не упомянуты, и прошу сообщать мне о таких случаях.)

Буду также признателен за сообщения об опечатках и предложения по улучшению изложения.

Дальнейшее чтение

Превосходным учебником может служить

> *Babai L.*, *Frankl P.* Linear Algebra Methods in Combinatorics (Preliminary version 2). Department of Computer Science, The University of Chicago, 1992.

К сожалению, эта книга никогда не публиковалась официально. С некоторым усилием её можно получить лишь в качестве записок лекций Чикагского университета. Она содержит некоторые темы, рассмотренные здесь, а также массу другого материала подобного рода и очень удачное изложение некоторых разделов линейной алгебры.

Алгебраической теории графов посвящены, например, книги

Biggs N. Algebraic Graph Theory. 2nd ed. Cambridge: Cambridge University Press, 1993

и

Godsil C., Royle G. Algebraic Graph Theory. New York: Springer, 2001.

Вероятностные алгоритмы в духе разделов 11 и 24 хорошо разобраны в книге

Motwani R., Raghavan P. Randomized Algorithms. Cambridge: Cambridge University Press, 1995.

Благодарности. За ценные комментарии к предварительным вариантам этой книги заслуживают благодарности Отфрид Чонг, Эстер Эзра, Нати Линиал, Яна Максова, Хелена Никлова, Ёсио Окамото, Павел Патак, Олег Пихурко, Зузана Сафернова и все те, кого я, может быть, забыл включить в этот список. Благодарю также Дэвида Уилсона за разрешение использовать его изображение случайного ромбического замощения в разделе 22, а также Дженнифер Райт Шарп за тщательное редактирование. Наконец, я признателен многочисленным сотрудникам Отделения прикладной математики Карлова университета в Праге и Института теоретической информатики Высшей технической школы в Цюрихе за превосходную рабочую обстановку.

Обозначения

В основном обозначения вводятся в тех разделах, где они используются. Здесь приведено несколько общих обозначений, не вполне унифицированных в литературе.

Множество целых чисел обозначается $\mathbb{Z}$, множество рациональных чисел — $\mathbb{Q}$, множество вещественных чисел — $\mathbb{R}$, а $\mathbb{F}_q$ обозначает конечное поле из q элементов.

Матрица, транспонированная к матрице A, обозначается A^T. Элементы матрицы A обозначаются a_{ij}, и аналогично для остальных букв латинского алфавита. Векторы обозначаются жирным шрифтом: $\mathbf{v}$, $\mathbf{x}$, $\mathbf{y}$ и так далее. Если $\mathbb{K}$ — некоторое поле, а $\mathbf{x}$ — вектор из $\mathbb{K}^n$, то его i-я компонента обозначается x_i, т. е. $\mathbf{x} = (x_1, x_2, \ldots, x_n)$.

Через $\langle \mathbf{x}, \mathbf{y} \rangle$ мы обозначаем скалярное (внутреннее) произведение векторов $\mathbf{x}, \mathbf{y} \in \mathbb{K}^n$: $\langle \mathbf{x}, \mathbf{y} \rangle = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n$. Иногда мы будем рассматривать векторы $\mathbf{x}, \mathbf{y}$ как $(n \times 1)$-матрицы, и тогда $\langle \mathbf{x}, \mathbf{y} \rangle$ можно записать как $\mathbf{x}^T \mathbf{y}$. Если $\mathbf{x} \in \mathbb{R}^n$, то $||\mathbf{x}|| = \langle \mathbf{x}, \mathbf{x} \rangle^{1/2}$ — евклидова норма (длина) вектора $\mathbf{x}$.

Графы считаются простыми и неориентированными, если не оговорено противное; это значит, что граф G рассматривается как множество пар (V, E), где V — множество вершин, E — множество рёбер, т. е. некоторых неупорядоченных пар элементов из V. Иногда мы будем обозначать множества вершин и рёбер графа G через $V(G)$ и $E(G)$ соответственно.

Некоторые соглашения. Определения важнейших понятий выделяются в тексте **жирным шрифтом**, чтобы легче было их находить. Менее важные определения, а также общие математические понятия, если они только упоминаются, выделены *курсивом*.

Миниатюра 1

Числа Фибоначчи — быстрое вычисление

Числа Фибоначчи $F_0, F_1, F_2, \ldots$ определяются формулами $F_0 = 0$, $F_1 = 1$ и $F_{n+2} = F_{n+1} + F_n$ при $n = 0, 1, 2, \ldots$ Ясно, что можно вычислить F_n примерно за n арифметических операций.

Следующий приём позволяет сократить вычисления и использовать лишь порядка $\log n$ арифметических операций. Рассмотрим (2×2)-матрицу $M := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Тогда

$$\begin{pmatrix} F_{n+2} \\ F_{n+1} \end{pmatrix} = M \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix},$$

а значит, $\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = M^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ (мы воспользовались ассоциативностью умножения матриц).

При $n = 2^k$ можно вычислить M^n, несколько раз возводя матрицу в квадрат. Потребуется k умножений (2×2)-матриц. Произвольное n запишем в двоичном виде: $n = 2^{k_1} + 2^{k_2} + \ldots + 2^{k_t}$, $k_1 < k_2 < \ldots < k_t$, а затем вычислим M^n по формуле $M^n = M^{2^{k_1}} M^{2^{k_2}} \ldots M^{2^{k_t}}$. Потребуется не более $2k_t \leqslant 2\log_2 n$ умножений (2×2)-матриц.

Замечания. Аналогичный приём можно применить к любой последовательности $(y_0, y_1, y_2, \ldots)$, заданной рекуррентным соотношением $y_{n+k} = a_{k-1}y_{n+k-1} + \ldots + a_0 y_n$, где k и $a_0, a_1, \ldots, a_{k-1}$ — константы.

При вычислении чисел Фибоначчи таким методом нужна аккуратность, поскольку F_n растёт очень быстро. Из формулы для F_n в миниатюре 2 можно видеть, что количество десятичных знаков в F_n имеет порядок n. Поэтому нужно использовать арифметику высокой точности, так что арифметические операции будут выполняться довольно медленно.

Литература

Этот приём хорошо известен, но до сих пор я не нашёл указаний на его происхождение.

Миниатюра 2

Числа Фибоначчи — формула

Выведем формулу для n-го числа Фибоначчи F_n (где $F_0 = 0$, $F_1 = 1$ и $F_{n+2} = F_{n+1} + F_n$ при $n = 0, 1, 2, \ldots$). Рассмотрим векторное пространство всех бесконечных последовательностей $\mathbf{x} = (x_0, x_1, x_2, \ldots)$ вещественных чисел (с покоординатным сложением, а также умножением на вещественные числа). В этом пространстве рассмотрим подпространство W всех последовательностей $\mathbf{x}$, удовлетворяющих уравнению $x_{n+2} = x_{n+1} + x_n$ при всех $n = 0, 1, \ldots$ Любой выбор первых двух членов x_0 и x_1 однозначно задаёт последовательность из W, поэтому $\dim(W) = 2$. (В частности, базис для W составляют две последовательности, начинающиеся с $(0, 1, 1, 2, 3, \ldots)$ и с $(1, 0, 1, 1, 2\ldots)$.)

Найдём теперь другой базис в W: это две последовательности, заданные простой формулой. Для этого потребуется «наитие»: попробуем найти их среди последовательностей $\mathbf{u} \in W$ вида $u_n = \tau^n$ для подходящего вещественного числа τ.

Нужные значения τ должны удовлетворять квадратному уравнению $\tau^2 = \tau + 1$, имеющему два различных корня

$$\tau_1 = \frac{1+\sqrt{5}}{2} \quad \text{и} \quad \tau_2 = \frac{1-\sqrt{5}}{2}.$$

Последовательности $\mathbf{u} := (\tau_1^0, \tau_1^1, \tau_1^2, \ldots)$ и $\mathbf{v} := (\tau_2^0, \tau_2^1, \tau_2^2, \ldots)$ принадлежат W и, как легко убедиться, линейно независимы (для проверки рассмотрим первые два члена). Значит, они составляют базис в W.

Разложим последовательность чисел Фибоначчи $\mathbf{F} := (F_0, F_1, \ldots)$ по этому базису: $\mathbf{F} = \alpha\mathbf{u} + \beta\mathbf{v}$. Коэффициенты α, β определяются по первым двум членам последовательностей; таким образом, нужно решить линейную систему $\alpha\tau_1^0 + \beta\tau_2^0 = F_0$, $\alpha\tau_1^1 + \beta\tau_2^1 = F_1$.

В результате получаем формулу

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

Замечательно, что эта формула, полная иррациональностей, при любом n задаёт целое число.

Аналогичные приёмы годятся для других рекуррентных последовательностей вида $y_{n+k} = a_{k-1}y_{n+k-1} + \ldots + a_0 y_n$, но в некоторых случаях добавляются усложнения. Например, если $y_{n+2} = 2y_{n+1} - y_n$, то потребуется найти базис другого вида, чего мы здесь делать не будем.

Литература

Вышеприведённую формулу для F_n иногда называют *формулой Бине*, но её знали Даниил Бернулли, Эйлер и Муавр в XVIII веке, до работы Бине. Более естественный способ вывода этой формулы использует производящие функции, но их правильное применение «с чистого листа» требует большей работы.

Миниатюра 3

Клубы Нечётнограда

В Нечётнограде ровно n жителей. Их главное занятие — создавать различные клубы, и в некоторый момент это стало угрожать самому существованию города. Чтобы ограничить количество клубов, городской совет принял следующие правила, с виду безобидные.

- Каждый клуб должен иметь *нечётное* количество членов.
- Каждые два клуба должны иметь *чётное* количество общих членов.

Теорема. *При соблюдении указанных правил невозможно создать больше чем n клубов, где n — количество жителей в городе.*

Доказательство. Обозначим жителей $1, 2, \ldots, n$, а клубы — C_1, C_2, …, C_m. Зададим $(m \times n)$-матрицу A, положив

$$a_{ij} = \begin{cases} 1 & \text{при } j \in C_i, \\ 0 & \text{в противном случае.} \end{cases}$$

(Таким образом, строки соответствуют клубам, а столбцы — жителям.)

Рассмотрим такую матрицу A над двухэлементным полем $\mathbb{F}_2$. Ясно, что её ранг не превосходит n.

Теперь посмотрим на произведение AA^T. Это $(m \times m)$-матрица, где в позиции (i, k) стоит $\sum_{j=1}^{n} a_{ij}a_{kj}$, т. е. количество жителей в $C_i \cap C_k$. Точнее, поскольку мы теперь имеем дело с $\mathbb{F}_2$, элемент матрицы равен 1, если $|C_i \cap C_k|$ нечётно, и равен 0, если $|C_i \cap C_k|$ чётно.

Из правил городского совета вытекает, что $AA^T = I_m$, где I_m — единичная матрица. Поэтому ранг матрицы AA^T не меньше m. Так как ранг произведения матриц не превосходит минимума рангов сомножителей[1], получаем, что $\operatorname{rank}(A) \geqslant m$, поэтому $m \leqslant n$. Теорема доказана. □

[1] Набросок доказательства: пусть $C = AB$ — произведение двух матриц, тогда каждая строка из C является линейной комбинацией строк из B, поэтому пространство строк из C содержится в пространстве строк из B. Ранг матрицы — это размерность пространства её строк, поэтому $\operatorname{rank}(C) \leqslant \operatorname{rank}(B)$. Неравенство $\operatorname{rank}(C) \leqslant \operatorname{rank}(A)$ вытекает из аналогичного рассуждения для пространств столбцов.

Литература

С этого примера начинается книга Бабая и Франкла, упомянутая в предисловии[1]. Не уверен, что он ранее появлялся «в чистом виде», но бесспорно это частный случай других результатов, например неравенства Франкла — Уилсона (см. миниатюру 17).

[1] См. с. 6. — *Прим. перев.*

Миниатюра 4

Пересечения одинакового размера

Теорема (обобщённое неравенство Фишера). *Пусть $C_1, C_2, \ldots, C_m$ — различные непустые подмножества n-элементного множества, причём все их пересечения $C_i \cap C_j$, $i \neq j$, содержат одинаковое количество элементов. Тогда $n \geqslant m$.*

Результат и его доказательство аналогичны миниатюре 3.

Доказательство. Пусть t — размер каждого из пересечений $C_i \cap C_j$, $i \neq j$. Вначале рассмотрим случай, когда одно из C_i, например C_1, имеет размер t. Тогда $t \geqslant 1$ и C_1 содержится в каждом из остальных C_j. Значит, $C_i \cap C_j = C_1$ для всех $i, j \geqslant 2$, $i \neq j$. Тогда все множества $C_i \setminus C_1$, $i \geqslant 2$, не пересекаются и непусты, поэтому их количество не превосходит $n - |C_1| \leqslant n - 1$. Таким образом, вместе с C_1 имеется не более n множеств.

Пусть теперь $d_i := |C_i| > t$ для всех i. Как и в миниатюре 3, зададим $(m \times n)$-матрицу A, положив

$$a_{ij} = \begin{cases} 1 & \text{при } j \in C_i, \\ 0 & \text{в противном случае.} \end{cases}$$

На этот раз будем считать элементы из A вещественными числами, и пусть $B := AA^T$. Тогда

$$B = \begin{pmatrix} d_1 & t & t & \ldots & t \\ t & d_2 & t & \ldots & t \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ t & t & t & \ldots & d_m \end{pmatrix},$$

где $t \geqslant 0$ и $d_1, d_2, \ldots, d_m > t$. Остаётся проверить, что матрица B невырожденна; тогда $m = \operatorname{rank}(B) \leqslant \operatorname{rank}(A) \leqslant n$ и теорема доказана.

Невырожденность матрицы B можно проверить рутинным способом, приведя B к треугольному виду методом Гаусса.

Вот другой способ. Покажем, что матрица B **положительно определённа**; это означает, что B симметрична и $\mathbf{x}^T B\mathbf{x} > 0$ для всех ненулевых $\mathbf{x} \in \mathbb{R}^m$.

Можно записать $B = tJ_n + D$, где J_n — матрица из единиц, а D — диагональная матрица с числами $d_1 - t, d_2 - t, \ldots, d_n - t$ на диагонали.

Пусть $\mathbf{x}$ — произвольный ненулевой вектор из $\mathbb{R}^n$. Ясно, что D — положительно определённая матрица, так как

$$\mathbf{x}^T D\mathbf{x} = \sum_{i=1}^{n} (d_i - t)x_i^2 > 0.$$

Далее,

$$\mathbf{x}^T J_n \mathbf{x} = \sum_{i,j=1}^{n} x_i x_j = \left(\sum_{i=1}^{n} x_i\right)^2 \geqslant 0,$$

т. е. J_n — *положительно полуопределённая матрица*. Наконец,

$$\mathbf{x}^T B\mathbf{x} = \mathbf{x}^T (tJ_n + D)\mathbf{x} = t\mathbf{x}^T J_n \mathbf{x} + \mathbf{x}^T D\mathbf{x} > 0;$$

это пример общей ситуации: сумма положительно определённой и положительно полуопределённой матрицы является положительно определённой матрицей.

Итак, B — положительно определённая матрица. Остаётся убедиться, что все положительно определённые матрицы невырожденны. Для этого достаточно заметить, что если $B\mathbf{x} = \mathbf{0}$, то $\mathbf{x}^T B\mathbf{x} = \mathbf{x}^T \mathbf{0} = 0$ и потому $\mathbf{x} = \mathbf{0}$. □

Литература

В меньшей общности неравенство появилось в статье

Fisher R. A. An examination of the different possible solutions of a problem in incomplete blocks // Ann. Eugenics. 1940. V. 10. P. 52—75.

Линейно-алгебраическое доказательство «однородного» варианта неравенства Фишера содержится в заметке

Bose R. C. A note on Fisher's inequality for balanced incomplete block designs // Ann. Math. Statistics. 1949. V. 20, № 4. P. 619—620.

Неоднородный вариант, рассмотренный выше, был отмечен в статье

Majumdar K. N. On some theorems in combinatorics relating to incomplete block designs // Ann. Math. Statistics. 1953. V. 24. P. 377—389.

Он был переоткрыт в работе

Isbell J. R. An inequality for incidence matrices // Proc. Amer. Math. Soc. 1959. V. 10. P. 216—218.

Миниатюра 5

Коды, исправляющие ошибки

Допустим, мы хотим передать (или записать, или прочитать) некие данные, скажем, строку $\mathbf{v}$ из нулей и единиц. Передающий канал не вполне надёжен, так что могут случиться ошибки — некоторые нули будут восприняты как единицы или наоборот. Пусть вероятность ошибки мала, причём вероятность k ошибок в сообщении существенно меньше, чем вероятность $k-1$ или меньшего количества ошибок.

Главная идея кодов, исправляющих ошибки, состоит в том, чтобы вместо исходного сообщения $\mathbf{v}$ послать более длинное сообщение $\mathbf{w}$. Строка $\mathbf{w}$ строится так, что мы можем исправить небольшое количество ошибок, случившихся при передаче.

Сегодня коды, исправляющие ошибки, применяются в устройствах многих видов, от CD-плееров до космических кораблей, а построение таких кодов составляет обширную область исследований. Здесь мы введём основные определения и опишем изящную конструкцию такого кода, основанную на линейной алгебре.

Рассмотрим следующую конкретную задачу. Мы хотим посылать произвольные четырёхбитовые строки $\mathbf{v}$ вида $abcd$, где $a, b, c, d \in \in \{0, 1\}$. Мы предполагаем, что вероятность двух или более ошибок при передаче незначительна, но одна ошибка может появиться с заметной ненулевой вероятностью и мы хотим исправлять эту ошибку.

Один из способов исправить единственную ошибку — утроить каждый бит и послать строку $\mathbf{w} = aaabbbcccddd$ (12 битов). Например, вместо $\mathbf{v} = 1011$ мы посылаем $\mathbf{w} = 111000111111$. Если на другом конце канала получено, скажем, 110000111111, то мы знаем, что ошибка была в третьем бите и правильная строка имела вид 111000111111 (разумеется, если всё же не было двух или больше ошибок).

Это довольно неэффективный способ кодирования. Мы увидим, что можно исправить единственную ошибку в любом бите, используя код, который преобразует 4-битовую строку в 7-битовую. Так что сообщение растягивается не в три раза, а лишь на 75 %.

Пример: код Хэмминга. Вероятно, это первый известный нетривиальный пример кода, исправляющего ошибки. Он был открыт в 1950-х годах. Вместо данной 4-битовой строки $\mathbf{v} = abcd$ мы посылаем 7-битовую строку $\mathbf{w} = abcdefg$, где $e := a + b + c$ (сложение по модулю 2), $f := a + b + d$ и $g := a + c + d$. Например, если $\mathbf{v} = 1011$, то $\mathbf{w} = 1011001$. Такое кодирование позволяет исправить любую ошибку в одном бите, что мы и покажем с помощью линейной алгебры.

Прежде чем приступить к этому, введём некоторые общие определения из теории кодирования. Пусть S — конечное множество, которое называется **алфавитом**; например, можно взять $S = \{0, 1\}$ или $S = \{a, b, c, \ldots, z\}$. Через $S^n = \{\mathbf{w} = a_1 a_2 \ldots a_n : a_1, \ldots, a_n \in S\}$ будем обозначать множество всех возможных слов длины n (здесь **слово** означает любую конечную последовательность букв алфавита).

Определение. Код длины n над алфавитом S — это произвольное подмножество $C \subseteq S^n$.

Например, в случае кода Хэмминга мы имеем $S = \{0, 1\}$, $n = 7$, а C — множество всех 7-битовых слов, которые получаются вышеописанным способом из всех $2^4 = 16$ возможных 4-битовых слов. Таким образом, $C = \{0000000, 0001011, 0010101, 0011110, 0100110, 0101101, 0110011, 0111000, 1000111, 1001100, 1010010, 1011001, 1100001, 1101010, 1110100, 1111111\}$.

Важное свойство этого кода состоит в том, что любые два его слова различаются как минимум в трёх битах. Возможна прямая, но трудоёмкая проверка этого факта через попарное сравнение всех слов из C. Вскоре мы докажем то же самое по-другому и почти без усилий.

Введём следующую терминологию:

- **расстояние Хэмминга** между двумя словами $\mathbf{u}, \mathbf{v} \in S^n$ равно

$$d(\mathbf{u}, \mathbf{v}) := |\{i : u_i \neq v_i, i = 1, 2, \ldots, n\}|,$$

  где u_i обозначает i-ю букву слова $\mathbf{u}$. Это означает, что можно получить $\mathbf{v}$, сделав $d(\mathbf{u}, \mathbf{v})$ «ошибок» в слове $\mathbf{u}$;
- код C **исправляет t ошибок**, если для любого $\mathbf{u} \in S^n$ существует не более одного такого $\mathbf{v} \in C$, что $d(\mathbf{u}, \mathbf{v}) \leqslant t$;
- **кодовое расстояние** кода C определяется как

$$d(C) := \min\{d(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in C, \mathbf{u} \neq \mathbf{v}\}.$$

Легко проверить, что последние два понятия связаны следующим образом: *код C исправляет t ошибок в точности тогда, когда*

$d(C) \geqslant 2t+1$. Таким образом, чтобы показать, что код Хэмминга исправляет одну ошибку, нужно доказать, что $d(C) \geqslant 3$.

Кодирование и декодирование. Вышеприведённое определение кода может показаться странным, поскольку в повседневной жизни слово «код» относится к методу кодирования сообщений. На самом деле для реального использования кода C из этого определения требуется ещё инъективное отображение $c\colon \Sigma^k \to C$, где Σ — алфавит исходного сообщения, k — его длина (или длина передаваемого блока символов).

По данному сообщению $\mathbf{v} \in \Sigma^k$ мы вычисляем слово $\mathbf{w} = c(\mathbf{v}) \in C$ и посылаем его. Затем, получив слово $\mathbf{w}' \in S^n$, мы находим слово $\mathbf{w}'' \in C$ с минимальным $d(\mathbf{w}', \mathbf{w}'')$ и по нему вычисляем

$$\mathbf{v}' = c^{-1}(\mathbf{w}'') \in \Sigma^k.$$

Если при передаче появилось не больше t ошибок и C исправляет t ошибок, то $\mathbf{w}'' = \mathbf{w}$ и потому $\mathbf{v}' = \mathbf{v}$. Иными словами, мы восстановили исходное сообщение.

Одна из главных задач теории кодирования — найти для данных S, t и n код C длины n над алфавитом S с условием $d(C) \geqslant t$, содержащий как можно больше слов (чем больше $|C|$, тем больше различной информации можно передать).

Нужно также сравнивать качество кодов с различными $|S|$, t, n. Такие вопросы изучает *теория информации Шеннона*, которой мы здесь не будем заниматься.

При построении кода нужно учитывать, кроме размера, и другие параметры кода, например скорость кодирования и декодирования.

Линейные коды. Линейные коды — это коды специального вида, и код Хэмминга — один из них. В данном случае алфавит S — конечное поле (важнейшим примером служит $S = \mathbb{F}_2$), так что S^n является векторным пространством над S. Каждое линейное подпространство в S^n называется **линейным кодом**.

Наблюдение. Для любого линейного кода C выполнено равенство

$$d(C) = \min\{d(\mathbf{0}, \mathbf{w})\colon \mathbf{w} \in C, \mathbf{w} \neq \mathbf{0}\}. \qquad \square$$

Не обязательно представлять линейный код как список слов. Линейная алгебра предлагает два основных способа задать линейное подпространство. Вот первый из них.

(1) *Задание базиса.* Можно задать C **порождающей матрицей** G. Это $(k\times n)$-матрица, $k := \dim(C)$, и её строки составляют базис подпространства C.

Порождающая матрица очень полезна при кодировании. Если нужно передать вектор $\mathbf{v}\in S^k$, мы посылаем вектор $\mathbf{w} := G^T\mathbf{v}\in C$.

Выбрав подходящий базис в C, всегда можно привести порождающую матрицу к виду $G = (I_k \mid A)$, где I_k обозначает единичную $(k \times k)$-матрицу. Тогда вектор $\mathbf{w}$ совпадает с $\mathbf{v}$ по первым k компонентам. Это значит, что процедура кодирования добавляет к исходному сообщению $n-k$ дополнительных символов[1]. (Иногда их называют *битами проверки чётности*, что оправдано для случая $S=\mathbb{F}_2$: каждый такой бит является линейной комбинацией некоторых битов исходного сообщения и, таким образом, «проверяет их чётность».) Важно понимать, что передающий канал не делает различия между исходным сообщением и проверочными символами; ошибки могут возникнуть где угодно, в том числе и в проверочных символах.

Рассмотренный нами код Хэмминга — это линейный код длины 7 над $\mathbb{F}_2$ с порождающей матрицей

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

А теперь — другой способ задания линейного кода.

(2) *Задание линейными уравнениями.* Линейный код C можно также задать как множество всех решений системы линейных уравнений вида $P\mathbf{w} = \mathbf{0}$, где P называется **проверочной матрицей** кода C.

Как мы увидим, такой способ задания кода особенно полезен при декодировании. Если порождающая матрица кода C имеет вид $G = (I_k \mid A)$, то, как нетрудно убедиться, проверочная матрица равна $P := (-A^T \mid I_{n-k})$.

[1] Обычно их называют *проверочными символами. — Прим. перев.*

Обобщённый код Хэмминга. Код Хэмминга имеет проверочную матрицу

$$P = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Её столбцы — в точности все ненулевые векторы из $\mathbb{F}_2^3$. Эту конструкцию можно обобщить: выберем параметр $\ell \geqslant 2$ и определим **обобщённый код Хэмминга** как линейный код над $\mathbb{F}_2$ длины $n := 2^\ell - 1$ с проверочной матрицей P, столбцы которой — все ненулевые векторы из $\mathbb{F}_2^\ell$.

Предложение. *Обобщённый код Хэмминга C имеет кодовое расстояние $d(C) = 3$ и, таким образом, исправляет одну ошибку.*

Доказательство. Чтобы показать, что $d(C) \geqslant 3$, достаточно проверить, что любой ненулевой вектор $\mathbf{w} \in C$ имеет не меньше трёх ненулевых компонент. Таким образом, требуется, чтобы никакой вектор $\mathbf{w} \in \mathbb{F}_2^n$ с одной или двумя единицами не удовлетворял условию $P\mathbf{w} = \mathbf{0}$. В случае одной единицы это условие означает, что P имеет нулевой столбец, а в случае двух единиц два столбца должны быть равны. Ни то ни другое невозможно[1]. □

Отметим, что (обобщённый) код Хэмминга оптимален в следующем смысле: не существует кода в $C \subseteq \mathbb{F}_2^{2^\ell - 1}$ с кодовым расстоянием не меньше 3 и с количеством слов больше, чем у обобщённого кода Хэмминга. Доказательство предоставляется в качестве (нетривиального) упражнения.

Декодирование обобщённого кода Хэмминга. Мы посылаем вектор $\mathbf{w}$ обобщённого кода Хэмминга и получаем $\mathbf{w}'$. Если случилось не более одной ошибки, то $\mathbf{w}' = \mathbf{w}$ или $\mathbf{w}' = \mathbf{w} + \mathbf{e}_i$ для некоторого $i \in \{1, 2, \ldots, n\}$, где i-я компонента вектора $\mathbf{e}_i$ равна 1, а остальные равны 0.

Рассмотрим произведение $P\mathbf{w}'$. Если $\mathbf{w}' = \mathbf{w}$, то $P\mathbf{w} = \mathbf{0}$, а если $\mathbf{w}' = \mathbf{w} + \mathbf{e}_i$, то $P\mathbf{w}' = P\mathbf{w} + P\mathbf{e}_i = P\mathbf{e}_i$, но это i-й столбец матрицы P. Если предполагать, что было не больше одной ошибки, то можно немедленно сказать, была ли ошибка и если да, то в каком месте.

[1] Невозможность неравенства $d(C) > 3$ вытекает из того, что столбец матрицы P равен сумме двух других столбцов. Если номера этих столбцов равны соответственно i, j, k, то $P\mathbf{w} = 0$ для вектора $\mathbf{w}$, у которого компоненты с номерами i, j, k равны единице, а остальные равны нулю. — *Прим. перев.*

Литература

Hamming R. W. Error detecting and error correcting codes // Bell System Tech. J. 1950. V. 29. P. 147—160.

Как отмечено выше, изучение кодов, исправляющих ошибки, составляет обширную область и по ней существует много учебников[1]. Хорошей отправной точкой, хотя не на все вкусы, может служить работа

Sudan M. Coding theory: Tutorial & survey // Proc. 42nd Annual Symposium on Foundations of Computer Science (FOCS). 2001. P. 36—53, `http://madhu.seas.harvard.edu/papers/2001/focs01-tut.pdf`.

[1] Один из наиболее фундаментальных источников по теории кодирования — *MacWilliams M. J., Sloane N. J. A.* The Theory of Error-Correcting Codes. North-Holland Publishing Company. 1977. Рус. перевод: *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь. 1979. — *Прим. перев.*

Миниатюра 6

Нечётные расстояния

Теорема. *Не существует четырёх точек на плоскости, попарные расстояния между которыми выражаются нечётными целыми числами.*

Доказательство. Предположим, напротив, что существуют четыре точки с нечётными попарными расстояниями. Можно считать, что одна из них соответствует нулевому вектору $\mathbf{0}$; остальные обозначим $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$. Тогда $\|\mathbf{a}\|$, $\|\mathbf{b}\|$, $\|\mathbf{c}\|$, $\|\mathbf{a}-\mathbf{b}\|$, $\|\mathbf{b}-\mathbf{c}\|$ и $\|\mathbf{c}-\mathbf{a}\|$ — нечётные целые числа, где $\|\mathbf{x}\|$ обозначает евклидову длину вектора $\mathbf{x}$.

Заметим, что если m — нечётное целое число, то $m^2 \equiv 1 \pmod 8$ (здесь $\equiv$ обозначает сравнимость: $x \equiv y \pmod k$ означает, что $x-y$ делится на k). Значит, квадраты всех рассматриваемых расстояний сравнимы с 1 по модулю 8.

Теперь воспользуемся *теоремой косинусов*, согласно которой для любых векторов $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ выполнено равенство

$$\|\mathbf{x}-\mathbf{y}\|^2 = \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2 - 2\langle \mathbf{x}, \mathbf{y}\rangle.$$

Применив её при $\mathbf{x}=\mathbf{a}$ и $\mathbf{y}=\mathbf{b}$, получаем

$$2\langle \mathbf{a}, \mathbf{b}\rangle = \|\mathbf{a}\|^2 + \|\mathbf{b}\|^2 - \|\mathbf{a}-\mathbf{b}\|^2 \equiv 1 \pmod 8,$$

и аналогичные формулы верны для $2\langle \mathbf{a}, \mathbf{c}\rangle$ и $2\langle \mathbf{b}, \mathbf{c}\rangle$.

Пусть B обозначает матрицу

$$\begin{pmatrix} \langle \mathbf{a}, \mathbf{a}\rangle & \langle \mathbf{a}, \mathbf{b}\rangle & \langle \mathbf{a}, \mathbf{c}\rangle \\ \langle \mathbf{b}, \mathbf{a}\rangle & \langle \mathbf{b}, \mathbf{b}\rangle & \langle \mathbf{b}, \mathbf{c}\rangle \\ \langle \mathbf{c}, \mathbf{a}\rangle & \langle \mathbf{c}, \mathbf{b}\rangle & \langle \mathbf{c}, \mathbf{c}\rangle \end{pmatrix}.$$

Тогда $2B$ сравнимо по модулю 8 с матрицей

$$R := \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}.$$

При этом $\det(R) = 4$ и, следовательно, $\det(2B) \equiv 4 \pmod 8$. (Чтобы убедиться в последнем, разложим оба определителя в сумму 3!

слагаемых согласно определению и заметим, что соответствующие слагаемые в $\det(2B)$ и в $\det(R)$ сравнимы по модулю 8.) Значит, $\det(2B) \neq 0$, а тогда и $\det(B) \neq 0$. Поэтому $\operatorname{rank}(B) = 3$.

С другой стороны, $B = A^T A$, где

$$A = \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix}.$$

При этом $\operatorname{rank}(A) \leqslant 2$, но хорошо известно, что ранг произведения матриц не превосходит минимума из рангов сомножителей (см. миниатюру 3). Значит, $\operatorname{rank}(B) \leqslant 2$, и это противоречие завершает доказательство. □

Литература

Этот результат взят из статьи

Graham R. L., *Rothschild B. L.*, *Straus E. G.* Are there $n+2$ points in E^n with pairwise odd integral distances? // Amer. Math. Monthly. 1974. V. 81. P. 21—25.

Приведённое выше доказательство сообщил мне Моше Розенфельд.

Миниатюра 7

Евклидовы ли эти расстояния?

Найдутся ли на плоскости три точки $\mathbf{p}, \mathbf{q}, \mathbf{r}$ с попарными евклидовыми расстояниями, равными 1? Разумеется, да — это вершины равностороннего треугольника.

А найдутся ли $\mathbf{p}, \mathbf{q}, \mathbf{r}$, для которых $\|\mathbf{p}-\mathbf{q}\|=\|\mathbf{q}-\mathbf{r}\|=1$ и $\|\mathbf{p}-\mathbf{r}\|=3$? Нет, поскольку прямой путь из $\mathbf{p}$ в $\mathbf{r}$ не может быть длиннее, чем путь через $\mathbf{q}$; такие расстояния противоречили бы **неравенству треугольника**, которое в евклидовом случае утверждает, что

$$\|\mathbf{p}-\mathbf{r}\| \leqslant \|\mathbf{p}-\mathbf{q}\|+\|\mathbf{q}-\mathbf{r}\|$$

для любых трёх точек $\mathbf{p}, \mathbf{q}, \mathbf{r}$ (в любом евклидовом пространстве).

В случае трёх точек неравенство треугольника оказывается *единственным* препятствием: для любых неотрицательных вещественных чисел x, y, z, удовлетворяющих условиям $x \leqslant y+z$, $y \leqslant x+z$, $z \leqslant x+y$, найдутся такие $\mathbf{p}, \mathbf{q}, \mathbf{r} \in \mathbb{R}^2$, для которых $\|\mathbf{p}-\mathbf{q}\|=x$, $\|\mathbf{q}-\mathbf{r}\|=y$ и $\|\mathbf{p}-\mathbf{r}\|=z$. Это общеизвестные условия существования треугольника с заданными длинами сторон.

Какие расстояния допустимы в случае четырёх точек? Эти точки следует искать в трёхмерном пространстве, т. е. нас интересует тетраэдр с данными длинами рёбер. Неравенство треугольника здесь служит необходимым, но не достаточным условием. Например, расстояния, указанные на рис. 1, не противоречат неравенству треугольника, однако не существует соответствующих $\mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{s} \in \mathbb{R}^3$. Это можно увидеть геометрически: если построен треугольник $\mathbf{pqr}$,

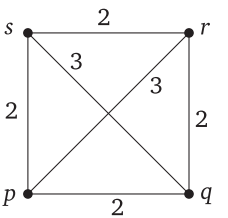


Рис. 1

то сферы с центрами **p**, **q**, **r**, которые должны содержать **s**, в действительности не имеют общей точки.

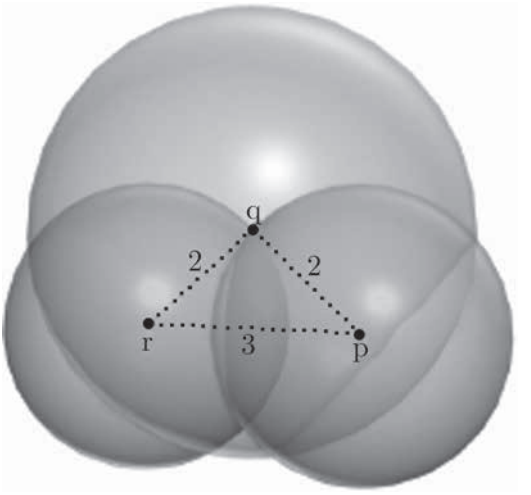


Рис. 2

Это рассуждение пригодно в довольно частном случае. Линейная алгебра даёт весьма изящную характеризацию наборов чисел, которые могут появиться в качестве наборов евклидовых попарных расстояний. Для этого используется понятие *положительно полуопределённой матрицы*[1]. Такая характеризация пригодна для любого количества точек; если количество равно $n+1$, то мы считаем их точками в $\mathbb{R}^n$. Формулировка становится более удобной, если нумеровать точки, начиная с нуля.

Теорема. *Пусть m_{ij}, $i, j = 0, 1, \ldots, n$, — неотрицательные целые числа, причём $m_{ij} = m_{ji}$ при всех i, j и $m_{ii} = 0$ при всех i. Тогда для существования точек $\mathbf{p}_0, \mathbf{p}_1, \ldots, \mathbf{p}_n \in \mathbb{R}^n$ с расстояниями $\|\mathbf{p}_i - \mathbf{p}_j\| = m_{ij}$ при всех i, j необходимо и достаточно, чтобы была положительно полуопределённой $(n \times n)$-матрица G, где*

$$g_{ij} = \frac{1}{2}\bigl(m_{0i}^2 + m_{0j}^2 - m_{ij}^2\bigr).$$

[1] Напомним, что вещественная матрица M называется **положительно полуопределённой**, если это симметричная $(n \times n)$-матрица (для некоторого n), причём $\mathbf{x}^T M \mathbf{x} \geqslant 0$ для всех $\mathbf{x} \in \mathbb{R}^n$.

Заметим, что неравенство треугольника не присутствует в теореме явно — оно спрятано в условии положительной полуопределённости (если хотите, проверьте это для случая $n=2$).

Доказательство теоремы опирается на следующую характеризацию положительно полуопределённых матриц.

Факт. *Вещественная симметричная $(n\times n)$-матрица A является положительно полуопределённой в точности тогда, когда существует вещественная $(n\times n)$-матрица X, для которой $A=X^TX$.*

Набросок доказательства факта. Если $A=X^TX$, то для любого $\mathbf{x}\in\mathbb{R}^n$ имеем $\mathbf{x}^TA\mathbf{x}=(X\mathbf{x})^T(X\mathbf{x})=\|X\mathbf{x}\|^2\geqslant 0$, так что A — положительно полуопределённая матрица.

Обратно, любая вещественная симметричная квадратная матрица A **диагонализуема**, т. е. может быть представлена в виде $A=T^{-1}DT$ с невырожденной $(n\times n)$-матрицей T и диагональной матрицей D (с собственными значениями матрицы A на диагонали). Более того, доказывая этот факт по индукции, получаем, что T **ортогональна**, т. е. $T^{-1}=T^T$, и, следовательно, $A=T^TDT$. Поэтому можно положить $X:=RT$, где $R=\sqrt{D}$ — диагональная матрица, на диагонали которой стоят квадратные корни из собственных значений матрицы A; здесь мы пользуемся тем, что собственные значения матрицы A неотрицательны, поскольку она является положительно полуопределённой.

Оказывается, в качестве X можно даже взять верхнюю треугольную матрицу, и в этом случае говорят о *разложении Холецкого* матрицы A. □

Доказательство теоремы. Сначала проверим необходимость. Мы должны показать, что если $\mathbf{p}_0,\ldots,\mathbf{p}_n$ — данные точки в $\mathbb{R}^n$, а $m_{ij}:=\|\mathbf{p}_i-\mathbf{p}_j\|$, то матрица G из условия теоремы является положительно полуопределённой.

Применим *теорему косинусов*, согласно которой

$$\|\mathbf{x}-\mathbf{y}\|^2=\|\mathbf{x}\|^2+\|\mathbf{y}\|^2-2\langle\mathbf{x},\mathbf{y}\rangle$$

для любых двух векторов $\mathbf{x},\mathbf{y}\in\mathbb{R}^n$. Следовательно, если положить $\mathbf{x}_i:=\mathbf{p}_i-\mathbf{p}_0$, $i=1,2,\ldots,n$, то

$$\langle\mathbf{x}_i,\mathbf{x}_j\rangle=\frac{1}{2}(\|\mathbf{x}_i\|^2+\|\mathbf{x}_j\|^2-\|\mathbf{x}_i-\mathbf{x}_j\|^2)=g_{ij}.$$

Таким образом, G является **матрицей Грама** векторов $\mathbf{x}_i$, можно записать $G=X^TX$, и потому G — положительно полуопределённая матрица.

Обратно, если G — положительно полуопределённая матрица, то её можно представить в виде $G = X^T X$ для некоторой вещественной $(n \times n)$-матрицы X. Пусть $\mathbf{p}_i \in \mathbb{R}^n$ обозначает i-й столбец матрицы X при $i = 1, 2, \ldots, n$, и пусть $\mathbf{p}_0 := \mathbf{0}$. Проводя предыдущую выкладку в обратном направлении, получаем $\|\mathbf{p}_i - \mathbf{p}_j\| = m_{ij}$, и доказательство завершено. □

Доказанная теорема решает вопрос о существовании $n+1$ точек в $\mathbb{R}^n$ с заданными расстояниями. Здесь n — наибольшая размерность, какая может потребоваться для $n+1$ точек. Можно также спросить, когда искомые $n+1$ точек принадлежат $\mathbb{R}^d$ с заданным d, например с $d = 2$. Модификация предыдущего рассуждения показывает, что ответ положителен в точности тогда, когда $G = X^T X$ для некоторой матрицы X ранга не выше d.

Литература

Schoenberg I. J. Remarks to Maurice Fréchet's article «Sur la definition axiomatique d'une classe d'espace distances vectoriellement applicable sur l'espace de Hilbert» // Ann. Math. 1935. V. 2, № 36. P. 724—732.

Миниатюра 8

Упаковка полных двудольных графов

Мы хотим разделить множество всех рёбер полного графа, например K_6, на множества рёбер полных двудольных графов, используя как можно меньше подграфов. Напомним, что граф G называется **полным двудольным**, если можно разделить множество его вершин $V(G)$ на два непересекающихся подмножества A, B таким образом, что $E(G) = \{\{a, b\} : a \in A, b \in B\}$. Такие A и B составляют **правильную раскраску** графа G.

На рис. 3 показано такое разбиение, использующее пять полных двудольных графов.

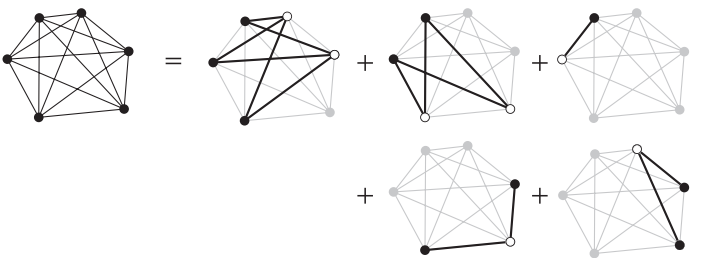


Рис. 3

Возможно ещё несколько различных разбиений этого графа на пять полных двудольных подграфов, а в общем случае нетрудно разбить K_n на $n-1$ полных двудольных подграфов. Но можно ли достичь лучшего?

Эта задача была мотивирована проблемами телекоммуникаций. Приведём прозрачное линейно-алгебраическое доказательство следующего факта.

Теорема. *Пусть $E(K_n)$, т. е. множество всех рёбер полного графа с n вершинами, представлено как дизъюнктное объединение множеств рёбер m полных двудольных графов. Тогда $m \geqslant n-1$.*

Доказательство. Пусть множества рёбер полных двудольных графов $H_1, H_2, \ldots, H_m$ не пересекаются и покрывают все рёбра графа

K_n, причём X_k и Y_k образуют правильную раскраску графа H_k при $k=1,2,\ldots,m$. (Множество $V(H_k)=X_k\cup Y_k$ не обязательно покрывает $V(K_n)$.)

Каждому графу H_k поставим в соответствие $(n\times n)$-матрицу A_k. На пересечении её i-й строки и j-го столбца стоит элемент

$$a_{ij}^{(k)}=\begin{cases}1 & \text{при } i\in X_k \text{ и } j\in Y_k,\\ 0 & \text{в противном случае.}\end{cases}$$

Мы утверждаем, что каждая из матриц A_k имеет ранг 1. Действительно, все ненулевые строки матрицы A равны фиксированному вектору, у которого стоят единицы в позициях, принадлежащих Y_k, и нули в остальных позициях.

Рассмотрим теперь матрицу $A=A_1+A_2+\ldots+A_m$. Ранг суммы двух матриц не превышает суммы их рангов (почему?), и потому ранг матрицы A не превышает m. Нам достаточно доказать, что этот ранг не меньше $n-1$.

Каждое ребро $\{i,j\}$ принадлежит ровно одному из графов H_k, поэтому для каждого $i\neq j$ либо $a_{ij}=1$ и $a_{ji}=0$, либо $a_{ij}=0$ и $a_{ji}=1$, где a_{ij} — элемент матрицы A в позиции (i,j). Кроме того, $a_{ii}=0$. Отсюда $A+A^T=J_n-I_n$, где I_n — единичная матрица, а J_n обозначает $(n\times n)$-матрицу из единиц.

Предположим, что $\operatorname{rank}(A)\leqslant n-2$. Добавим к A в качестве дополнительного столбца вектор $\mathbf{1}\in\mathbb{R}^n$ (все компоненты которого равны 1). Полученная $((n+1)\times n)$-матрица имеет ранг не больше $n-1$, поэтому некоторая нетривиальная линейная комбинация её столбцов равна $\mathbf{0}$. Иными словами, существует вектор-столбец $\mathbf{x}\in\mathbb{R}^n$, $\mathbf{x}\neq\mathbf{0}$, для которого $A\mathbf{x}=\mathbf{0}$ и $\mathbf{1}^T\mathbf{x}=0$.

Ввиду последнего равенства $J_n\mathbf{x}=\mathbf{0}$. Отсюда следует, что

$$\mathbf{x}^T(A+A^T)\mathbf{x}=\mathbf{x}^T(J_n-I_n)\mathbf{x}=\mathbf{x}^T(J_n\mathbf{x})-\mathbf{x}^T(I_n\mathbf{x})=$$
$$=0-\mathbf{x}^T\mathbf{x}=-\sum_{i=1}^n x_i^2<0.$$

С другой стороны,

$$\mathbf{x}^T(A^T+A)\mathbf{x}=(\mathbf{x}^TA^T)\mathbf{x}+\mathbf{x}^T(A\mathbf{x})=\mathbf{0}^T\mathbf{x}+\mathbf{x}^T\mathbf{0}=0,$$

и мы получаем противоречие. □

Литература

Этот результат содержится в статье

Graham R. L., *Pollak H. O.* On the addressing problem for loop switching // Bell System Tech. J. 1971. V. 50. P. 2495—2519.

Доказательство по существу следует заметке

Tverberg H. On the decomposition of K_n into complete bipartite graphs // J. Graph Theory. 1982. V. 6, № 4. P. 493—494.

Миниатюра 9

Равноугольные прямые

Какое наибольшее количество прямых можно провести в $\mathbb{R}^3$ так, чтобы углы между любыми двумя из них были одинаковы (будем называть такие прямые равноугольными)?

Все знают, что в $\mathbb{R}^3$ не может быть больше трёх попарно ортогональных прямых. Но для углов другой величины ситуация сложнее. Например, шесть больших диагоналей правильного икосаэдра (соединяющих пары противоположных вершин) равноугольны, см. рис. 4.

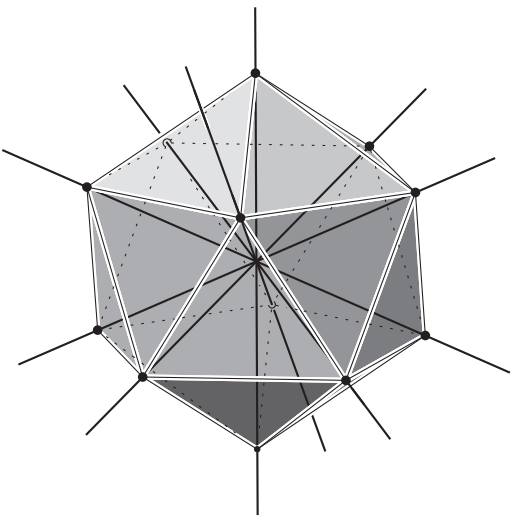


Рис. 4

Как мы докажем, это количество наибольшее, какого можно достичь.

Теорема. *Наибольшее количество равноугольных прямых в* $\mathbb{R}^3$ *равно* 6. *В общем случае в* $\mathbb{R}^d$ *не может быть больше* $\binom{d+1}{2}$ *равноугольных прямых.*

Доказательство. Рассмотрим конфигурацию из n прямых, где любая пара образует угол $\vartheta \in \left(0; \frac{\pi}{2}\right]$. Пусть $\mathbf{v}_i$ — единичный вектор в направлении i-й прямой (одну из двух его возможных ориентаций выберем произвольно). Равенство углов равносильно тому, что

$$|\langle \mathbf{v}_i, \mathbf{v}_j \rangle| = \cos\vartheta \quad \text{при всех } i \neq j.$$

Рассмотрим $\mathbf{v}_i$ как вектор-столбец, т. е. $(d\times 1)$-матрицу. Тогда $\mathbf{v}_i^T \mathbf{v}_j$ — скалярное произведение $\langle \mathbf{v}_i, \mathbf{v}_j \rangle$, точнее — (1×1)-матрица с единственным элементом $\langle \mathbf{v}_i, \mathbf{v}_j \rangle$. С другой стороны, $\mathbf{v}_i \mathbf{v}_j^T$ — это $(d\times d)$-матрица.

Покажем, что $\mathbf{v}_i \mathbf{v}_i^T$, $i = 1, 2, \ldots, n$, линейно независимы. Тогда, поскольку они принадлежат векторному пространству всех вещественных симметричных $(d\times d)$-матриц, имеющему размерность $\binom{d+1}{2}$, мы получим $n \leqslant \binom{d+1}{2}$, что и требовалось.

Чтобы доказать линейную независимость, рассмотрим линейную комбинацию

$$\sum_{i=1}^{n} a_i \mathbf{v}_i \mathbf{v}_i^T = 0,$$

где $a_1, a_2, \ldots, a_n$ — некоторые коэффициенты. Умножим обе части этого равенства слева на $\mathbf{v}_j^T$ и справа на $\mathbf{v}_j$. В силу ассоциативности умножения матриц

$$0 = \sum_{i=1}^{n} a_i \mathbf{v}_j^T (\mathbf{v}_i \mathbf{v}_i^T) \mathbf{v}_j = \sum_{i=1}^{n} a_i \langle \mathbf{v}_i, \mathbf{v}_j \rangle^2 = a_j + \sum_{i\neq j} a_i \cos^2\vartheta$$

при всех i. Иными словами, мы доказали, что $M\mathbf{a} = \mathbf{0}$, где $\mathbf{a} = (a_1, \ldots, a_n)$ и $M = (1 - \cos^2\vartheta) I_n + (\cos^2\vartheta) J_n$. Здесь I_n — единичная матрица, а J_n — матрица из единиц. Легко проверить, что матрица M невырожденна (при условии $\cos\vartheta \neq 1$); например, можно показать как в миниатюре 4, что она является положительно определённой. Значит, $\mathbf{a} = \mathbf{0}$, матрицы $\mathbf{v}_i \mathbf{v}_i^T$ линейно независимы и теорема доказана. □

Замечание. Доказанная верхняя оценка является строгой для $d = 3$, но для некоторых значений $d > 3$ её можно улучшить другими методами. В общем случае наилучшее возможное значение неизвестно. Наилучшая нижняя оценка, известная в 2000 г., равна $\frac{2}{9}(d+1)^2$. Она выполняется точно для всех d вида $3 \cdot 2^{2t-1} - 1$, где t — натуральное число.

Литература

Эта теорема сформулирована в статье

Lehmmens P. W. H., *Seidel J. J.* Equiangular lines // J. of Algebra. 1973. V. 24. P. 494—512

и приписывается Герзону (частное сообщение)[1]. Наилучшая нижняя оценка, упомянутая выше, взята из работы

de Caen D. Large equiangular sets of lines in Euclidean space // Electr. J. Comb. 2000. V. 7. R55.

[1] Видимо, имеется в виду М. Герзон (1945—1996), математик и специалист по цифровой звукозаписи. — *Прим. перев.*

Миниатюра 10

Где находится треугольник?

Содержится ли в данном графе **треугольник**, т. е. три вершины u, v, w, попарно соединённые рёбрами? Это не совсем лёгкий вопрос, если в графе много вершин и рёбер. Например, где расположен треугольник, на рис. 5?

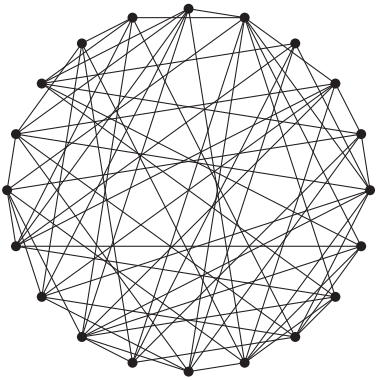


Рис. 5

Очевидный алгоритм для отыскания треугольника проверяет каждую тройку вершин и, таким образом, требует примерно n^3 операций для графа с n вершинами (нужно проверить $\binom{n}{3}$ троек, а это примерно $n^3/6$ при больших n). Можно ли существенно повысить скорость?

Да, можно. Но удивительно, что единственный известный способ сломать барьер n^3 — алгебраический, основанный на быстром матричном умножении.

Покажем это. Будет удобно обозначить вершины данного графа G через $\{1, 2, \ldots, n\}$. **Матрица смежности** графа G — это $(n \times n)$-матрица A с элементами

$$a_{ij} = \begin{cases} 1 & \text{при } i \neq j \text{ и } \{i, j\} \in E(G), \\ 0 & \text{в противном случае.} \end{cases}$$

Алгоритм устроен следующим образом.

1. Вычисляем матрицу $B := A^2$.
2. Для каждой пары индексов (i, j), $1 \leqslant i < j \leqslant n$, проверяем условия $a_{ij} \neq 0$ и $b_{ij} \neq 0$.
3. Если хотя бы одна пара (i, j) удовлетворяет этому условию, то G содержит треугольник. В противном случае G не содержит треугольников.

Чтобы понять, почему алгоритм работает, прежде всего надо выяснить смысл матрицы $B = A^2$. По определению умножения матриц имеем $b_{ij} = \sum_{k=1}^{n} a_{ik} a_{kj}$, при этом

$$a_{ik} a_{kj} = \begin{cases} 1 & \text{для вершины } k, \text{ смежной с } i \text{ и } j, \\ 0 & \text{в противном случае.} \end{cases}$$

Таким образом, b_{ij} — количество общих соседей у i и j.

Найти треугольник — значит найти две смежные вершины i, j с общим соседом k. Смежность вершин i и j означает, что $a_{ij} \neq 0$, а наличие общего соседа равносильно условию $b_{ij} \neq 0$. Поэтому алгоритм даёт правильный ответ.

Как быстро? Ясно, что в описанном алгоритме шаги 2 и 3 можно выполнить за время $O(n^2)$. Наибольшего времени требует вычисление матрицы A^2 на шаге 1. Если выполнять умножение матриц согласно определению, потребуется примерно n^3 арифметических операций, так что мы ничего не выиграем по сравнению с наивным методом проверки всех троек вершин.

Однако известны остроумные методы, позволяющие перемножать $(n \times n)$-матрицы с лучшей асимптотикой скорости. Первый из них принадлежит Штрассену и требует порядка $n^{2{,}807}$ арифметических операций. Он основан на простом, но очень разумном приёме — если вы его не встречали, то полезно с ним ознакомиться, см. источники.

Экспонента матричного умножения определяется как инфимум чисел ω, для которых существует алгоритм перемножения двух квадратных матриц за $O(n^\omega)$ операций. Его значение неизвестно (все верят, что он равен 2); сейчас лучшая известная оценка сверху — примерно 2,376. Поэтому существование треугольника можно проверить за время $O(n^{2{,}376})$, что асимптотически гораздо лучше, чем $O(n^3)$ при наивном алгоритме.

Известно много вычислительных задач, где быстрое умножение матриц асимптотически даёт ускорение. Отыскание треугольников — одна из простейших среди них. Дальше мы встретим ещё некоторые более сложные алгоритмы такого рода.

Замечания. Описанный метод отыскания треугольников — самый быстрый из известных для *плотных* графов, т. е. таких графов, у которых относительно много рёбер по сравнению с количеством вершин. Другой изящный алгоритм, который мы здесь не рассматриваем, может отыскать треугольник за время $O(m^{2\omega/(\omega+1)})$, где m — количество рёбер.

Аналогичные методы можно применять и для отыскания подграфов, отличных от треугольников; этой задаче посвящена обширная литература. Например, наличие цикла длины 4 можно проверить за время $O(n^2)$ — гораздо быстрее, чем в лучшем известном алгоритме для отыскания треугольника!

Литература

Itai A., Rodeh M. Finding a minimum circuit in a graph // SIAM J. Comput. 1978. V. 7, № 4. P. 413—423.

Среди многочисленных работ о быстром отыскании фиксированного подграфа в данном графе отметим статью

Kloks T., Kratsch D., Müller H. Finding and counting small induced subgraphs efficiently // Inform. Process. Lett. 2000. V. 74, № 3—4. P. 115—121,

которая может служить отправной точкой дальнейших исследований по этой теме.

Первый алгоритм «быстрого» умножения матриц принадлежит Штрассену:

Strassen V. Gaussian elimination is not optimal // Numer. Math. 1969. V. 13. P. 354—356.

Самый быстрый асимптотически из известных алгоритмов умножения матриц содержится в статье

Coppersmith D., Winograd S. Matrix multiplication via arithmetic progressions // J. Symbolic Computation. 1990. V. 9, № 3. P. 251—280.

Интересный новый метод, который даёт иные алгоритмы примерно той же скорости, появился в работе

Cohn H., Kleinberg R., Szegedy B., Umans C. Group-theoretic algorithms for matrix multiplication // Proc. 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS). 2005. P. 379—388.

Миниатюра 11

Проверка умножения матриц

Умножение двух $(n \times n)$-матриц — очень важная операция. Обычный алгоритм умножения строк на столбцы требует около n^3 арифметических действий, но, как отмечено в миниатюре 10, найдены более остроумные алгоритмы, асимптотически гораздо более быстрые. Текущий рекорд имеет вид $O(n^{2,376})$. Однако коэффициент пропорциональности астрономически велик, так что алгоритм интересен лишь теоретически. На самом деле матрицы, на которых он превзошёл бы обычный алгоритм, не поместятся ни в какой существующий или будущий компьютер.

Однако прогресс невозможно остановить, и вскоре какая-нибудь компания может начать продажу программы под названием MATRIX WIZARD, которая, как предполагается, перемножает матрицы *действительно* быстро. Поскольку ошибки здесь могут иметь катастрофические последствия, желательно иметь простую *программу проверки* в дополнение к MATRIX WIZARD, чтобы проверять, что полученная матрица C действительно является произведением входных матриц A и B.

Разумеется, мало смысла в программе проверки, которая действительно перемножает A и B и сравнивает результат с C, поскольку мы не умеем перемножать матрицы быстрее, чем MATRIX WIZARD. Но оказывается, если разрешить маленькую вероятность ошибки, то существует очень простая и эффективная проверка умножения матриц.

Ради конкретности будем рассматривать матрицы, состоящие из рациональных чисел, хотя всё без изменений пригодно для матриц над любым полем. Алгоритм проверки получает на входе $(n \times n)$-матрицы A, B, C. С помощью генератора случайных чисел строится случайный n-мерный вектор $\mathbf{x}$ из нулей и единиц. При этом любой вектор из $\{0, 1\}^n$ появляется с одинаковой вероятностью, равной 2^{-n}. Алгоритм вычисляет произведения $C\mathbf{x}$ (использовав $O(n^2)$ операций) и $AB\mathbf{x}$ (снова за $O(n^2)$ операций; подразумевается расстановка скобок $A(B\mathbf{x})$). Если результаты совпали, алгоритм отвечает ДА, в противном случае НЕТ.

Если $C = AB$, алгоритм обязательно ответит ДА, что правильно. Но если $C \neq AB$, он может ответить и ДА, и НЕТ. Мы утверждаем, что ложный ответ ДА имеет вероятность не больше $\frac{1}{2}$, так что алгоритм находит ошибку в умножении матриц с вероятностью не меньше $\frac{1}{2}$.

Положим $D := C - AB$. Достаточно показать, что если D — любая ненулевая $(n \times n)$-матрица, а $\mathbf{x} \in \{0, 1\}^n$ случайно распределено, то вектор $\mathbf{y} := D\mathbf{x}$ равен нулю с вероятностью не больше $\frac{1}{2}$.

Предположим, что $D \neq 0$, и зафиксируем такие индексы k и ℓ, что $d_{k\ell} \neq 0$. Покажем, что тогда вероятность равенства $y_k = 0$ не превосходит $\frac{1}{2}$.

Выполнено равенство

$$y_k = d_{k1}x_1 + d_{k2}x_2 + \ldots + d_{kn}x_n = d_{k\ell}x_\ell + S,$$

где

$$S = \sum_{\substack{j=1,2,\ldots,n \\ j \neq \ell}} d_{kj}x_j.$$

Предположим, что мы выбираем компоненты вектора $\mathbf{x}$ в соответствии с последовательными бросаниями монеты, причём значение x_ℓ определяется последним бросанием (это несущественно, так как бросания независимы). Перед этим последним бросанием величина S уже определена, так как она не зависит от x_ℓ. После этого бросания мы либо оставляем S прежним (если $x_\ell = 0$), либо добавляем к нему ненулевое число $d_{k\ell}$ (если $x_\ell = 1$). Хотя бы в одном из этих случаев мы должны получить ненулевое число, так что $D\mathbf{x} \neq \mathbf{0}$ имеет вероятность не меньше $\frac{1}{2}$, как и утверждалось.

Описанный алгоритм проверки быстр, но не очень надёжен: он может пропустить ошибку с вероятностью до $\frac{1}{2}$. Но если повторить его, скажем, пятьдесят раз для одних и тех же A, B, C, то он пропустит ошибку с вероятностью не больше $2^{-50} < 10^{-15}$, и для практических целей такой вероятностью можно пренебречь.

Замечание. Идея *вероятностной проверки* вычислений, которую мы представили здесь в простой форме, оказалась очень плодотворной. Так называемая PCP-теорема из теории вычислительной сложности показывает, что за очень малое время можно вероятностно проверить решение любой эффективно разрешимой вычислительной задачи. Медленный персональный компьютер может, в принципе, проверять работу мощнейших суперкомпьютеров.

Были также открыты удивительные взаимосвязи этих результатов с алгоритмами аппроксимации.

Литература

Freivalds R. Probabilistic machines can use less running time // B: Information. Processing77 (Proc. of the IFIP Congress 1977). Amsterdam: North-Holland, 1977. P. P. 839—842.

Для ознакомления с PCP-теоремой и теорией вычислительной сложности можно обратиться, например, к книге

Goldreich O. Computational complexity: A conceptual perspective. Cambridge: Cambridge University Press, 2008.

Миниатюра 12

Замощение прямоугольника квадратами

Теорема. *Прямоугольник R с длинами сторон 1 и x, где x иррационально, нельзя замостить конечным множеством квадратов* (*так, чтобы внутренности квадратов не пересекались и весь прямоугольник был покрыт*).

Доказательство. Предположим, наоборот, что указанное замощение существует и состоит из квадратов $Q_1, Q_2, \ldots, Q_n$, причём сторона квадрата Q_i равна s_i.

Нам потребуется рассматривать множество $\mathbb{R}$ всех вещественных чисел как векторное пространство над полем $\mathbb{Q}$ рациональных чисел. Это довольно странное бесконечномерное векторное пространство, но очень полезное. Далее, нам потребуется следующий простой факт: если α — вещественное число, то 1 и α линейно независимы в рассматриваемом векторном пространстве в точности тогда, когда α иррационально.

Пусть $V \subseteq \mathbb{R}$ — линейное подпространство, порождённое числами 1, x и $s_1, s_2, \ldots, s_n$. Иначе говоря, V — множество всех рациональных линейных комбинаций этих чисел.

Определим линейное отображение $f\colon V \to \mathbb{R}$, положив $f(1) = 1$ и $f(x) = -1$ (а в остальном задав произвольно). Это возможно, так как 1 и x линейно независимы над $\mathbb{Q}$. В самом деле, в пространстве V есть базис $(b_1, b_2, \ldots, b_k)$, где $b_1 = 1$ и $b_2 = x$, и мы можем положить, например, $f(b_1) = 1$, $f(b_2) = -1$, $f(b_3) = \ldots = f(b_k) = 0$ и продолжить f на V линейно.

Для каждого прямоугольника A со сторонами a и b, где $a, b \in V$, положим $v(A) := f(a)f(b)$.

Мы утверждаем, что если прямоугольник R размера $1 \times x$ замощён квадратами $Q_1, Q_2, \ldots, Q_n$, то

$$v(R) = \sum_{i=1}^{n} v(Q_i).$$

Это приводит к противоречию, поскольку $v(R) = f(1)f(x) = -1$, тогда как

$$v(Q_i) = f(s_i)^2 \geqslant 0 \quad \text{при всех } i.$$

Чтобы доказать наше утверждение, продолжим стороны всех квадратов Q_i из предполагаемого замощения на весь прямоугольник R, как показано на рис. 6.

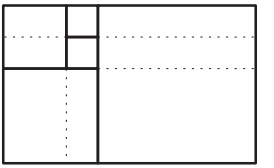


Рис. 6

Тогда R разбивается на маленькие прямоугольники, и из линейности отображения f легко следует, что $v(R)$ равно сумме $v(B)$ по всем маленьким прямоугольникам B. Точно так же $v(Q_i)$ равно сумме $v(B)$ по всем маленьким прямоугольникам, лежащим внутри Q_i. Таким образом, $v(R) = \sum_{i=1}^{n} v(Q_i)$. □

Замечание. Получается, что прямоугольник можно замостить квадратами в точности тогда, когда отношение его сторон рационально. Подобными методами можно доказать и различные другие теоремы о невозможности замощений. Например, невозможно рассечь куб на конечное множество выпуклых частей, из которых можно было бы сложить правильный тетраэдр.

К сожалению, до сих пор я не нашёл источник вышеприведённого доказательства. Другое очень красивое доказательство следует из замечательной взаимосвязи замощений квадратами и электрических сетей на плоскости[1]: *Brooks R. L.*, *Smith C. A. B.*, *Stone A. H.*, *Tutte W. T.* The dissection of rectangles into squares // Duke Math. J. 1940. V. 7. P. 312—340.

Литература

Доказанная теорема — частный случай результата Дена:

Dehn M. Über Zerlegung von Rechtecken in Rechtecke // Math. Ann. 1903. V. 57, № 3. P. 314—332.

К сожалению, до сих пор я не нашёл источник вышеприведённого доказательства. Другое очень красивое доказательство следует из замечательной взаимосвязи замощений квадратами и электрических сетей на плоскости:

Brooks R. L., *Smith C. A. B.*, *Stone A. H.*, *Tutte W. T.* The dissection of rectangles into squares // Duke Math. J. 1940. V. 7. P. 312—340.

[1] На русском языке про это можно прочитать в книге: *Яглом И. М.* Как разрезать квадрат? М.: Наука, 1968. — *Прим. ред.*

Миниатюра 13

Трёх графов Петерсена недостаточно

Известный **граф Петерсена** имеет 10 вершин степени 3 (см. рис. 7).

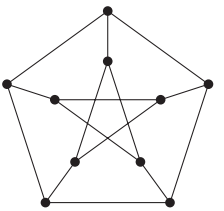


Рис. 7

Полный граф K_{10} имеет 10 вершин степени 9. Однако невозможно покрыть все его рёбра тремя экземплярами графа Петерсена.

Теорема. *В графе K_{10} нет трёх подграфов, изоморфных графу Петерсена и вместе покрывающих все рёбра графа K_{10}.*

Очевидно, можно доказать эту теорему обширным перебором случаев. Приведём её изящное доказательство — маленький пример на тему **спектральной теории графов**. Это часть теории графов, в которой рассматриваются собственные значения матрицы смежности графа.

Доказательство. Напомним, что **матрица смежности** графа G с множеством вершин $\{1, 2, \ldots, n\}$ — это $(n\times n)$-матрица A, в которой

$$a_{ij} = \begin{cases} 1 & \text{при } i \neq j \text{ и } \{i, j\} \in E(G), \\ 0 & \text{в противном случае.} \end{cases}$$

Например, матрица смежности графа K_{10} равна $J_{10} - I_{10}$, где J_n обозначает $(n\times n)$-матрицу из единиц, а I_n — единичную матрицу.

Под **собственными значениями графа G** мы понимаем собственные значения его матрицы смежности. Поскольку это вещественная симметричная матрица, она имеет n вещественных собственных значений (с учётом кратностей). Собственному значению кратности k отвечает собственное подпространство размерности k.

Напомним, что два графа $G=(V,E)$ и $G'=(V',E')$ **изоморфны**, если существует такая биекция $f\colon V\to V'$, что для любых двух различных вершин $u,v\in V$ найдется ребро $\{u,v\}\in E$ в точности тогда, когда $\{f(u),f(v)\}\in E'$. Неформально говоря, G и G' изоморфны, если можно получить G' из G переименованием вершин.

Легко видеть, что матрицы смежности двух изоморфных графов имеют одинаковые собственные значения, а соответствующие собственные подпространства имеют одинаковые размерности.

Нам потребуются следующие факты.

Лемма. *Граф Петерсена имеет собственное значение* 1 *кратности* 5*, а число* -3 *не является его собственным значением.*

Прямолинейное доказательство. Пусть A — матрица смежности. Чтобы доказать, что 1 — собственное значение кратности 5, достаточно проверить, что матрица $A-I_{10}$ имеет пятимерное ядро. Это можно сделать методом Гаусса. Для -3 проверяется, что матрица $A+3I_{10}$ невырожденна. Можно также вычислить собственные значения одним из многих существующих алгоритмов. □

Более продвинутое доказательство леммы (набросок). Можно найти собственные значения более изящным способом, используя свойства графа Петерсена. А именно, как показано ниже в миниатюре 14, граф Петерсена является *графом Мура* и его матрица смежности A удовлетворяет уравнению $A^2+A=J_{10}+2I_{10}$. Простое линейно-алгебраическое рассуждение показывает, что каждое её собственное значение λ либо равно 3, т. е. равно степени каждой вершины графа Петерсена, либо удовлетворяет уравнению $\lambda^2+\lambda=2$. Поэтому собственные значения могут быть равны 3, -2 и 1, а дальнейшее применение этого подхода позволяет найти их кратности — см. подробности в доказательстве основной теоремы из миниатюры 14. □

Окончательное Доказательство теоремы. Предположим, что рёбра графа K_{10} покрыты подграфами P, Q и R, каждый из которых изоморфен графу Петерсена. Если A_P — матрица смежности графа P и аналогично определены A_Q и A_R, то $A_P+A_Q+A_R=J_{10}-I_{10}$.

Поскольку граф P изоморфен графу Петерсена, собственное подпространство матрицы A_P, отвечающее значению 1, имеет размерность 5 согласно лемме; иначе говоря, A_P-I_{10} имеет пятимерное ядро.

Далее, в каждом столбце матрицы A_P-I_{10} стоят три единицы и одна минус единица. Поэтому, сложив все уравнения системы

$(A_P - I_{10})\mathbf{x} = \mathbf{0}$, мы получим $2x_1 + 2x_2 + \ldots + 2x_{10} = 0$. Это означает, что ядро матрицы $A_P - I_{10}$ содержится в 9-мерном ортогональном дополнении вектора $\mathbf{1} = (1, 1, \ldots, 1)$.

Аналогичный результат верен для ядра матрицы $A_Q - I_{10}$, и по соображениям размерности оба ядра содержат общий ненулевой вектор $\mathbf{w}$, для которого $\mathbf{1}^T\mathbf{w} = 0$. Отсюда

$$\begin{aligned} A_R\mathbf{w} &= (J_{10} - I_{10} - A_P - A_Q)\mathbf{w} = \\ &= J_{10}\mathbf{w} - I_{10}\mathbf{w} - (A_P - I_{10})\mathbf{w} - (A_Q - I_{10})\mathbf{w} - 2I_{10}\mathbf{w} = \\ &= \mathbf{0} - \mathbf{w} - \mathbf{0} - \mathbf{0} - 2\mathbf{w} = -3\mathbf{w}. \end{aligned}$$

Таким образом, -3 должно быть собственным значением матрицы A_R, но по предыдущей лемме это неверно — приходим к противоречию. □

Литература

Lossers O. P., *Schwenk A. J.* Solution of advanced problem 6434 // Am. Math. Monthly. 1987. V. 94. P. 885—887.

Миниатюра 14

Петерсен, Хоффман—Синглтон и, может быть, 57

Это классический фрагмент математики 1960-х годов. Он воспроизводился много раз, но остаётся одним из красивейших, какие я видел, применений собственных чисел графа. Более того, доказательство хорошо передаёт общий дух алгебраических доказательств несуществования для различных «высоко регулярных» структур.

Пусть G — граф обхвата $g \geqslant 4$ и наименьшей степени $r \geqslant 3$, где **обхват** графа G — длина кратчайшего цикла в нём, а **наименьшая степень** r — наименьшее количество соседей у вершины. Не очевидно, что для всех r и g существуют соответствующие графы, но известно, что это так.

Пусть $n(r, g)$ — наименьшее возможное количество вершин в таком графе G. Отыскание этого количества, хотя бы приближённо, принадлежит к замечательнейшим задачам теории графов, и её решение, вероятно, имело бы много интересных следствий.

Нижняя граница. Нижняя граница для $n(r, g)$ получается простым подсчётом ветвей (линейная алгебра появляется позже). Вначале предположим, что $g = 2k + 1$ нечётно.

Пусть G — граф обхвата g и наименьшей степени r. Зафиксируем в нём вершину u и рассмотрим два пути длины k, начинающиеся в u. До некоторого момента они могут совпадать, затем разветвляются и больше не встречаются — иначе они замкнули бы цикл длины не больше $2k$. Таким образом, G содержит подграф, изображённый на рис. 8 (здесь $r = 4$ и $k = 2$).

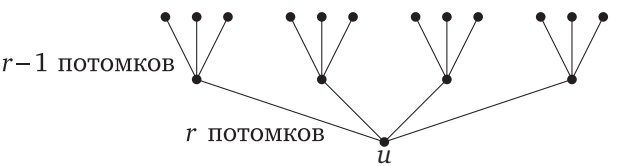


Рис. 8

Этот подграф — дерево T высоты k со степенью ветвления r в корне и $r-1$ в других внутренних вершинах. (В графе G могут быть дополнительные рёбра, соединяющие некоторые листья — тупиковые вершины дерева. И, разумеется, G может содержать больше вершин, чем T.)

Легко подсчитать, что количество вершин дерева T равно

$$1+r+r(r-1)+r(r-1)^2+\ldots+r(r-1)^{k-1}, \qquad (1)$$

это и есть обещанная нижняя граница для $n(r,2k+1)$. При чётном $g=2k$ похожее, но чуть более сложное рассуждение, которое мы опустим, даёт для $n(r,2k)$ нижнюю оценку

$$1+r+r(r-1)+\ldots+r(r-1)^{k-2}+(r-1)^{k-1}. \qquad (2)$$

Верхние границы. Для больших r и g уровень знаний об $n(r,g)$ неудовлетворителен. Наилучшие известные верхние оценки равны примерно *степени* $\frac{3}{2}$ от нижних оценок (1), (2), так что уже в показателе есть неопределённость.

До сих пор (1), (2) остаются по существу лучшими известными нижними границами для $n(r,g)$, и значительное внимание уделено графам, для которых они достигаются, поскольку эти графы весьма упорядоченны и имеют, как правило, много замечательных свойств. По историческим причинам они называются **графами Мура** при нечётных g и **обобщёнными многоугольниками**[1] при чётных g.

Графы Мура. Здесь мы рассмотрим лишь графы Мура (об обобщённых многоугольниках и известных точных значениях $n(r,g)$ см., например, веб-страницу Г. Ройла (G. Royle) `https://web.archive.org/web/20090224031515/http://people.csse.uwa.edu.au/gordon/cages/`) Граф Мура — это граф обхвата $2k+1$ и наименьшей возможной степени r, имеющий $1+r+r(r-1)+\ldots+r(r-1)^{k-1}$ вершин.

Чтобы исключить тривиальные случаи, положим $r\geqslant 3$ и $k\geqslant 2$. Отметим также, что *каждая* вершина в графе Мура имеет степень ровно r, так как вершину большей степени можно было бы взять в качестве u в доказательстве нижней оценки и показать, что количество вершин превышает $1+r+r(r-1)+\ldots+r(r-1)^{k-1}$.

Вопрос о существовании графа Мура для данных k и r — своего рода головоломка. Множество его вершин должно совпадать с мно-

[1] Однако в некоторых источниках термин «граф Мура» применяется и при нечётном, и при чётном обхвате.

жеством вершин дерева T из доказательства нижней оценки, а дополнительные рёбра, не содержащиеся в T, могут соединять только его листья. Таким образом, мы чертим T, добавляем по $r-1$ «лап» ко всем листьям и хотим соединить лапы так, чтобы не появился цикл длины меньше $2k+1$. На рис. 9 это показано для обхвата $2k+1=5$ и $r=3$.

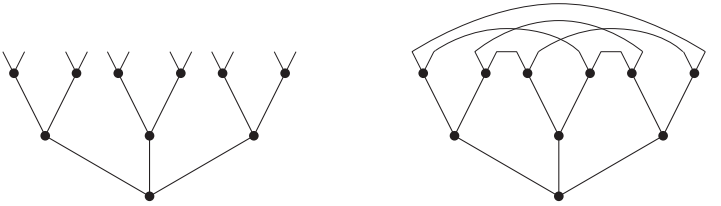


Рис. 9

В этом случае головоломка имеет решение, показанное справа, и можно доказать, что оно единственно с точностью до изоморфизма. Это известный **граф Петерсена**, который был показан в более привычном виде в миниатюре 13.

Известен лишь один граф Мура, отличный от этого. Он имеет 50 вершин, обхват 5 и степень $r=7$. Этот граф получается весьма симметричным склеиванием множества экземпляров графа Петерсена и называется **графом Хоффмана—Синглтона**. К удивлению, оказалось, что этот очень короткий список исчерпывает все графы Мура, с единственным возможным исключением: не доказано и не опровергнуто существование графа Мура с обхватом 5 и степенью 57.

Здесь будет показано, что графы Мура с обхватом 5 не могут иметь степень, отличную от 3, 7, 57. Несуществование графов Мура при большем обхвате доказывается довольно похожими методами.

Теорема. *Если существует граф G с обхватом* 5, *наименьшей степенью $r \geqslant 3$ и $n = 1 + r + (r-1)r = r^2 + 1$ вершинами, то $r \in \in \{3, 7, 57\}$.*

Начнём доказательство этой теоремы с теоретико-графового рассуждения, которое легко следует из вывода выражения (1) при $k=2$.

Лемма. *Если G — граф из условия теоремы, то любые две его несмежные вершины имеют ровно одного общего соседа.*

Доказательство леммы. Пусть u, v — произвольные несмежные вершины. Предоставим u играть роль u в рассуждении, которым выводится оценка (1). В нашем случае дерево T имеет высоту 2, поэто-

му v обязательно является в нём листом и существует единственный путь длины 2, соединяющий его с u. □

Доказательство теоремы. Напомним понятие **матрицы смежности** A графа G, уже использованное в миниатюрах 10 и 13. Если G имеет множество вершин $\{1, 2, \ldots, n\}$, то A — это $(n\times n)$-матрица с элементами вида

$$a_{ij} = \begin{cases} 1 & \text{при } i \neq j \text{ и } \{i, j\} \in E(G), \\ 0 & \text{в противном случае.} \end{cases}$$

Ключевой шаг в доказательстве — рассмотреть $B := A^2$. Как уже отмечено в миниатюре 10, из определения умножения матриц легко видеть, что b_{ij} равно количеству вершин, смежных и с i и с j. Следовательно, b_{ij} при $i \neq j$ равно количеству общих соседей вершин i и j, а b_{ii} — это просто степень вершины i.

Применив эти общие факты к графу G из условия теоремы, получаем

$$b_{ij} = \begin{cases} r & \text{при } i = j, \\ 0 & \text{при } i \neq j \text{ и } \{i, j\} \in E(G), \\ 1 & \text{при } i \neq j \text{ и } \{i, j\} \notin E(G). \end{cases} \tag{3}$$

Действительно, в первом случае утверждается, что степени всех вершин равны r, во втором — что у двух смежных вершин нет общих соседей (поскольку G имеет обхват 5 и, значит, не содержит треугольников), а третий случай — переформулировка утверждения леммы: любые две несмежные вершины имеют ровно одного общего соседа.

Далее, перепишем соотношение (3) в матричной форме:

$$A^2 = rI_n + J_n - I_n - A, \tag{4}$$

где I_n — единичная матрица, J_n — матрица из единиц.

Теперь займёмся собственными числами графа. Обычно при этом начинают со следующих сведений из линейной алгебры: любая вещественная симметричная $(n\times n)$-матрица A имеет n попарно ортогональных собственных векторов $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$, а все её собственные значения $\lambda_1, \lambda_2, \ldots, \lambda_n$ вещественны (и не обязательно различны).

Пусть A — матрица смежности графа, в котором степени всех вершин равны r. Тогда $A\mathbf{1} = r\mathbf{1}$, где $\mathbf{1}$ обозначает вектор из одних единиц. Значит, r — собственное значение с собственным векто-

ром $\mathbf{1}$, и поэтому можно положить $\lambda_1 = r$, $\mathbf{v}_1 = \mathbf{1}$. В силу ортогональности собственных векторов имеем $\mathbf{1}^T\mathbf{v}_i = 0$ при всех $i \neq 1$, откуда следует, что $J_n\mathbf{v}_i = \mathbf{0}$.

Вооружившись этими фактами, посмотрим, что произойдёт при умножении равенства (4) справа на некоторый вектор $\mathbf{v}_i$, $i \neq 1$. Левая часть превращается в $A^2\mathbf{v}_i = A\lambda_i\mathbf{v}_i = \lambda_i^2\mathbf{v}_i$, а правая в $r\mathbf{v}_i - \mathbf{v}_i - \lambda_i\mathbf{v}_i$. Обе части — скалярные кратные ненулевого вектора $\mathbf{v}_i$, поэтому скалярные коэффициенты при нём должны быть одинаковы, следовательно,

$$\lambda_i^2 + \lambda_i - (r-1) = 0.$$

Таким образом, каждое λ_i, $i \neq 1$, равно одному из корней ρ_1, ρ_2 квадратного уравнения $\lambda^2 + \lambda - (r-1) = 0$, из которого находим

$$\rho_1 = \frac{-1+\sqrt{D}}{2}, \quad \rho_2 = \frac{-1-\sqrt{D}}{2}, \quad \text{где } D := 4r-3.$$

Значит, A имеет лишь три различных собственных значения: r, ρ_1 и ρ_2. Предположим, что ρ_1 появляется m_1 раз среди λ_i, а ρ_2 появляется m_2 раз; поскольку r появляется один раз, получаем $m_1 + m_2 = n-1$.

Последнее, что нам потребуется из линейной алгебры, — тот факт, что сумма всех собственных значений матрицы A равна её *следу*, т. е. сумме всех диагональных элементов, в нашем случае нулевой. Отсюда следует, что

$$r + m_1\rho_1 + m_2\rho_2 = 0. \tag{5}$$

Оставшаяся часть доказательства — лишь вычисления плюс простое рассуждение о делимости (немного теории чисел, если мы хотим выразиться ярче). Подставив в равенство 5 выражения для ρ_1 и ρ_2, умножив на 2 и воспользовавшись равенствами $m_1 + m_2 = n - 1 = r^2$ (последнее равенство — одно из допущений теоремы), приходим к формуле

$$(m_1 - m_2)\sqrt{D} = r^2 - 2r. \tag{6}$$

Если D — не квадрат натурального числа, то $\sqrt{D}$ иррационален и равенство (6) может выполняться лишь при $m_1 = m_2$. Но тогда $r^2 - 2r = 0$, что невозможно при $r \geqslant 3$. Следовательно, $\sqrt{D}$ — целое число, т. е. $D = 4r-3 = s^2$ для некоторого натурального числа s. Отсюда следует, что $r = \dfrac{s^2+3}{4}$. Подставляя это выражение в формулу (6) и упрощая, получаем

$$s^4 - 2s^2 - 16(m_1 - m_2)s = s(s^3 - 2s - 16(m_1 - m_2)) = 15.$$

Следовательно, s делит 15, т. е. $s \in \{1, 3, 5, 15\}$, а значит,

$$r \in \{1, 3, 7, 57\},$$

и теорема доказана. □

Литература

Hoffman A. J., *Singleton R. R.* On Moore graphs with diameters 2 and 3 // IBM J. Res. Develop. 1960. V. 4. P. 497—504.

Миниатюра 15

Только два расстояния

Каково наибольшее количество точек на плоскости, все попарные расстояния между которыми одинаковы? Если даны хотя бы три точки, они должны образовать равносторонний треугольник и нет способа добавить четвёртую.

А сколько точек на плоскости можно найти, если расстояниям разрешено принимать *два* различных значения? Легко найти четырёхточечную конфигурацию с двумя расстояниями — например, вершины квадрата. Немного поразмыслив, находим следующую пятиточечную конфигурацию.

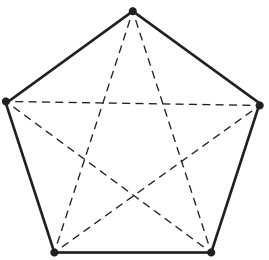


Рис. 10

Но как доказать, что нет большей конфигурации?

Тот же вопрос можно задать и для высших размерностей, т. е. в пространстве $\mathbb{R}^d$, $d \geqslant 3$: каково наибольшее число $n = n(d)$, для которого существуют n точек в $\mathbb{R}^d$ лишь с двумя попарными расстояниями? Следующий изящный метод даёт довольно хорошую верхнюю оценку для $n(d)$, даже при том, что результат для плоскости не вдохновляет (получается верхняя граница 9 вместо правильной 5).

Теорема. *Справедливо неравенство* $n(d) \leqslant \frac{1}{2}(d^2 + 5d + 4)$.

Доказательство. Пусть $\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_n$ — точки в $\mathbb{R}^d$, а $\|\mathbf{p}_i - \mathbf{p}_j\|$ — евклидово расстояние от $\mathbf{p}_i$ до $\mathbf{p}_j$. Тогда

$$\|\mathbf{p}_i - \mathbf{p}_j\|^2 = (p_{i1} - p_{j1})^2 + (p_{i2} - p_{j2})^2 + \ldots + (p_{id} - p_{jd})^2,$$

где p_{ij} обозначает j-ю координату точки $\mathbf{p}_i$. Пусть $\|\mathbf{p}_i - \mathbf{p}_j\| \in \{a, b\}$ для любых $i \neq j$.

Для каждой точки p рассмотрим соответствующую функцию

$$f_i \colon \mathbb{R}^d \to \mathbb{R}$$

вида

$$f_i(\mathbf{x}) := (\|\mathbf{x} - \mathbf{p}_i\|^2 - a^2)(\|\mathbf{x} - \mathbf{p}_i\|^2 - b^2),$$

где $\mathbf{x} = (x_1, x_2, \ldots, x_d) \in \mathbb{R}^d$.

Ключевое свойство этих функций состоит в том, что

$$f_i(\mathbf{p}_j) = \begin{cases} 0 & \text{при } i \neq j, \\ a^2 b^2 \neq 0 & \text{при } i = j, \end{cases} \tag{1}$$

что непосредственно следует из допущения о двух расстояниях.

Рассмотрим векторное пространство всех вещественных функций $\mathbb{R}^d \to \mathbb{R}$ и линейное подпространство V, порождённое функциями $f_1, f_2, \ldots, f_n$. Прежде всего мы утверждаем, что $f_1, f_2, \ldots, f_n$ линейно независимы. Предположим, что линейная комбинация $f = \alpha_1 f_1 + \alpha_2 f_2 + \ldots + \alpha_n f_n \colon \mathbb{R}^d \to \mathbb{R}$ является тождественным нулём. В частности, это нуль на каждом $\mathbf{p}_i$. В силу соотношения (1) получаем $0 = f(\mathbf{p}_i) = \alpha_i a^2 b^2$, а значит, $\alpha_i = 0$ для всех i. Таким образом, $\dim V = n$.

Теперь попробуем найти (как можно меньшую) систему G функций $\mathbb{R}^d \to \mathbb{R}$, не обязательно принадлежащих V, которая порождает V; это означает, что каждая функция $f \in V$ является линейной комбинацией функций из G. Тогда мы получим оценку $|G| \geqslant \dim V = n$.

Каждая из функций f_i — это многочлен от переменных $x_1, x_2, \ldots, x_d$ степени не выше 4. Поэтому она является линейной комбинацией мономов от $x_1, x_2, \ldots, x_d$ степени не выше 4. Легко подсчитать, что существует $\binom{d+4}{4}$ таких мономов (подсчёт приведён в миниатюре 25), следовательно, существует порождающая система G, для которой $|G| = \binom{d+4}{4}$.

Более тщательный анализ приводит к ещё меньшей системе G. Можно записать

$$\|\mathbf{x} - \mathbf{p}_i\|^2 = \sum_{j=1}^{d} (x_j - p_{ij})^2 = X - \sum_{j=1}^{d} 2 x_j p_{ij} + P_i,$$

где $X := \sum_{j=1}^{d} x_j^2$ и $P_i := \sum_{j=1}^{d} p_{ij}^2$. Тогда

$$f_i(\mathbf{x}) = (\|\mathbf{x}-\mathbf{p}_i\|^2 - a^2)(\|\mathbf{x}-\mathbf{p}_i\|^2 - b^2) = \\ = \Big(X - \sum_{j=1}^{d} 2x_j p_{ij} + A_i\Big)\Big(X - \sum_{j=1}^{d} 2x_j p_{ij} + B_i\Big),$$

где $A_i := P_i - a^2$ и $B_i := P_i - b^2$. Дальнейшие преобразования приводят к равенству

$$f_i(\mathbf{x}) = X^2 - 4X\sum_{j=1}^{d} p_{ij}x_j + \Big(\sum_{j=1}^{d} 2p_{ij}x_j\Big)^2 + \\ + (A_i + B_i)\Big(X - \sum_{j=1}^{d} 2p_{ij}x_j\Big) + A_iB_i.$$

Отсюда видно, что каждая функция f_i является линейной комбинацией функций из следующей системы G:

$$\begin{aligned} &X^2, \\ &x_jX, \quad j = 1, 2, \ldots, d, \\ &x_j^2, \quad j = 1, 2, \ldots, d, \\ &x_ix_j, \quad 1 \leqslant i < j \leqslant d, \\ &x_j, \quad j = 1, 2, \ldots, d, \\ &1. \end{aligned}$$

(Отметим, что X само является линейной комбинацией функций x_j^2.) Получаем

$$|G| = 1 + d + d + \binom{d}{2} + d + 1 = \frac{1}{2}(d^2 + 5d + 4),$$

откуда следует, что $n \leqslant \frac{1}{2}(d^2 + 5d + 4)$. Теорема доказана. □

Замечание. Дополнительные ухищрения, которые мы здесь не рассматриваем, улучшают верхнюю оценку до $\binom{d+2}{2}$.

Следующий пример показывает, что $n(d) \geqslant \frac{1}{2}(d^2 + d)$, так что квадратичное слагаемое в верхней оценке оптимально. Построение примера начнём с $\binom{d}{2}$ точек из множества $\{0, 1\}^d$, у которых в точности две координаты равны 1. В этом множестве два различных

расстояния, и оно лежит в гиперплоскости $\sum_{i=1}^{d} x_i = 2$. Значит, мы можем поместить его и в $\mathbb{R}^{d-1}$, а это даёт обещанную нижнюю границу $n(d) \geqslant \binom{d+1}{2} = \frac{1}{2}(d^2+d)$.

Литература

Larman D. G., *Rogers C. A.*, *Seidel J. J.* On two-distance sets in Euclidean space // Bull. London Math. Soc. 1977. V. 9, № 3. P. 261—267.

Согласно книге Л. Бабая и П. Франкла, упомянутой во введении, описанный приём впервые появляется в заметке

Koornwinder T. H. A note on the absolute bound for systems of lines // Indag. Math. 1976. V. 38, № 2. P. 152—153.

Улучшенная верхняя оценка $\binom{d+2}{2}$ получена в заметке

Blokhuis A. A new upper bound for the cardinality of 2-distance sets in Euclidean space // Ann. Discrete Math. 1984. V. 20. P. 65—66.

Миниатюра 16

Покрытие куба без одной вершины

Рассмотрим множество $\{0, 1\}^d \subset \mathbb{R}^d$, состоящее из всех вершин d-мерного единичного куба. Мы хотим покрыть гиперплоскостями все эти вершины, кроме одной, скажем $\mathbf{0} = (0, 0, \ldots, 0)$. (Напомним, что **гиперплоскость** в $\mathbb{R}^d$ — множество вида $\{\mathbf{x} \in \mathbb{R}^d : a_1x_1 + \ldots + a_dx_d = b\}$, где $a_1, \ldots, a_d, b \in \mathbb{R}$ — какие-то коэффициенты, причём хотя бы одно из a_i не равно нулю.)

Разумеется, можно покрыть все вершины всего лишь двумя гиперплоскостями, скажем $\{x_1 = 0\}$ и $\{x_1 = 1\}$, но задача становится интересной, если гиперплоскости не должны содержать точку $\mathbf{0}$. Каково наименьшее возможное количество гиперплоскостей при этих условиях?

Легко найти (по крайней мере) два разных способа покрытия d гиперплоскостями. Можно использовать гиперплоскости $\{x_i = 1\}$, $i = 1, 2, \ldots, d$, или $\{x_1 + x_2 + \ldots + x_d = k\}$, $k = 1, 2, \ldots, d$. Как мы увидим, d — наименьшее возможное количество.

Теорема. *Пусть $h_1, \ldots, h_m$ — гиперплоскости в $\mathbb{R}^d$, не проходящие через $\mathbf{0}$ и покрывающие все остальные точки из $\{0, 1\}^d$. Тогда $m \geqslant d$.*

Доказательство. Пусть плоскость h_i задана уравнением $a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{id}x_d = b_i$. Так как h_i не содержит $\mathbf{0}$, получаем, что $b_i \neq 0$. Поэтому мы можем (и будем) считать, что $b_i = 1$ при всех i.

Рассмотрим следующий должным образом выбранный многочлен:

$$f(x_1, x_2, \ldots, x_d) = \prod_{i=1}^{m}\left(1 - \sum_{j=1}^{d} a_{ij}x_j\right) - \prod_{j=1}^{d}(1 - x_j).$$

Он построен так, что $f(\mathbf{x}) = 0$ при всех $\mathbf{x} = (x_1, \ldots, x_d) \in \{0, 1\}^d$. (Для проверки нужно рассмотреть отдельно случаи $\mathbf{x} = \mathbf{0}$ и $\mathbf{x} \neq \mathbf{0}$ и использовать условие теоремы.)

Предположим теперь, что $m < d$. Тогда степень многочлена f равна d, а единственный моном степени d с ненулевым коффициентом имеет вид $\pm x_1x_2\ldots x_d$.

Теперь рассмотрим векторное пространство V всех вещественных функций на множестве $\{0, 1\}^d$. Каждый многочлен p от переменных $x_1, \ldots, x_d$ задаёт элемент из V, а именно функцию, равную p во всех точках из $\{0, 1\}^d$. В частности, введённый выше многочлен f задаёт элемент $0 \in V$, т. е. тождественный нуль на $\{0, 1\}^d$. Это означает, что моном $x_1x_2\ldots x_d$, также в качестве элемента из V, является линейной комбинацией мономов более низких степеней. Покажем, что это невозможно.

Вначале заметим, что многочлены x_i^2 и x_i определяют *один и тот же* элемент из V (поскольку $0^2 = 0$ и $1^2 = 1$). Следовательно, любой многочлен эквивалентен линейной комбинации *полилинейных мономов* вида $x_I = \prod\limits_{i \in I} x_i$, где $I \subseteq \{1, 2, \ldots, d\}$. Поэтому достаточно доказать, что все x_I линейно независимы в пространстве V.

С этой целью рассмотрим линейную комбинацию

$$\sum_{I \subseteq \{1,2,\ldots,d\}} \alpha_I x_I = 0 \qquad (1)$$

(правая часть — тождественный нуль на $\{0, 1\}^d$). Предположим, что некоторое α_I не равно нулю. Выберем *наименьшее* I, для которого $\alpha_I \neq 0$, — наименьшее в том смысле, что $\alpha_J = 0$ для каждого собственного подмножества $J \subset I$. Если в формулу (1) подставить $x_i = 1$ при $i \in I$ и $x_i = 0$ при $i \notin I$, то мы получим $\alpha_I = 0$ и придём к противоречию. □

Литература

Alon N., *Füredi Z.* Covering the cube by affine hyperplanes // European J. Combin. 1993. V. 14, № 2. P. 79—83.

Миниатюра 17

Трудно избежать пересечений среднего размера

Обширная область комбинаторики, *теория экстремальных множеств*, посвящена задачам следующего рода. Пусть $\mathscr{F}$ — система подмножеств n-элементного множества, которая не содержит некоторую просто описываемую конфигурацию множеств. Каково наибольшее возможное количество множеств в $\mathscr{F}$?

Вот краткий список известных примеров.

- **Лемма Шпернера** (точнее, одна из лемм Шпернера): если не существует двух различных множеств $A, B \in \mathscr{F}$, $A \subset B$, то $|\mathscr{F}| \leqslant \leqslant \binom{n}{\lfloor n/2 \rfloor}$[1].
- **Теорема Эрдёша—Ко—Радо**: если $k \leqslant n/2$, каждое $A \in \mathscr{F}$ содержит ровно k элементов и $A \cap B \neq \varnothing$ для любых двух $A, B \in \mathscr{F}$, то $|\mathscr{F}| \leqslant \binom{n-1}{k-1}$.
- **Теорема о Нечётнограде** из миниатюры 3: если каждое $A \in \mathscr{F}$ содержит нечётное количество элементов, а $|A \cap B|$ чётно для любых двух различных $A, B \in \mathscr{F}$, то $|\mathscr{F}| \leqslant n$.

Этот список теорем можно продолжить на много страниц. Одним из главных инструментов в их доказательстве служат методы линейной алгебры.

Здесь будет представлен сильный и, может быть, удивительный результат такого рода. У него есть красивое геометрическое приложение, которое рассмотрено ниже в миниатюре 18.

Теорема. *Пусть p — простое число, а $\mathscr{F}$ — система $(2p-1)$-элементных подмножеств n-элементного множества X, причём среди них нет двух множеств, пересекающихся ровно по $p-1$ элементам. Тогда количество множеств в $\mathscr{F}$ не превосходит*

$$|\mathscr{F}| \leqslant \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{p-1}.$$

[1] Напомним, что $\lfloor x \rfloor$ означает наибольшее целое число, не превосходящее x. — *Прим. перев.*

Всего в n-элементном множестве имеется $\binom{n}{2p-1}$ подмножеств из $p-1$ элементов. Теорема утверждает, что если запретить один определённый размер пересечений, а именно $p-1$, то количество подмножеств намного уменьшится. Ниже показано, как сделать «намного меньше» количественно определённым.

Следствие. *Пусть $\mathscr{F}$ таково, как в условии теоремы, и пусть $n=4p$. Тогда*

$$\frac{\binom{4p}{2p-1}}{|\mathscr{F}|} \geqslant 1{,}1^n.$$

Доказательство следствия. Прежде всего,

$$\binom{n}{k-1} = \frac{k}{n-k+1}\binom{n}{k},$$

так что при $n \geqslant 4k$ получаем $\binom{n}{k-1} \leqslant \frac{1}{3}\binom{n}{k}$. Значит,

$$\binom{4p}{p-1}+\binom{4p}{p-2}+\ldots+\binom{4p}{0} \leqslant \binom{4p}{p}\left(\frac{1}{3}+\frac{1}{3^2}+\frac{1}{3^3}+\ldots\right) \leqslant \frac{1}{2}\binom{4p}{p}.$$

Тогда

$$\frac{\binom{4p}{2p-1}}{|\mathscr{F}|} \geqslant 2\cdot\frac{\binom{4p}{2p-1}}{\binom{4p}{p}} = 2\cdot\frac{(3p)(3p-1)\ldots(2p+2)}{(2p-1)(2p-2)\ldots(p+1)} \geqslant$$

$$\geqslant 2\left(\frac{3}{2}\right)^{p-1} > \left(\frac{3}{2}\right)^{p} > 1{,}1^n.$$

(Есть много способов проводить подобные выкладки, и можно применять общеизвестные оценки, такие как $(n/k)^k \leqslant \binom{n}{k} \leqslant (en/k)^k$ или формула Стирлинга, но мы не хотели здесь опираться на них.) □

Доказательство теоремы. В доказательстве скомбинированы приёмы, уже встречавшиеся нам в миниатюрах 15 и 16.

Каждому множеству $A \in \mathscr{F}$ соответствуют два объекта.

- Вектор $\mathbf{c}_A \in \{0,1\}^n$. Это просто **характеристический вектор** множества A, у которого i-я компонента равна 1 при $i \in A$ и 0 в противном случае.
- Функция $f_A\colon \{0,1\}^n \to \mathbb{F}_p$ вида

$$f_A(\mathbf{x}) := \prod_{s=0}^{p-2}\left(\left(\sum_{i\in A} x_i\right) - s\right).$$

Все арифметические операции в определении функции f_A выполняются в конечном поле $\mathbb{F}_p$ — иначе говоря, по модулю p (так что 0 и 1 тоже считаются элементами из $\mathbb{F}_p$). Например, при $p=3$, $n=8$ и $A=\{2,3,4,6,8\}$ получаем

$$\mathbf{c}_A = (0,1,1,1,0,1,0,1) \quad \text{и}$$
$$f_A(\mathbf{x}) = (x_2+x_3+x_4+x_6+x_8)(x_2+x_3+x_4+x_6+x_8-1).$$

Важнейшие свойства функций f_A таковы:

(i) $f_A(\mathbf{c}_A)\neq 0$ при всех $A\in\mathscr{F}$;

(ii) $f_A(\mathbf{c}_B)=0$ при всех $A,B\in\mathscr{F}$, $A\neq B$.

В самом деле, $f_A(\mathbf{c}_B)=\prod\limits_{s=0}^{p-2}(|A\cap B|-s) \pmod p$, и это произведение не равно нулю в точности тогда, когда[1] $|A\cap B|\equiv p-1 \pmod p$. При $A=B$ получаем $|A\cap A|=2p-1\equiv p-1 \pmod p$, так что $f_A(\mathbf{c}_A)\neq 0$. При $A\neq B$ получаем $|A\cap B|\leqslant 2p-2$ и $|A\cap B|\neq p-1$ в силу «запрета на пересечения» («omitted intersection» assumption), поэтому $|A\cap B|\not\equiv p-1 \pmod p$ и, следовательно, $f_A(\mathbf{c}_B)=0$.

Как обычно, рассмотрим множество всех функций из $\{0,1\}^n$ в $\mathbb{F}_p$ как векторное пространство над $\mathbb{F}_p$, и пусть $V_{\mathscr{F}}$ — подпространство в нём, натянутое на функции f_A, $A\in\mathscr{F}$.

Прежде всего проверим, что f_A линейно независимы и потому $\dim(V_{\mathscr{F}})=|\mathscr{F}|$. Это вытекает стандартным образом из свойств (i) и (ii). Пусть $\sum\limits_{A\in\mathscr{F}}\alpha_A f_A=0$ для каких-то коэффициентов $\alpha_A\in\mathbb{F}_p$. Подставим $\mathbf{c}_B$ в левую часть, тогда все слагаемые $f_A(\mathbf{c}_B)$ с $A\neq B$ исчезают. Остаётся лишь $\alpha_B f_B(\mathbf{c}_B)=0$, а значит, $\alpha_B=0$, поскольку $f_B(\mathbf{c}_B)\neq 0$. Так как B было произвольным, функции f_A линейно независимы, как и утверждалось.

Теперь оценим $\dim(V_{\mathscr{F}})$ сверху. В конкретном примере, приведённом выше, выполнено равенство

$$f_A(\mathbf{x}) = (x_2+x_3+x_4+x_6+x_8)(x_2+x_3+x_4+x_6+x_8-1).$$

Перемножая выражения в скобках, получаем

$$f_A(\mathbf{x}) = -x_2+x_2^2-x_3+2x_2x_3+x_3^2-x_4+2x_2x_4+2x_3x_4+x_4^2-x_6+$$
$$+2x_2x_6+2x_3x_6+2x_4x_6+x_6^2-x_8+2x_2x_8+2x_3x_8+2x_4x_8+2x_6x_8+x_8^2.$$

[1] Напомним, что запись $x\equiv y \pmod p$ означает, что $x-y$ делится на p.

В общем случае каждая функция f_A является многочленом от $x_1, x_2, \ldots, x_n$ степени не выше $p-1$, так что это линейная комбинация мономов вида $x_1^{i_1}x_2^{i_2}\ldots x_n^{i_n}$, $i_1+i_2+\ldots+i_n \leqslant p-1$.

Далее, можно избавиться от мономов степени i_j выше единицы, поскольку x_j^2 и x_j представляют *одну и ту же* функцию $\{0,1\}^n \to \mathbb{F}_p$ (вместо переменных подставляются лишь нули и единицы). Поэтому достаточно подсчитать слагаемые с $i_j \in \{0,1\}$, а количество таких мономов равно количеству подмножеств из $\{1, 2, \ldots, n\}$ размера не больше $p-1$. Таким образом,

$$\dim(V_{\mathscr{F}}) \leqslant \binom{n}{0}+\binom{n}{1}+\ldots+\binom{n}{p-1},$$

и теорема доказана. □

Литература

Теорема является частным случаем неравенства Франкла—Уилсона из работы

Frankl P., Wilson R. M. Intersection theorems with geometric consequences // Combinatorica. 1981. V. 1, № 4. P. 357—368.

Доказательство следует статье

Alon N., Babai L., Suzuki H. Multilinear polynomials and Frankl—Ray-Chaudhuri—Wilson type intersection theorems // J. Combin. Theory. Ser. A. 1991. V. 58, № 2. P. 165—180.

Более общие теоремы о «запрете на пересечения» доказаны другими методами в статье

Frankl P., Rödl V. Forbidden intersections // Trans. Amer. Math. Soc. 1987. V. 300, № 1. P. 259—286.

Миниатюра 18

О трудности уменьшения диаметра

Следующий результат из нашей коллекции в виде исключения опирается на ранее доказанную теорему — из миниатюры 17.

Диаметр множества $X \subseteq \mathbb{R}^d$ определяется как

$$\operatorname{diam}(X) := \sup\{\|\mathbf{x}-\mathbf{y}\| : \mathbf{x}, \mathbf{y} \in X\},$$

где $\|\mathbf{x}-\mathbf{y}\|$ обозначает евклидово расстояние от $\mathbf{x}$ до $\mathbf{y}$. Если X замкнуто и ограниченно, например, конечно, то супремум обязательно достигается и можно сказать просто, что диаметр — наибольшее расстояние между двумя точками в X.

Вопрос. Кароль Борсук в 1933 г. поставил следующий вопрос.

> *Верно ли, что любое множество $X \subset \mathbb{R}^d$ конечного диаметра можно разделить на $d+1$ подмножеств $X_1, X_2, \dots, X_{d+1}$ так, чтобы диаметр каждого множества X_i был строго меньше, чем диаметр множества X?*

Назовём разбиение множества $X \subset \mathbb{R}^d$ на k подмножеств $X_1, X_2, \dots, X_k$, где $\operatorname{diam}(X_i) < \operatorname{diam}(X)$ при всех i, **понижающим диаметр**.

Легко видеть, что в $\mathbb{R}^d$ есть множества, которые не допускают разбиение на d частей, понижающее диаметр. Например, пусть X состоит из $d+1$ точек с попарными расстояниями 1 (другими словами, из всех вершин правильного d-мерного симплекса — явное построение такого множества намечено в миниатюре 30). Если разбить X на d частей, то одна из частей содержит не менее двух точек и, значит, имеет диаметр 1, такой же как у X. В своей статье 1933 г. Борсук доказал, среди прочего, что d-мерный шар имеет разбиение на $d+1$ частей, понижающее диаметр (это легко), но не на d частей (а это нелегко).

Вплоть до 1993 г. многие верили, что *любое* множество $X \subset \mathbb{R}^d$ конечного диаметра должно иметь разбиение на $d+1$ частей, понижающее диаметр, и это утверждение стали называть *гипотезой Борсука* (хотя сам Борсук в своей статье не выражал такого мнения).

Проблему Борсука часто переформулировали с дополнительным условием, что X выпукло. Ясно, что это не ведёт к потере общности,

поскольку диаметр множества равен диаметру его выпуклой оболочки.

В течение ряда лет было доказано несколько частичных результатов, подтверждающих (так называемую) гипотезу Борсука. Она доказана для произвольных множеств X в размерностях 2 и 3, для любых *гладких* выпуклых множеств во всех размерностях (здесь термин «гладкий» означает примерно «без выступающих углов и рёбер») и для некоторых других специальных классов выпуклых множеств.

Ответ. Как читатель мог догадаться или знать заранее, проблема Борсука была в итоге решена в *отрицательном* смысле. Начнём с предварительных замечаний, которые на самом деле не требуются в доказательстве, но могут облегчить его понимание.

Прежде всего нужно понять, что дополнительное условие выпуклости, по видимости упрощающее проблему, оказывается дымовой завесой: по существу проблема Борсука относится к конечным множествам.

Полезный класс конечных множеств можно получить из конечных систем множеств. Пусть $\mathscr{F}$ — некоторая система подмножеств множества $\{1, 2, \ldots, n\}$, а $X_{\mathscr{F}} \subset \mathbb{R}^n$ — множество всех их характеристических векторов, т. е. $X_{\mathscr{F}} := \{\mathbf{c}_A : A \in \mathscr{F}\}$, где i-я компонента в $\mathbf{c}_A$ равна 1, если $i \in A$, и 0 в противном случае.

Переведём результат миниатюры 17 на язык характеристических векторов и расстояний. Напомним следствие из теоремы в этой миниатюре: пусть p — простое число, $n = 4p$, а $\mathscr{F}$ — некоторая система $(2p-1)$-элементных подмножеств из $\{1, 2, \ldots, n\}$, причём $|A \cap B| \neq \neq p-1$ для любых $A, B \in \mathscr{F}$; тогда $\binom{n}{2p-1} / |\mathscr{F}| \geqslant 1{,}1^n$.

Пусть теперь $\mathscr{A}$ — система *всех* $(2p-1)$-элементных подмножеств из $\{1, 2, \ldots, n\}$ (так что $|\mathscr{A}| = \binom{n}{2p-1}$). Из утверждения в предыдущем абзаце вытекает следующее.

> *Если все множества из $\mathscr{A}$ разделены на менее чем $1{,}1^n$ классов, то хотя бы один из этих классов содержит два множества с пересечением размера ровно $p-1$.* (1)

Заметим, что, поскольку все множества в $\mathscr{A}$ имеют одинаковый размер, евклидово расстояние между двумя характеристическими векторами $\mathbf{c}_A, \mathbf{c}_B \in X_{\mathscr{A}}$ определяется размером пересечения $|A \cap B|$.

Действительно,

$$\|\mathbf{c}_A - \mathbf{c}_B\|^2 = |A \setminus B| + |B \setminus A| = |A| + |B| - 2|A \cap B| = \\ = 2(2p-1) - 2|A \cap B|.$$

В частности, если $|A \cap B| = p-1$, то $\|\mathbf{c}_A - \mathbf{c}_B\| = \sqrt{2p}$. Следовательно, если некоторое множество точек $X_{\mathscr{A}}$ разделено на менее чем $1{,}1^n$ подмножеств, то одно из подмножеств содержит две точки $\mathbf{c}_A, \mathbf{c}_B$ с расстоянием $\sqrt{2p}$.

Это звучит уже похоже на гипотезу Борсука: утверждается, что нельзя избавиться от расстояния $\sqrt{2p}$, разделив $X_{\mathscr{A}}$ на менее чем экспоненциальное количество частей. Единственная трудность: $\sqrt{2p}$ — не диаметр множества $X_{\mathscr{A}}$, а меньшее расстояние. Значит, нам нужно преобразовать $X_{\mathscr{A}}$ в такое множество, чтобы пары с расстоянием $\sqrt{2p}$ из $X_{\mathscr{A}}$ стали парами, реализующими диаметр нового множества. Такое преобразование возможно, но повышает размерность: полученное множество точек, которое мы обозначим $Q_{\mathscr{A}}$, лежит в размерности n^2.

На этом мы закончим предварительное обсуждение. Теперь сформулируем результат и дадим строгое доказательство.

Теорема. *Для каждого простого числа p существует множество точек в $\mathbb{R}^{n^2}$, $n = 4p$, у которого нет разбиения на менее чем $1{,}1^n$ частей, понижающего диаметр. Следовательно, ответ на вопрос Борсука отрицательный.*

Доказательство. Прежде всего напомним понятие **тензорного произведения**[1] векторов $\mathbf{x} \in \mathbb{R}^m$, $\mathbf{y} \in \mathbb{R}^n$. Оно обозначается через $\mathbf{x} \otimes \mathbf{y}$ и представляет собой вектор из $\mathbb{R}^{mn}$, компоненты которого — всевозможные произведения $x_i y_j$, $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$. (Иногда полезно рассматривать $\mathbf{x} \otimes \mathbf{y}$ как $(m \times n)$-матрицу $\mathbf{x}\mathbf{y}^T$.)

Нам потребуется следующее тождество, содержащее скалярное и тензорное произведение:

$$\langle \mathbf{x} \otimes \mathbf{x}, \mathbf{y} \otimes \mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle^2 \quad \text{для всех } \mathbf{x}, \mathbf{y} \in \mathbb{R}^n, \tag{2}$$

что проверяется очень легко.

Теперь приступим к построению множества точек, о котором говорится в теореме. Напомним, что $\mathscr{A}$ состоит из всех $(2p-1)$-элементных подмножеств из $\{1, 2, \ldots, 4p\}$. Для множества $A \in \mathscr{A}$ пусть

[1] В линейной алгебре тензорное произведение определяется более общим образом, для произвольной пары векторных пространств. Тензорное произведение с нашим определением можно считать «стандартным».

$\mathbf{u}_A \in \{-1, 1\}^n$ обозначает вектор, у которого i-я компонента равна $+1$, если $i \in A$, и -1 в противном случае. Положим $\mathbf{q}_A := \mathbf{u}_A \otimes \mathbf{u}_A \in \mathbb{R}^{n^2}$, тогда утверждение теоремы будет верно для множества точек

$$Q_{\mathscr{A}} := \{\mathbf{q}_A : A \in \mathscr{A}\}.$$

Прежде всего убедимся, что если $A, B \in \mathscr{A}$ и $|A \cap B| = s$, то

$$\langle \mathbf{u}_A, \mathbf{u}_B \rangle = 4(s - p + 1). \tag{3}$$

Это можно проверить с помощью схемы, изображённой на рис. 11.

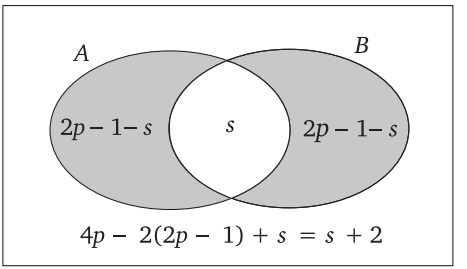


Рис. 11

Здесь компоненты, принадлежащие $(A \setminus B) \cup (B \setminus A)$ (серые), дают вклад -1 в скалярное произведение, а остальные (белые) дают вклад $+1$.

Из соотношения 3 мы видим, что $\langle \mathbf{u}_A, \mathbf{u}_B \rangle = 0$ в точности тогда, когда $|A \cap B| = p - 1$. Используя равенство 2, получаем соотношение для евклидовых расстояний в $Q_{\mathscr{A}}$:

$$\begin{aligned} \|\mathbf{q}_A - \mathbf{q}_B\|^2 &= \langle \mathbf{q}_A, \mathbf{q}_A \rangle + \langle \mathbf{q}_B, \mathbf{q}_B \rangle - 2\langle \mathbf{q}_A, \mathbf{q}_B \rangle = \\ &= \langle \mathbf{u}_A, \mathbf{u}_A \rangle^2 + \langle \mathbf{u}_B, \mathbf{u}_B \rangle^2 - 2\langle \mathbf{u}_A, \mathbf{u}_B \rangle^2. \end{aligned}$$

Но число $\langle \mathbf{u}_A, \mathbf{u}_A \rangle^2 + \langle \mathbf{u}_B, \mathbf{u}_B \rangle^2$ не зависит от A и B, а $\langle \mathbf{u}_A, \mathbf{u}_B \rangle^2$ — неотрицательное число, которое равно нулю в точности тогда, когда $|A \cap B| = p - 1$. Таким образом, максимальное возможное расстояние между $\mathbf{q}_A$ и $\mathbf{q}_B$, равное $\operatorname{diam}(Q_{\mathscr{A}})$, достигается в точности тогда, когда $|A \cap B| = p - 1$. С учётом утверждения (1) получаем, что $Q_{\mathscr{A}}$ не имеет разбиения меньше чем на $1{,}1^n$ частей, понижающего диаметр, что и утверждалось в теореме.

В итоге, если выбрать p достаточно большим, чтобы выполнялось равенство $1{,}1^n > n^2 + 1$, и положить $d := n^2$, мы получим мно-

жество точек в $\mathbb{R}^d$, не имеющее разбиения на $d+1$ частей, понижающего диаметр. □

Какова наименьшая размерность d, для которой вопрос Борсука имеет отрицательный ответ? Из утверждения только что доказанной теоремы получаем верхнюю оценку, близкую к 10^4. Её можно несколько улучшить, проведя более точные вычисления. На момент написания книги (2010 г.) наилучшая верхняя оценка равна $d = 298$, и её доказательство требует дополнительных соображений. Возможно, что и эта оценка весьма далека от наименьшей возможной.

Литература

Гипотеза Борсука была сформулирована в работе

Borsuk K. Drei Sätze über die n-dimensionale euklidische Sphäre // Fundamenta Mathematicae. 1933. V. 20. P. 177—190.

Контрпример опубликован в заметке

Kahn J., *Kalai G.* A counterexample to Borsuk's conjecture // Bull. Amer. Math. Soc. 1993. V. 29. P. 60—62.

Контрпример в размерности 298 приведён в статье

Hinrichs A., *Richter C.* New sets with large Borsuk numbers // Disc. Math. 2003. V. 270. P. 137—147.

Миниатюра 19

Конец мелким монетам

Интернет-магазин выполнял m заказов, каждый из которых состоял из нескольких продуктов. Внезапно все монеты стоимостью меньше 1 евро были изъяты из обращения и все цены были округлены вверх или вниз до целого количества евро.

Как округлить цены, чтобы суммарная стоимость каждого заказа не изменилась сильно? Эта и похожие задачи изучаются в теории рассогласования (discrepancy theory). Приведём здесь изящную теорему с линейно-алгебраическим доказательством.

Теорема. *Пусть заказано не более t порций каждого продукта, причём в каждый заказ входит не более одной его порции. Тогда можно так округлить цены, что полная стоимость каждого заказа изменится не более чем на t евро.*

Отметим, что если каждый заказ включает не более s продуктов, то их цены тривиально округляются так, что общая стоимость каждого продукта изменяется не более чем на s евро. Таким образом, теорема интересна в том случае, когда заказы включают много продуктов, но t не слишком велико.

Математическая формулировка задачи. Обозначим продукты $1, 2, \ldots, n$, и пусть c_j — цена j-го продукта. Можно считать, что $c_j \in (0; 1)$ при всех j (поскольку в задаче существенно только округление). Каждый заказ включает не больше одной порции каждого продукта, так что можно представить i-й заказ как множество $S_i \subseteq \{1, 2, \ldots, n\}$, $i = 1, 2, \ldots, m$. Теперь теорема утверждает, что если никакое j не содержится более чем в t множествах, то существуют такие числа $z_1, z_2, \ldots, z_n \in \{0, 1\}$, что

$$\left|\sum_{j\in S_i} c_j - \sum_{j\in S_i} z_j\right| \leqslant t, \quad \text{при каждом } i = 1, 2, \ldots, m.$$

Доказательство. Каждому индексу $j \in \{1, 2, \ldots, n\}$ сопоставим вещественную переменную $x_j \in [0; 1]$ с начальным значением c_j. Это значение будет меняться в ходе доказательства, в конце станет для каждого x_j равным 0 или 1 и будет использовано в качестве z_j.

На каждом шаге некоторые из переменных x_j уже зафиксированы, а остальные «плавают». Вначале все x_j «плавают». Зафиксированные x_j имеют значения 0 или 1 и в дальнейшем не меняются. Значения плавающих переменных лежат в интервале (0; 1). На каждом шаге хотя бы одна плавающая переменная становится фиксированной.

Назовём множество S_i **опасным**, если оно содержит больше t индексов j, для которых x_j ещё «плавает»; остальные множества **безопасны**. Будем всё время обеспечивать выполнение следующего условия:

$$\sum_{j\in S_i} x_j = \sum_{j\in S_i} c_j \quad \text{для всех опасных множеств } S_i. \tag{1}$$

Пусть F — множество номеров всех плавающих переменных. Рассмотрим (1) как систему линейных уравнений с плавающими переменными в качестве неизвестных (значения фиксированных переменных считаем константами). Ясно, что эта система имеет решение — текущие значения плавающих переменных. Поскольку они должны лежать в интервале (0; 1), решение системы является внутренней точкой $|F|$-мерного куба $[0; 1]^{|F|}$. Нам нужно доказать, что существует решение и на границе этого куба, т. е. что в некотором решении хотя бы одна из переменных принимает значение 0 или 1.

Ключевое соображение состоит в том, что опасных множеств всегда меньше, чем плавающих переменных, поскольку для каждого опасного множества требуется более чем t плавающих переменных, тогда как каждая плавающая переменная даёт вклад в не более чем t опасных множеств. Таким образом, рассматриваемая система уравнений содержит меньше уравнений, чем неизвестных, и потому пространство решений имеет размерность не меньше 1. Значит, через каждое решение проходит прямая (одномерное аффинное подпространство), все точки которой также являются решениями. Эта прямая пересекает поверхность куба в некоторой точке $\mathbf{y}$. Возьмём координаты этой точки в качестве значений плавающих переменных на следующем шаге. При этом все плавающие переменные x_j, для которых соответствующая координата $\mathbf{y}$ равна 0 или 1, сделаем фиксированными.

Будем повторять описанную процедуру, пока все переменные не станут фиксированными. Мы утверждаем, что если взять оконча-

тельные значения x_j в качестве z_j, $j=1, 2, \ldots, n$, то

$$\left|\sum_{j\in S_i} c_j - \sum_{j\in S_i} z_j\right| \leqslant t$$

для каждого $i=1, 2, \ldots, m$, как мы и хотели.

Чтобы убедиться в этом, рассмотрим одно из множеств S_i. В момент, когда оно перестало быть опасным, в силу условия (1) по-прежнему выполнялось равенство $\sum\limits_{j\in S_i} c_j - \sum\limits_{j\in S_i} x_j = 0$ и S_i содержало номера не более чем t плавающих переменных. В оставшейся части процедуры значение каждой из них меняется не больше чем на 1 (например, переменная могла быть равна 0,001, а позже стать фиксированной со значением 1). Этим завершается доказательство. □

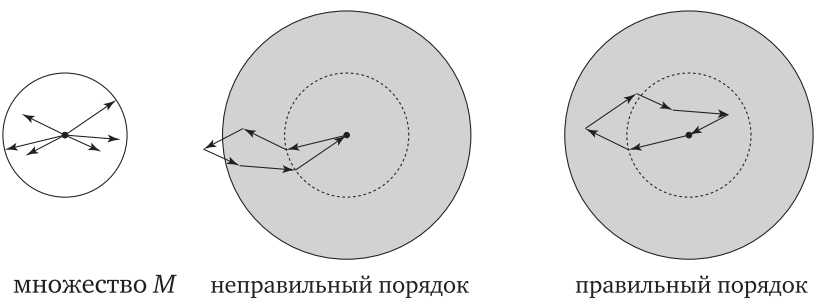
Литература

Beck J., Fiala T. «Integer making» theorems // Discr. Appl. Math. 1981. V. 3. P. 1—8.

Миниатюра 20

Прогулка по двору

Тюремный охранник, склонный к математике, выводит заключённого на прогулку и даёт ему следующие строгие указания. Заключённый получает конечное множество M векторов, имеющих длину не больше 10 м. Он должен начать прогулку в центре круглого тюремного двора радиусом 20 м, пройти вдоль некоторого вектора $\mathbf{v}_1 \in M$, затем вдоль другого вектора $\mathbf{v}_2 \in M$ и т. д., использовав каждый вектор из M ровно один раз. Векторы из M в сумме дают $\mathbf{0}$, так что заключённый в итоге вернётся в центр двора. Однако он не должен пересекать границу двора ни в какой момент прогулки (см. рис. 12), в противном случае охранник начинает стрелять без предупреждения.



множество M неправильный порядок правильный порядок

Рис. 12

Следующая теорема показывает, что безопасная прогулка возможна при любом конечном M, и это верно также для дворов в виде d-мерных шаров.

Теорема. *Пусть M — произвольное множество из n векторов в пространстве $\mathbb{R}^d$, причём $\|\mathbf{v}\| \leqslant 1$ для каждого $\mathbf{v} \in M$, где норма $\|\mathbf{v}\|$ — обычная евклидова длина и $\sum\limits_{\mathbf{v}\in M} \mathbf{v} = \mathbf{0}$. Тогда можно расположить все векторы из M в последовательность $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ таким образом, что $\|\mathbf{v}_1 + \mathbf{v}_2 + \ldots + \mathbf{v}_k\| \leqslant d$ для каждого $k = 1, 2, \ldots, n$.*

В примере с картинки можно даже расположить векторы так, чтобы весь путь лежал внутри круга радиуса 1, но для произвольного множества векторов радиус 1 может оказаться невозможен (найдите пример). Для плоскости наименьший возможный радиус двора известен: $\sqrt{5}/2 \approx 1{,}118$. В произвольной размерности d наилучшая нижняя оценка, найденная к моменту написания книги (2010 г.), имеет порядок $\sqrt{d}$, в то время как теорема обеспечивает наилучшую возможную верхнюю оценку, т. е. d. Закрыть пробел между этими оценками — до сих пор очень привлекательная открытая проблема.

Ниже фактически доказано более общее утверждение — для произвольного (не обязательно круглого) двора: пусть $B \subset \mathbb{R}^d$ — ограниченное выпуклое множество, содержащее начало координат, а M — множество из n векторов, причём $\mathbf{v} \in B$ для каждого $\mathbf{v} \in M$ и $\sum\limits_{\mathbf{v}\in M} \mathbf{v} = 0$. Тогда существует такое упорядочение $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ векторов из M, что $\mathbf{v}_1 + \mathbf{v}_2 + \ldots + \mathbf{v}_k \in dB$ для всех $k = 1, 2, \ldots, n$, где $dB = \{d\mathbf{x} : \mathbf{x} \in B\}$.

При такой более общей постановке константу d *нельзя* улучшить. Чтобы убедиться в этом для $d = 2$, возьмём в качестве B равносторонний треугольник с центром в начале координат.

Доказательство теоремы начнём с простой общей леммы (которая неявно использована также в миниатюре 19).

Лемма. *Пусть $A\mathbf{x} = \mathbf{b}$ — система из m линейных уравнений с $n \geqslant m$ неизвестными, имеющая решение $\mathbf{x}_0 \in [0; 1]^n$. Тогда существует решение $\widetilde{\mathbf{x}} \in [0; 1]^n$, в котором не менее $n - m$ неизвестных равны* 0 *или* 1.

Доказательство леммы. Проведём индукцию по $n - m$. При $n = m$ доказательство не требуется, поэтому пусть $n > m$. Тогда пространство решений имеет размерность не меньше 1 и, значит, содержит прямую, проходящую через $\mathbf{x}_0$. Эта прямая пересекает поверхность куба $[0; 1]^n$; пусть $\mathbf{y}$ — точка пересечения. Тогда $y_i \in \{0, 1\}$ для некоторого индекса i.

Построим новую систему линейных уравнений с $n - 1$ неизвестными, которая получается из системы $A\mathbf{x} = \mathbf{b}$, если положить x_i равным y_i. Эта новая система удовлетворяет условию леммы (решение, лежащее в кубе $[0; 1]^{n-1}$, получается из $\mathbf{y}$ выбрасыванием y_i), и по предположению индукции она имеет решение, в котором не менее чем $n - m - 1$ неизвестных равны 0 или 1. Добавляя y_i, получаем решение исходной системы, в котором $n - m$ или больше нулей и единиц. □

Доказательство теоремы. Идея доказательства в следующем: множество M «очень хорошее», так как сумма его векторов равна $\mathbf{0}$ и, значит, норма суммы равна нулю. Введём более слабое понятие «хорошего» множества векторов. Определение строится так, чтобы сумма всех векторов хорошего множества K имела норму не больше d. Сверх того — и в этом суть доказательства — мы покажем, что любое хорошее множество K из $k > d$ векторов имеет хорошее подмножество из $k-1$ векторов. Это позволит нам найти по индукции нужное упорядочение векторов в M.

Определение таково: множество $K = \{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k\}$ из $k \geqslant d$ векторов пространства $\mathbb{R}^d$ с длинами не больше 1 называется **хорошим**, если существуют коэффициенты $\alpha_1, \ldots, \alpha_k$, удовлетворяющие условиям

$$\alpha_i \in [0; 1], \quad i = 1, 2, \ldots, k,$$

$$\alpha_1\mathbf{w}_1 + \alpha_2\mathbf{w}_2 + \ldots + \alpha_k\mathbf{w}_k = \mathbf{0}, \tag{1}$$

$$\alpha_1 + \alpha_2 + \ldots + \alpha_k = k - d. \tag{2}$$

Заметим, что если бы правая часть формулы (2) была равна k, а не $k-d$, то все α_i обратились бы в 1, так что условие (1) просто означало бы, что $\sum\limits_{i=1}^{k} \mathbf{w}_i = \mathbf{0}$. Но так как $\sum\limits_{i=1}^{n} \alpha_i$ равно $k-d$, большинство из α_i должны быть близки к 1, однако остаётся некоторая свобода выбора.

Сначала проверим, что если множество $K = \{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k\}$ хорошее, то $\|\mathbf{w}_1 + \mathbf{w}_2 + \ldots + \mathbf{w}_k\| \leqslant d$. Действительно,

$$\begin{aligned}\left\|\sum_{i=1}^{k} \mathbf{w}_i\right\| &= \left\|\sum_{i=1}^{k} \mathbf{w}_i - \sum_{i=1}^{k} \alpha_i\mathbf{w}_i\right\| \leqslant \\ &\leqslant \sum_{i=1}^{k} \|(1-\alpha_i)\mathbf{w}_i\| = \sum_{i=1}^{k} (1-\alpha_i)\|\mathbf{w}_i\| \leqslant \\ &\leqslant \sum_{i=1}^{k} (1-\alpha_i) = d.\end{aligned}$$

Теперь сформулируем ключевое утверждение.

Утверждение. *Если $K = \{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k\}$ — хорошее множество из $k > d$ векторов, то найдётся такое i, что $K \setminus \{\mathbf{w}_i\}$ — хорошее множество из $k-1$ векторов.*

Доказательство утверждения. Рассмотрим следующую систему линейных уравнений с неизвестными $x_1, \ldots, x_k$:

$$x_1\mathbf{w}_1 + x_2\mathbf{w}_2 + \ldots + x_k\mathbf{w}_k = \mathbf{0}, \tag{3}$$

$$x_1 + x_2 + \ldots + x_k = k - d - 1. \tag{4}$$

Здесь соотношение (3) выражает равенство двух d-мерных векторов и, значит, фактически состоит из d уравнений. Последнее уравнение (4) похоже на (2), лишь с заменой правой части на $k-d-1$; мы готовимся показать, что подходящее подмножество из $k-1$ векторов в K является хорошим.

Система (3)—(4) состоит из $d+1$ уравнений с k неизвестными. Если $\alpha_1, \ldots, \alpha_k$ — коэффициенты, обеспечивающие, что множество K хорошее, то при $x_i := \dfrac{k-d-1}{k-d}\alpha_i$ мы получим решение этой системы, лежащее в $[0;1]^k$.

Таким образом, с учётом леммы существует и такое решение $\widetilde{\mathbf{x}} \in [0;1]^k$, в котором по крайней мере $k-d-1$ компонент равны 0 или 1. Мы хотим убедиться, что по крайней мере одна из этих компонент равна 0. Но если все $k-d-1$ компонент, существующих в силу леммы, окажутся равными 1, то все остальные $d+1$ компонент должны быть равны 0, поскольку сумма всех компонент равна $k-d-1$ согласно равенству 4.

Далее, легко проверить, что если $\widetilde{x}_i = 0$ для некоторого i, то множество $K \setminus \{\mathbf{w}_i\}$ хорошее. Действительно, остальные компоненты в $\widetilde{\mathbf{x}}$ могут играть роль α_i в определении хорошего множества. Утверждение доказано. □

Окончание доказательства теоремы легко проводится по индукции. Начнём с множества $M_n := M$, заведомо хорошего. Используя только что доказанное утверждение, найдём вектор в M_n, при удалении которого получается хорошее множество. Обозначим этот вектор $\mathbf{v}_n$ и положим $M_{n-1} := M_n \setminus \{\mathbf{v}_n\}$. Аналогично, построив хорошее множество M_k, найдём такой вектор $\mathbf{v}_k \in M_k$, что множество $M_{k-1} := M_k \setminus \{\mathbf{v}_k\}$ хорошее, и так далее вплоть до M_d.

Мы получили множество M_d из d векторов, которые мы обозначим в произвольном порядке $\mathbf{v}_1, \ldots, \mathbf{v}_d$. При $k \leqslant d$, очевидно,

$$\|\mathbf{v}_1 + \ldots + \mathbf{v}_k\| \leqslant k \leqslant d,$$

а при $k > d$ норма суммы всех векторов из M_k не превосходит d, поскольку M_k — хорошее множество. Теорема доказана. □

Литература

Эту теорему иногда называют леммой Штейница, поскольку Штейниц дал первое полное доказательство более слабого утверждения в 1913 г., следуя неполному доказательству Леви (1905 г.). Вышеприведённое доказательство взято из заметки

Гринберг В. С., *Севастьянов С. В.* О величине константы Штейница // Функц. анализ и его прил. 1980. Т. 14, вып. 2. С. 56—57.

О контексте и нескольких результатах подобного рода см.

Bárány I. On the power of linear dependencies / Eds. Gy. O. H. Katona, M. Grötschel // Building Bridges: Between Mathematics and Computer Science. Berlin: Springer, 2008. P. 31—46.

Миниатюра 21

Подсчёт остовных деревьев

Остовным деревом графа G называется его связный подграф с тем же множеством вершин, не содержащий циклов. На рис. 13 показан граф с 5 вершинами и одно из его остовных деревьев, выделенное жирными линиями.

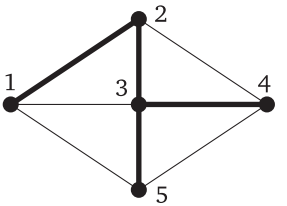


Рис. 13

Каково количество $\kappa(G)$ остовных деревьев данного графа G? Вот ответ.

Теорема (матричная теорема о деревьях).[1] *Пусть G — граф с множеством вершин $\{1, 2, \ldots, n\}$, а L —* **матрица Лапласа** *графа G, т. е. $(n \times n)$-матрица, в которой элемент ℓ_{ij} имеет вид*

$$\ell_{ij} := \begin{cases} \deg(i) & \text{при } i = j, \\ -1 & \text{при } \{i, j\} \in E(G), \\ 0 & \text{в противном случае}, \end{cases}$$

где $\deg(i)$ — количество соседей (степень) вершины i в графе G. Пусть L^- обозначает $((n-1) \times (n-1))$-матрицу, полученную из L удалением последней строки и последнего столбца. Тогда

$$\kappa(G) = \det(L^-).$$

[1] Эта теорема известна также как теорема Кирхгофа. — *Прим. ред.*

Например, для графа G, изображённого на рисунке,

$$L = \begin{pmatrix} 3 & -1 & -1 & 0 & -1 \\ -1 & 3 & -1 & -1 & 0 \\ -1 & -1 & 4 & -1 & -1 \\ 0 & -1 & -1 & 3 & -1 \\ -1 & 0 & -1 & -1 & 3 \end{pmatrix}, \quad L^- = \begin{pmatrix} 3 & -1 & -1 & 0 \\ -1 & 3 & -1 & -1 \\ -1 & -1 & 4 & -1 \\ 0 & -1 & -1 & 3 \end{pmatrix}$$

и $\det(L^-) = 45$. (Сумеете ли вы подсчитать остовные деревья непосредственно?)

До сих пор помню, с каким восхищением я впервые увидел матричную теорему о деревьях. На мой взгляд, она остаётся одним из самых впечатляющих примеров использования определителей. Она довольно хорошо известна, но можно надеяться, что нижеприведённое доказательство — не из числа самых распространённых. При этом оно напоминает доказательство *леммы Гесселя—Вьенно*, которая служит мощным инструментом во многих задачах перечисления.

Доказательство теоремы. Начнём с обычного разложения $\det(L^-)$, исходя из определения определителя как суммы по всем перестановкам индексов $\{1, 2, \ldots, n-1\}$:

$$\det(L^-) = \sum_{\pi} \operatorname{sgn}(\pi) \prod_{i=1}^{n-1} \ell_{i,\pi(i)}. \tag{1}$$

Здесь $\operatorname{sgn}(\pi)$ — знак перестановки π, который можно определить как $(-1)^t$, где t — количество транспозиций при получении π из тождественной перестановки.

Запишем теперь каждый диагональный элемент ℓ_{ii} из L^- в формуле (1) как сумму единиц — например, вместо 3 напишем $(1+1+1)$. Затем перемножим скобки, так что каждое из произведений в формуле (1) разложится в сумму произведений, все сомножители которых равны 1 или -1. Полученную сумму назовём **сверхразложением** определителя $\det(L^-)$.

Поясним это наглядно: чтобы получить каждое ненулевое слагаемое сверхразложения, нужно выбрать по одной единице или минус единице в каждой строке и каждом столбце матрицы L^-. Вот при-

мер, в котором выбранные элементы обведены кружком:

$$\begin{pmatrix} 1+1+1 & \textcircled{-1} & -1 & 0 \\ -1 & 1+1+1 & \textcircled{-1} & -1 \\ \textcircled{-1} & -1 & 1+1+1+1 & -1 \\ 0 & -1 & -1 & 1+\textcircled{1}+1 \end{pmatrix}.$$

Знак такого слагаемого равен $(-1)^m \operatorname{sgn}(\pi)$, где m — количество множителей, равных -1, а π — соответствующая перестановка. В нашем примере $m=3$ и $\pi=(2,3,1,4)$, знак перестановки равен $+1$, так что слагаемое даёт вклад -1 в сверхразложение.

Далее, каждому слагаемому сверхразложения поставим в соответствие комбинаторный объект. Он представляет собой *направленный граф* (или кратко *орграф*) с множеством вершин $\{1, 2, \ldots, n\}$, причём каждое направленное ребро либо *положительно*, либо *отрицательно*. Этот орграф со знаками строится по следующим правилам.

- Если на пересечении строки i и столбца j стоит обведённая минус единица, то из i в j проводится *отрицательное* направленное ребро.
- Если в диагональном элементе ℓ_{ii} обведена k-я единица, то проводится *положительное* направленное ребро из i к k-му наименьшему соседу вершины i в графе G (вершины пронумерованы, так что можно говорить о k-м наименьшем соседе).

В результате для слагаемого, показанного выше кружками, получаем орграф со знаками, показанный на рис. 14 (отрицательные рёбра чёрные, положительные — белые).

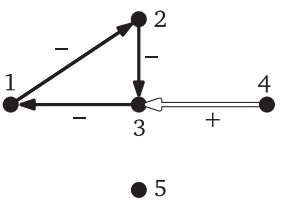


Рис. 14

Пусть $\mathscr{D}$ обозначает множество всех орграфов со знаками D, полученных таким способом из слагаемых сверхразложения. Легко

видеть, что каждый такой орграф $D \in \mathscr{D}$ возникает из ровно одного слагаемого. Поэтому можно говорить о $\operatorname{sgn}(D)$, подразумевая знак соответствующего слагаемого, а соответствующую перестановку обозначать π_D.

Разделим $\mathscr{D}$ на три части следующим образом:

- $\mathscr{T}$ — орграфы $D \in \mathscr{D}$ без направленных циклов;
- $\mathscr{D}^+$ — орграфы $D \in \mathscr{D}$ с $\operatorname{sgn}(D) = +1$ и хотя бы одним направленным циклом;
- $\mathscr{D}^-$ — орграфы $D \in \mathscr{D}$ с $\operatorname{sgn}(D) = -1$ и хотя бы одним направленным циклом.

Дальнейший план доказательства таков. Мы покажем, что все $D \in \mathscr{T}$ — «ациклические объекты» — имеют положительный знак и взаимно однозначно соответствуют остовным деревьям графа G; таким образом, их количество нам и нужно. Затем, построив подходящую биекцию, мы докажем, что $|\mathscr{D}^+| = |\mathscr{D}^-|$. Тогда мы получим

$$\det(L^-) = \sum_{D \in \mathscr{D}} \operatorname{sgn}(D) = |\mathscr{T}| + |\mathscr{D}^+| - |\mathscr{D}^-| = |\mathscr{T}|$$

и теорема будет доказана.

Чтобы осуществить этот план, вначале перечислим несколько простых свойств орграфов из $\mathscr{D}$.

(i) *Если $i \to j$ — направленное ребро, то $\{i, j\}$ — ребро графа G.* (Очевидно.)

(ii) *Из каждой вершины, кроме n, выходит ровно одно ребро, а из n ни одно ребро не выходит.* (Очевидно.)

(iii) *Все рёбра, входящие в n, положительны.* (Поскольку L^- имеет лишь $n-1$ строк и столбцов.)

(iv) *В каждую вершину входит не более одного отрицательного ребра.* (Поскольку два отрицательных входящих ребра $j \to i$ и $k \to i$ означали бы два обведённых элемента ℓ_{ji} и ℓ_{ki} в i-м столбце.)

(v) *Если в вершину i входит отрицательное ребро, то исходящее ребро также отрицательно.* (Действительно, отрицательное входящее ребро $j \to i$ означает, что обведён недиагональный элемент ℓ_{ji} и потому не может быть обведена единица в диагональном элементе ℓ_{ii}, а это единственный способ получить положительное ребро, исходящее из i.)

Утверждение A. *Перечисленные свойства характеризуют $\mathscr{D}$. Иными словами, если орграф D со знаками удовлетворяет условиям* (i)—(v), *то $D \in \mathscr{D}$.*

Доказательство утверждения A. Для данного D найдём обведённый элемент в каждой строке i $(1 \leqslant i \leqslant n-1)$ матрицы L^-. Рассмотрим единственное выходящее из него ребро $i \to j$. Если оно положительно, то обведём соответствующую единицу в элементе ℓ_{ii}, а если отрицательно, то обведём ℓ_{ij}. В одном столбце не может быть двух обведённых элементов, поскольку они отвечали бы ситуациям, исключённым в силу условий (iv) и (v)[1]. □

Теперь применим свойства (i)—(v), чтобы описать структуру графа D.

Утверждение B. *Каждый орграф $D \in \mathscr{D}$ имеет следующую структуру* (*показанную на рис.* 15).

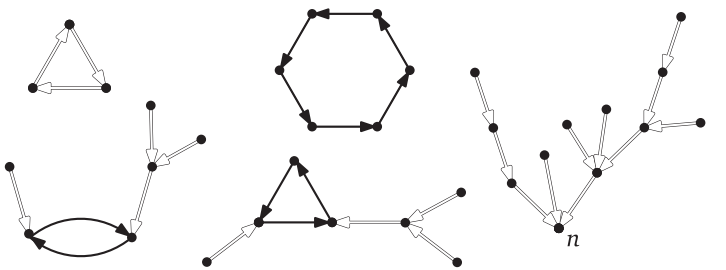


Рис. 15

(a) *Множество вершин состоит из одного или более непересекающихся подмножеств $V_1, V_2, \ldots, V_k$, отвечающих компонентам графа D, причём различные V_i не соединены рёбрами. Если подмножество V_1 содержит вершину n, то подграф с множеством вершин V_1 является деревом, все рёбра которого направлены в сторону n. Подграф с любым другим V_i в качестве множества вершин содержит ровно один направленный цикл длины не меньше 2 и для каждой его вершины — содержащее её дерево* (*возможно, пустое*), *рёбра которого направлены в сторону цикла.*

[1] Если обведены два недиагональных элемента, то нарушается условие (iv), а если обведена единица, отвечающая элементу ℓ_{ii}, и недиагональный элемент ℓ_{ij}, то в вершину i входит отрицательное ребро, а исходит из неё положительное, что противоречит условию (v). — *Прим. перев.*

(b) *Все рёбра, не принадлежащие направленным циклам, положительны, а в каждом направленном цикле либо все рёбра положительны, либо все рёбра отрицательны.*

(c) *Обратно, любой орграф D с такой структурой, удовлетворяющий условию* (i), *принадлежит $\mathscr{D}$.*

Набросок доказательства утверждения B. Пункт (a) непосредственно вытекает из условия (ii) (единственность исходящего ребра для каждой вершины, кроме n), и мы предоставляем его в качестве упражнения. (Если добавить направленную петлю при вершине n, то у каждой вершины будет ровно одно исходящее ребро и мы получим так называемый *функциональный орграф*, для которого структура, описанная в п. (a), хорошо известна.)

Перейдём к п. (b). Если начать путь по графу с отрицательного ребра, то в силу условия (v) нам встретятся только отрицательные рёбра. Значит, мы не сможем достичь вершины n, поскольку входящие в неё рёбра положительны, и с какого-то момента начнём двигаться по отрицательному циклу. При этом отрицательное ребро не может войти извне в такой цикл в силу условия (iv).

Что касается п. (c), то для графа D со структурой, описанной в п. (a) и (b), условия (ii)—(v) заведомо выполнены и можно применить утверждение A. Тем самым доказано утверждение B. □

Теперь совсем легко завершить первую часть нашего плана.

Следствие. *Все $D \in \mathscr{T}$ имеют положительный знак. Они взаимно однозначно соответствуют остовным деревьям графа G.*

Доказательство следствия. Если $D \in \mathscr{D}$ не содержит направленных циклов, то D является деревом с положительными рёбрами, направленными в сторону вершины n. При этом перестановка π_D тождественная, поскольку все обведённые элементы в слагаемом, отвечающем графу D, лежат на диагонали матрицы L^-. Значит, $\operatorname{sgn}(D) = +1$, и если забыть об ориентациях рёбер, то получится остовное дерево графа G. Обратно, если дано остовное дерево графа G, то можно ориентировать его рёбра в сторону n и получить орграф $D \in \mathscr{T}$. □

Осталось разобраться с «циклическими объектами». Пусть $D \in \in \mathscr{D}^+ \cup \mathscr{D}^-$. Назовём *наименьшим циклом* направленный цикл, содержащий вершину с наименьшим номером (среди всех вершин в циклах). Пусть $\overline{D}$ получается из D переменой знака всех рёбер в наименьшем цикле.

Очевидно, $\overline{\overline{D}} = D$, и если $D \in \mathscr{D}$, то и $\overline{D} \in \mathscr{D}$, как можно видеть из утверждения B. Следующее утверждение показывает, что отображение, переводящее D в $\overline{D}$, является биекцией между $\mathscr{D}^+$ и $\mathscr{D}^-$, а это всё, что требуется, чтобы завершить доказательство теоремы.

Утверждение C. *Справедливо равенство* $\operatorname{sgn}(\overline{D}) = -\operatorname{sgn}(D)$.

Доказательство утверждения C. Выполнено равенство

$$\operatorname{sgn}(D) = \operatorname{sgn}(\pi_D)(-1)^m,$$

где m — количество отрицательных рёбер в графе D, а π_D — ассоциированная перестановка.

Пусть $i_1, i_2, \ldots, i_s$ — вершины наименьшего цикла в D, занумерованные так, что направленные рёбра цикла имеют вид $i_1 \to i_2$, $i_2 \to i_3$, …, $i_{s-1} \to i_s$, $i_s \to i_1$.

В одном из графов D и $\overline{D}$ наименьший цикл положителен, например в D (если он положителен в $\overline{D}$, рассуждение аналогично). Положительные рёбра отвечают диагональным элементам в L^-, поэтому i_j являются неподвижными точками перестановки π_D, т. е. $\pi_D(i_j) = i_j$, $j = 1, 2, \ldots, s$. В графе $\overline{D}$ наименьший цикл отрицателен, так что $\pi_{\overline{D}}(i_1) = i_2, \ldots, \pi_{\overline{D}}(i_{s-1}) = i_s$, $\pi_{\overline{D}}(i_s) = i_1$, т. е. вершины $i_1, i_2, \ldots, i_s$ образуют *цикл* перестановки $\pi_{\overline{D}}$.

Теперь легко проверить, что $\pi_{\overline{D}}$ можно преобразовать в π_D посредством $s-1$ транспозиций («уничтожающих» цикл $(i_1, i_2, \ldots, i_s)$). Поскольку каждая транспозиция меняет знак перестановки, получаем $\operatorname{sgn}(\pi_{\overline{D}}) = (-1)^{s-1}\operatorname{sgn}(\pi_D)$, откуда следует, что

$$\operatorname{sgn}(\overline{D}) = \operatorname{sgn}(\pi_{\overline{D}})(-1)^{m+s} = (-1)^{s-1}\operatorname{sgn}(\pi_D)(-1)^{m+s} = -\operatorname{sgn}(D).$$

Утверждение C доказано. □

Тем самым доказана и теорема. □

Литература

Источником этой теоремы обычно считается работа[1]

Kirchhoff G. Über die Auflösung der Gleichungen, auf welche man bei der Untersuchung der linearen Verteilung galvanischer Ströme geführt wird // Ann. Phys. Chem. 1847. V. 148, № 12. P. 497—508,

[1] Русский перевод этой статьи доступен в книге: *Кирхгоф Г. Р.* Избранные труды. М.: Наука, 1988. В ней содержатся и другие замечательные результаты. Один из них говорит о том, как рассчитывать сопротивление между узлами электрической сети, подсчитывая остовные деревья. В этой же статье сформулированы правила Кирхгофа, которые сводят нахождение токов в электрической сети к решению системы линейных уравнений. Второй замечательный

а первым полным доказательством — содержащееся в статье

Sylvester J. J. On the change of systems of independent variables // Quart. J. Pure Appl. Math. 1857. V. 1. P. 42—56.

Вышеприведённое доказательство в основном следует работе

Benjamin A. T., *Cameron N. T.* Counting on determinants // Amer. Math. Monthly 2005. V. 112. P. 481—492.

Бенджамин и Кэмерон указывают как источник доказательства статью

Chaiken S. A Combinatorial proof of the all-minors matrix tree theorem // SIAM J. Alg. Disc. Methods. 1982. V. 3, № 3. P. 319—329,

но его там нелегко обнаружить, так как в статье рассматривается более общая ситуация.

результат статьи — теорема о том, что система линейных уравнений, составленная по правилам Кирхгофа, всегда имеет единственное решение. В конце миниатюры 12 уже упоминалась связь между электрическими сетями на плоскости и замощениями прямоугольника квадратами. Если задано разбиение прямоугольника на квадраты, то можно составить систему линейных уравнений, неизвестными в которой будут стороны квадратов разбиения. Результат Кирхгофа означает, что решение этой системы также всегда существует и однозначно определено. (Однако нет гарантии, что решения окажутся неотрицательными числами.) — *Прим. ред.*

Миниатюра 22

Сколькими способами можно замостить доску?

Ответ, друзья мои, имеет вид определителя, по крайней мере во многих интересных случаях.

Существует 12 988 816 замощений шахматной доски 8×8 доминошками (прямоугольниками 2×1). На рис. 16 показано одно из них.

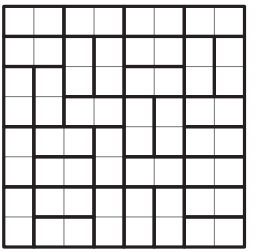


Рис. 16

Как их можно сосчитать?

Из рис. 17 видно, что замощения шахматной доски доминошками биективно соответствуют **совершенным паросочетаниям**[1] в соответствующем **решётчатом** графе.

Рис. 17

[1] Совершенным паросочетанием в графе G называется такое подмножество $M \subseteq E(G)$ множества его рёбер, что каждая вершина графа принадлежит ровно одному ребру из M.

Другой популярный вид замощений — **ромбические замощения**. В этом случае доска составлена из равносторонних треугольников, а плитки замощения — ромбы трёх видов, полученные склеиванием двух смежных треугольников.

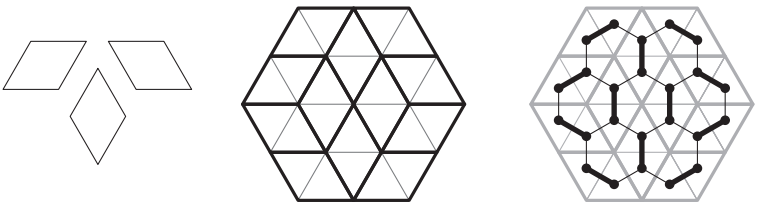


Рис. 18

Как показано на рис. 18 справа, эти замощения соответствуют совершенным паросочетаниям в **сотах**.

Объясним теперь, как выразить количества совершенных паросочетаниях в этих и многих других графах через определители. Сначала потребуется ввести некоторые понятия.

Двудольная матрица смежности и кастелейновы расстановки знаков. Напомним, что граф G называется **двудольным**, если его вершины можно разделить на два класса

$$\{u_1, u_2, \ldots, u_n\} \quad \text{и} \quad \{v_1, v_2, \ldots, v_m\}$$

таким образом, что рёбра проходят только между классами, но не внутри одного класса.

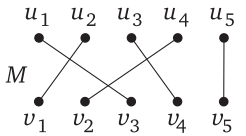
Можно считать, что $m = n$, т. е. размер классов одинаков, так как в противном случае совершенное паросочетание не существует.

Определим **двудольную матрицу смежности** такого графа G как $(n \times n)$-матрицу B вида

$$b_{ij} := \begin{cases} 1 & \text{при } \{u_i, v_j\} \in E(G), \\ 0 & \text{в противном случае.} \end{cases}$$

Пусть S_n обозначает множество всех перестановок множества $\{1, 2, \ldots, n\}$. Каждое совершенное паросочетание M в графе G соответствует однозначно определённой перестановке $\pi \in S_n$, где $\pi(i)$ —

тот индекс j, для которого ребро $\{u_i, v_j\}$ лежит в M. Пример показан на рис. 19.



$\pi(1)=3,\ \pi(2)=1,\ \pi(3)=4,\ \pi(4)=2,\ \pi(5)=5$

Рис. 19

Обратно: когда в G существует совершенное паросочетание, соответствующее данной перестановке $\pi \in S_n$? В точности тогда, когда $b_{1,\pi(1)} = b_{2,\pi(2)} = \ldots = b_{n,\pi(n)} = 1$. Следовательно, количество совершенных паросочетаний в G равно $\sum\limits_{\pi\in S_n} b_{1,\pi(1)} b_{2,\pi(2)} \ldots b_{n,\pi(n)}$.

Это выражение называется **перманентом** матрицы B и обозначается $\mathrm{per}(B)$. Понятие перманента имеет смысл для любых квадратных матриц, но здесь мы ограничимся двудольными матрицами смежности, которые заполнены нулями и единицами.

Приведённая выше формула перманента выглядит очень похоже на определение определителя; последний имеет «лишь» один дополнительный коэффициент $\mathrm{sgn}(\pi)$ перед каждым слагаемым. Но на самом деле это различие — важнейшее: у перманента отсутствуют многие привлекательные свойства определителя, и если определитель можно вычислить за разумное время даже для больших матриц, то вычисление перманента трудоёмко даже для матриц из нулей и единиц[1].

Вот ключевая идея этого раздела. Нельзя ли устранить эффект множителя $\mathrm{sgn}(\pi)$, поменяв знаки на некотором правильно выбранном подмножестве из b_{ij} и тем самым превратив *перманент* матрицы B в *определитель* некоторой другой матрицы? Как мы увидим, для многих графов это возможно. Введём определение, выражающее эту идею более формально.

Расстановкой знаков на G будем называть произвольное приписывание знаков его рёбрам, т. е. отображение $\sigma\colon E(G) \to \{-1, +1\}$. Определим матрицу B^σ, состоящую из «знаков матрицы B», положив

$$b_{ij}^\sigma := \begin{cases} \sigma(u_i, v_j) & \text{при } \{u_i, v_j\} \in E(G), \\ 0 & \text{в противном случае.} \end{cases}$$

[1] В терминах сложности вычислений нахождение перманента матрицы из нулей и единиц, равносильное подсчёту совершенных паросочетаний в двудольном графе, является #P-полным.

Назовём σ **расстановкой знаков Кастелейна (кастелейновой расстановкой знаков)** в графе G, если

$$|\det(B^\sigma)| = \mathrm{per}(B).$$

Не для всех двудольных графов существует кастелейнова расстановка знаков; например, её нет для полного двудольного графа $K_{3,3}$, как может проверить прилежный и энергичный читатель. Но оказывается что для всех *планарных*[1] двудольных графов такие расстановки существуют.

Чтобы сосредоточиться на сути дела и обойти некоторые технические подробности, будем рассматривать только **двусвязные** графы. Это означает, что граф связен и каждое ребро содержится хотя бы в одном цикле (что верно для решётчатых графов и для сот). Хорошо известно и без труда проверяется, что если изобразить двусвязный граф G на плоскости, то граница каждой полученной области образует цикл в G.

Теорема. *Для каждого двусвязного планарного двудольного графа G существует кастелейнова расстановка знаков и её можно найти эффективно*[2]*. Как отсюда следует, количество совершенных паросочетаний в таком графе может быть вычислено за полиномиальное время.*

Для решётчатых графов из приведённых примеров замощений кастелейнова расстановка знаков оказывается очень простой. Для квадратной решётки она показана на рис. 20.

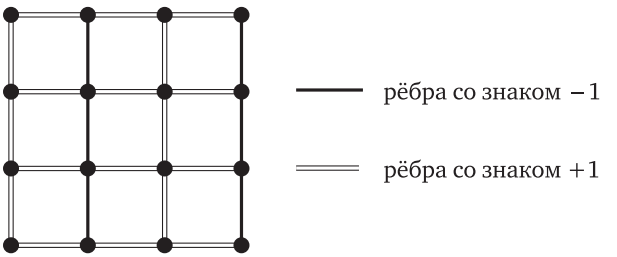


Рис. 20

[1] Напомним, что граф **планарен**, если его можно изобразить на плоскости без пересечений рёбер не по вершинам.

[2] Из доказательства очевидно следует алгоритм её отыскания за полиномиальное время, но некоторая дополнительная работа позволяет получить даже линейное время.

В шестиугольной решётке можно даже дать всем рёбрам знак $+1$. Оба эти факта сразу вытекают из леммы B (см. ниже).

Ограничение двусвязными графами можно удалить из условия теоремы без большого труда. Ограничение *двудольными* графами также несущественно. Оно слегка упрощает изложение, но можно аналогичным образом развить теорию и для недвудольного случая — заинтересованные читатели найдут её в литературе.

С другой стороны, допущение о *планарности* более существенно: метод, безусловно, не годится для произвольного непланарного графа и, как отмечено выше, подсчёт совершенных паросочетаний в произвольном графе представляет вычислительную трудность. Класс графов, где работает данный подход, — так называемые *графы Пфаффа* — несколько шире, чем класс планарных графов, но его нелегко описать, так что в большинстве приложений рассматриваются планарные графы.

Правильно помеченные циклы. В качестве первого шага к доказательству дадим достаточный признак кастелейновости расстановки знаков. На первый взгляд он выглядит загадочно, но из доказательства мы увидим, откуда он возникает.

Пусть C — цикл в двудольном графе G. Тогда C имеет чётную длину, которую мы обозначим 2ℓ. Пусть σ — расстановка знаков в G, а n_C — количество *отрицательных рёбер* (т. е. рёбер со знаком -1). Назовём цикл C **правильно помеченным** относительно σ, если

$$n_C \equiv \ell - 1 \pmod 2.$$

Иначе говоря, правильно помеченный цикл длины 4, 8, 12, … содержит нечётное количество отрицательных рёбер, а правильно помеченный цикл длины 6, 10, 14, … — чётное.

Далее, будем говорить, что цикл C **равномерно размещён**, если при удалении из G всех вершин цикла C (и смежных с ними рёбер) получается граф с совершенным паросочетанием.

Лемма A. *Пусть σ — расстановка знаков в двудольном графе G (планарность здесь не предполагается), причём каждый равномерно размещённый цикл в G правильно помечен. Тогда расстановка знаков σ является кастелейновой.*

Доказательство леммы A. Лемма доказывается прямолинейно. Пусть зафиксирована расстановка знаков σ из условия леммы, и пусть M — совершенное паросочетание в графе G, отвечающее перестановке π. В качестве его **знака** возьмём знак соответствующего

слагаемого в $\det(B^\sigma)$; в явном виде

$$\operatorname{sgn}(M) := \operatorname{sgn}(\pi) b^\sigma_{1,\pi(1)} b^\sigma_{2,\pi(2)} \ldots b^\sigma_{n,\pi(n)} = \operatorname{sgn}(\pi) \prod_{e\in M} \sigma(e).$$

Легко видеть, что расстановка знаков σ будет кастелейновой тогда (и только тогда), когда все совершенные паросочетания в графе G имеют одинаковый знак.

Пусть M и M' — два совершенных паросочетания в графе G, а π и π' — соответствующие перестановки. Тогда

$$\operatorname{sgn}(M)\operatorname{sgn}(M') = \operatorname{sgn}(\pi)\operatorname{sgn}(\pi')\Big(\prod_{e\in M}\sigma(e)\Big)\Big(\prod_{e\in M'}\sigma(e)\Big) =$$
$$= \operatorname{sgn}(\pi)\operatorname{sgn}(\pi') \prod_{e\in M\triangle M'} \sigma(e),$$

гдео $\triangle$ обозначает симметрическую разность.

Симметрическая разность $M\triangle M'$ является дизъюнктным объединением равномерно размещённых циклов, как видно из рис. 21.

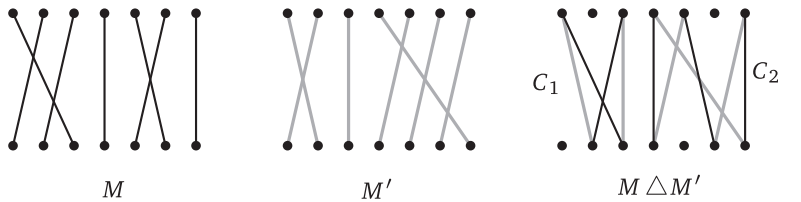


Рис. 21

Пусть $C_1, C_2, \ldots, C_k$ — эти циклы, причём длина цикла C_i равна $2\ell_i$. Поскольку C_i равномерно размещён, он согласно условию леммы правильно помечен, а значит, $\prod_{e\in C_i}\sigma(e) = (-1)^{\ell_i - 1}$. Таким образом,

$$\prod_{e\in M\triangle M'} \sigma(e) = (-1)^t,$$

где $t := \ell_1 - 1 + \ell_2 - 1 + \ldots + \ell_k - 1$.

Осталось проверить, что π можно преобразовать в π' за t транспозиций (тогда в силу свойств знака перестановки

$$\operatorname{sgn}(\pi) = (-1)^t \operatorname{sgn}(\pi'),$$

а значит, $\operatorname{sgn}(M) = \operatorname{sgn}(M')$, что и требуется).

Это можно проделать по очереди для каждого цикла C_i. Как показано на рис. 22 для цикла длины $2\ell_i = 8$, применив к π подходящую транспозицию, можно «вычеркнуть» из цикла два ребра и перейти к циклу длины $2\ell_i - 2$ (чёрные рёбра принадлежат множеству M, серые — множеству M', а пунктирное ребро на правом рис. 22 принадлежит теперь обоим множествам).

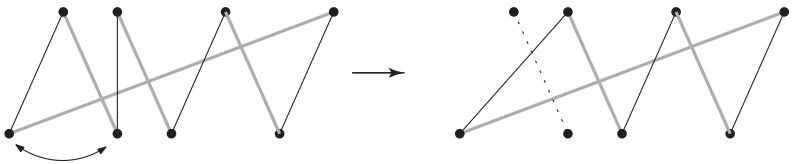


Рис. 22

Выполнив $\ell_i - 1$ таких шагов, мы вычеркнем C_i и можем перейти к следующему циклу. Лемма А доказана. □

Доказательство теоремы завершается простыми теоретико-графовыми рассуждениями. Вначале покажем, что в случае графов, о которых говорится в теореме, достаточно проверить условие леммы А лишь для циклов специального вида, а именно границ областей. Ясно, что достаточно рассматривать *связные* графы.

Лемма В. *Пусть G — планарный двудольный двусвязный граф. Зафиксируем его изображение на плоскости. Пусть σ — расстановка знаков на G, причём граничный цикл каждой внутренней области на чертеже правильно помечен. Тогда расстановка знаков σ кастелейнова.*

Доказательство леммы В. Пусть C — равномерно размещённый цикл в графе G; нужно доказать в силу леммы А, что он правильно помечен.

Пусть длина цикла C равна 2ℓ; $F_1, \ldots, F_k$ — внутренние области, расположенные на рис. 23 внутри C; C_i $(i = 1, \ldots, k)$ — граничный цикл области F_i, имеющий длину $2\ell_i$; H — подграф в G, полученный удалением всех вершин и рёбер, начерченных вне C; иначе говоря, H — объединение всех C_i.

Мы хотим понять, как чётность числа ℓ связана с чётностями ℓ_i. Это потребует некоторых вычислений. Количество вершин в H равно $r + 2\ell$, где r — количество вершин, лежащих внутри C. Каждое ребро в H принадлежит ровно двум циклам из $C, C_1, \ldots, C_k$, так что

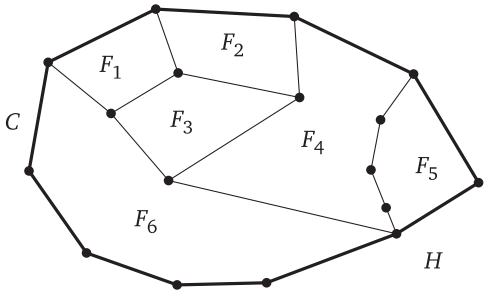


Рис. 23

количество рёбер в H равно $\ell+\ell_1+\ldots+\ell_k$. Наконец, изображение графа H содержит $k+1$ областей: F_1, ..., F_k и одну внешнюю.

Применим теперь **формулу Эйлера**, согласно которой на любом изображении связного планарного графа сумма количества вершин и количества областей равна количеству рёбер плюс 2. Значит,

$$r+2\ell+k+1=\ell+\ell_1+\ldots+\ell_k+2. \tag{1}$$

Теперь используем условие, что цикл C равномерно размещён. Поскольку граф, полученный удалением из G этого цикла и всех смежных с ним рёбер, обладает совершенным паросочетанием, количество r вершин внутри C должно быть чётным. Поэтому из равенства (1) вытекает, что

$$\ell-1\equiv\ell_1+\ldots+\ell_k-k \pmod 2. \tag{2}$$

Пусть n_C — количество отрицательных рёбер в C, и аналогично определим n_{C_i}. Сумма $n_C+n_{C_1}+\ldots+n_{C_k}$ чётна, поскольку в неё включены по два раза все отрицательные рёбра, т. е.

$$n_C\equiv n_{C_1}+\ldots+n_{C_k} \pmod 2. \tag{3}$$

Наконец, $n_{C_i}\equiv\ell_i-1 \pmod 2$, поскольку циклы C_i правильно помечены. Объединяя это соотношение с формулами (2) и (3), получаем

$$n_C\equiv\ell-1 \pmod 2.$$

Значит, цикл C правильно помечен. Теперь лемма B вытекает из леммы A. □

Доказательство теоремы. Пусть дан связный двусвязный планарный двудольный граф G. Зафиксируем некоторое его изображение на плоскости. Мы хотим построить такую расстановку знаков,

как в лемме B, т. е. чтобы граница каждой внутренней области была правильно помечена.

Сначала займёмся удалением рёбер из G, как показано на рис. 24.

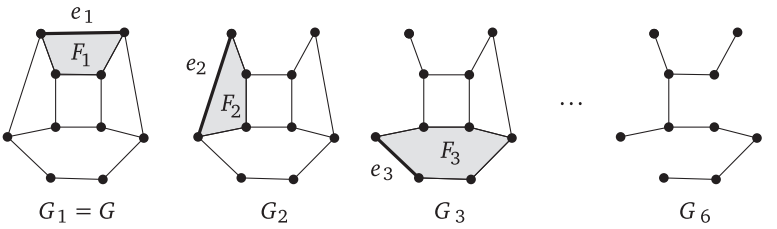


Рис. 24

Положим $G_1 := G$, и пусть G_{i+1} получается из G_i удалением ребра e_i, отделяющего внутреннюю область F_i от внешней (неограниченной) области (в данном изображении). Процесс останавливается на некотором графа G_k, не имеющем такого ребра. Изображение G_k тогда имеет лишь внешнюю область.

Теперь на рёбрах графа G_k произвольно расставим знаки. Продолжим эту расстановку на все рёбра графа G обратным ходом, расставляя знаки на рёбрах $e_{k-1}, e_{k-2}, \ldots, e_1$ в таком порядке. Каждое e_i содержится в границе ровно одной внутренней области F_i в изображении графа G_i, поэтому можно выбрать $\sigma(e_i)$ так, чтобы граница области F_i была правильно помечена. Теорема доказана. □

Из формулы, выражающей количество совершенных паросочетаний через определитель, можно получить, ценой некоторых усилий, следующую замечательную формулу для количества замощений доминошками доски $m \times n$:

$$\left[\prod_{k=1}^{m}\prod_{\ell=1}^{n}\Big(2\cos\frac{\pi k}{m+1}+2\mathrm{i}\cos\frac{\pi\ell}{n+1}\Big)\right]^{1/2},$$

где i — мнимая единица. Но определители можно использовать не только для подсчёта, но и для генерирования *случайных* совершенных паросочетаний (равномерно распределённых среди всех возможных совершенных паросочетаний) и для анализа их характерных свойств. Подобные результаты имеют отношение к проблемам теоретической физики.

Кстати, вот картинка интересного явления, связанного со случайными замощениями. На рис. 25 показано случайное ромбическое замощение большого шестиугольника.

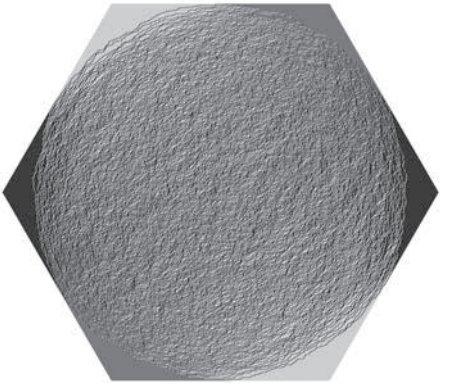


Рис. 25

Три типа плиток закрашены чёрным, белым и серым. Можно видеть, что, хотя в центральном круге замощение выглядит хаотичным, области вне этого круга «заморожены», т. е. каждая покрыта ромбами одного типа. (Это свойство характерно для *случайного* замощения — заведомо *не все* замощения так выглядят.) Это так называемый «феномен полярного круга».

В зависимости от формы многоугольника, роль полярного круга могут играть различные сложные кривые. В некоторых случаях вообще нет «замороженных» областей — например, замощения доминошками прямоугольных досок выглядят повсюду хаотично. Формула, использующая определитель, обеспечивает принципиальную основу для анализа таких явлений.

Литература[1]

Подсчёт совершенных паросочетаний имеет значение в различных областях науки: математики нередко говорят о *замощениях*, информатики — о *совершенных паросочетаниях*, а физики — о *модели димера* (это весьма упрощённая, но всё же интересная модель в физике твёрдого те-

[1] Дополнительные точки зрения на задачи о замощениях читатель может найти в брошюре: *Смирнов Е. Ю.* Три взгляда на ацтекский бриллиант. М: МЦНМО, 2015. — *Прим. ред.*

ла). Идея подсчёта совершенных паросочетаний в квадратной решётке через определители была выдвинута в контексте модели димера в статье

Kasteleyn P. W. The statistics of dimers on a lattice I. The number of dimer arrangements on a quadratic lattice // Physica. 1961. V. 27. P. 1209—1225

и независимо в заметке

Temperley H. N. V., *Fisher M. E.* Dimer problem in statistical mechanics—An exact result // Philos. Magazine. 1961. V. 6. P. 1061—1063.

Материал этого раздела служит отправным пунктом замечательных теорий различной направленности. Знакомство с ними можно начать, например, с работ

Kenyon R. The planar dimer model with boundary: A survey // Directions in Mathematical Quasicrystals, CRM Monograph. Ser. 13. Providence, R.I.: Amer. Math. Soc., 2000. P. 307—328

(где рассматриваются замощения, димеры, феномен полярного круга, случайные поверхности и т.п.) и

Thomas R. A survey of Pfaffian orientations of graphs // International Congress of Mathematicians. V. III. Zürich: Eur. Math. Soc., 2006. P. 963—984

(графы Пфаффа в теоретико-графовом и алгоритмическом аспекте).

Миниатюра 23

Больше кирпичей — больше стенок?

Одна из классических тем в теории перечислений — **целочисленные разбиения**. Например, существуют пять целочисленных разбиений числа 4:

$$4 = 1+1+1+1+1,$$
$$4 = 2+1+1+1,$$
$$4 = 2+2,$$
$$4 = 3+1,$$
$$4 = 4.$$

Порядок слагаемых в разбиении несуществен, и принято записывать их в порядке невозрастания, как мы сделали выше.

Часто изображают разбиение целого числа k графически посредством **диаграммы Ферре**, которую можно представлять себе как неубывающую последовательность столбцов (стенку) из k кирпичей. Например, диаграмма Ферре, показанная на рис. 26, соответствует разбиению $16 = 5+3+3+2+1+1+1$.

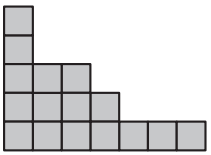


Рис. 26

Как найти или оценить количество разбиений числа k, которое мы обозначим $p(k)$? Эта задача теории перечислений неожиданно трудна и в итоге решается формулой Харди — Рамануджана. Асимптотика $p(k)$ имеет вид

$$p(k) \sim \frac{1}{4k\sqrt{3}} e^{\pi\sqrt{2k/3}},$$

где запись $f(k) \sim g(k)$ означает, что $\lim_{k\to\infty} \frac{f(k)}{g(k)} = 1$.

Здесь мы рассмотрим другую величину — количество $p_{w,h}(k)$ разбиений числа k, содержащих не более w слагаемых, каждое из которых не превосходит h. Иначе говоря, $p_{w,h}(k)$ — количество способов построить невозрастающую стенку из k кирпичей внутри ящика ширины w и высоты h (см. рис. 27)[1].

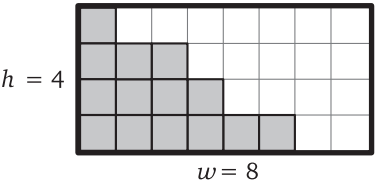


Рис. 27

Вот главный результат этого раздела.

Теорема. *Для любых $w \geqslant 1$ и $h \geqslant 1$ выполнены неравенства*[2]

$$p_{w,h}(0) \leqslant p_{w,h}(1) \leqslant \ldots \leqslant p_{w,h}\left(\left\lfloor \frac{wh}{2} \right\rfloor\right)$$

и

$$p_{w,h}\left(\left\lceil \frac{wh}{2} \right\rceil\right) \geqslant p_{w,h}\left(\left\lceil \frac{wh}{2} \right\rceil + 1\right) \geqslant \ldots \geqslant p_{w,h}(wh-1) \geqslant p_{w,h}(wh).$$

Иначе говоря, $p_{w,h}(k)$ как функция от k не убывает при $k \leqslant \frac{wh}{2}$ и не возрастает при $k \geqslant \frac{wh}{2}$.

Таким образом, первая часть теоремы утверждает, что при большем количестве кирпичей можно построить больше (или хотя бы столько же) стенок. Так продолжается, пока кирпичи не заполнят половину ящика; после этого остаётся уже слишком мало места и количество возможных стенок начинает убывать.

На самом деле если величина $p_{w,h}(k)$ не убывает при $k \leqslant \frac{wh}{2}$, то она не может возрастать при $k \geqslant \frac{wh}{2}$, поскольку

$$p_{w,h}(k) = p_{w,h}(wh-k),$$

[1] Если зафиксировать размеры ящика w и k, то можно все значения $p_{w,h}(k)$ собрать в единую производящую функцию $f_{w,h}(q) = \sum_k p_{w,h}(k) q^k$. Такие функции известны как многочлены Гаусса, а также как гауссовы биномиальные коэффициенты или как q-аналоги биномиальных коэффициентов. Их свойства во многом аналогичны свойствам обычных биномиальных коэффициентов. — *Прим. ред.*

[2] Напомним, что $\lfloor x \rfloor$ и $\lceil x \rceil$ означают целые числа, ближайшие к x снизу и сверху соответственно. — *Прим. перев.*

как показывает биекция на рис. 28, превращающая стенки из k кирпичей в стенки из $wh-k$ кирпичей.

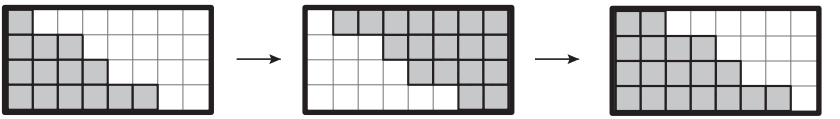


Рис. 28

Эта теорема — одна из тех, что интуитивно очевидны, но доказываются неожиданно трудно. Великий Кэли в своём мемуаре 1856 г. использовал этот факт как не требующий доказательства, однако первое доказательство было найдено Сильвестром лишь примерно через двадцать лет.

Естественно ожидать, что подобная комбинаторная задача имеет и комбинаторное решение, может быть, просто в виде вложения, сопоставляющего каждой стенке из k кирпичей стенку из $k+1$ кирпичей (при $k+1\leqslant\frac{wh}{2}$). Но, насколько я знаю, никому не удалось найти доказательство такого рода. С другой стороны, оценка величины $p_{w,h}(k)$ или выражение её в виде формулы вряд ли приводит к цели.

Ранние доказательства этой теоремы использовали довольно громоздкий инструментарий — в основном представления алгебр Ли. Доказательство, приведённое здесь, явилось результатом нескольких упрощений первоначальных идей и использует «только» соображения о ранге матриц.

Функции и последовательности, которые вначале не убывают, а начиная с некоторой точки не возрастают, называются **унимодальными** (так же как и функции, которые вначале не возрастают, а потом не убывают). В разных областях математики есть много важных результатов и гипотез о том, что некие величины образуют унимодальную последовательность, и приведённое ниже доказательство содержит приёмы с широкой возможностью применения.

Предварительные рассмотрения. Пусть $n:=wh$ обозначает площадь основания ящика. Занумеруем n единичных клеток основания числами $1, 2, \ldots, n$.

Чтобы доказать теорему, покажем, что

$$p_{w,h}(k) \leqslant p_{w,h}(\ell) \quad \text{при } 0 \leqslant k < \ell \leqslant \frac{n}{2}.$$

Прежде всего представим стенку как *класс эквивалентности*. А именно, возьмём произвольное множество из k кирпичей, заполняющих некоторые k клеток в ящике, и соберём из них невозрастающую стенку (см. рис. 29).

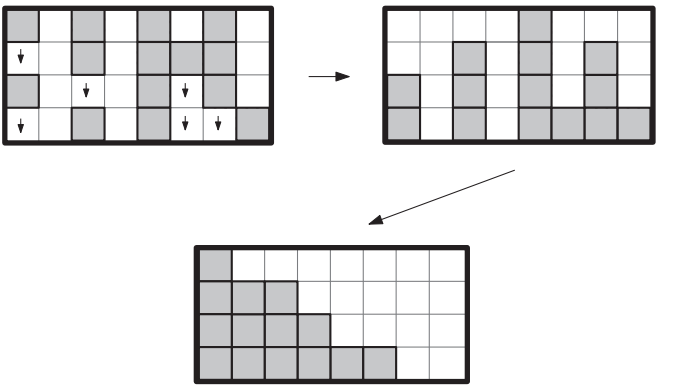


Рис. 29

Сначала мы в каждом столбце спускаем кирпичи вниз, а затем переставляем столбцы в порядке невозрастания.

Назовём два k-элементных подмножества $K, K' \subseteq \{1, 2, \ldots, n\}$, считая их множествами из k клеток в ящике, **(стеночно) эквивалентными** (wall-equivalent), если они порождают одну и ту же невозрастающую стенку. Тем самым действительно определено отношение эквивалентности на множестве $\mathscr{K}$ всех k-элементных подмножеств множества $\{1, 2, \ldots, n\}$. Обозначим классы этой эквивалентности $\mathscr{K}_1, \mathscr{K}_2, \ldots, \mathscr{K}_r$, где $r := p_{w,h}(k)$.

Теперь сформулируем определение той же эквивалентности по-другому, что в дальнейшем окажется удобнее. Пусть π — некоторая перестановка n клеток в ящике; будем говорить, что перестановка π **не ломает столбцы**, если она вначале переставляет клетки в каждом столбце, а затем переставляет столбцы. Легко видеть, что два подмножества $K, K' \in \mathscr{K}$ эквивалентны в точности тогда, когда $K' = \pi(K)$, где π — некоторая перестановка, не ломающая столбцы[1].

[1] На более развитом математическом языке перестановки, не ломающие столбцы, образуют группу перестановок, действующую на $\mathscr{K}$, а классы эквива-

Далее, пусть $\mathscr{L}$ — множество всех ℓ-элементных подмножеств множества $\{1, 2, \ldots, n\}$, и пусть оно аналогично разделено на $s := p_{w,h}(\ell)$ классов эквивалентности $\mathscr{L}_1, \ldots, \mathscr{L}_s$. Мы хотим доказать, что $r \leqslant s$.

Рассмотрим двудольный граф G с множеством вершин $\mathscr{K} \cup \mathscr{L}$ и с рёбрами, обозначающими вложения; таким образом, k-элементное множество $K \in \mathscr{K}$ соединено ребром с ℓ-элементным множеством $\mathscr{L}$ в том случае, когда $K \subseteq L$. Рисунок 30 — небольшая иллюстрация для случая $w = 2$, $h = 3$, $k = 2$, $\ell = 3$.

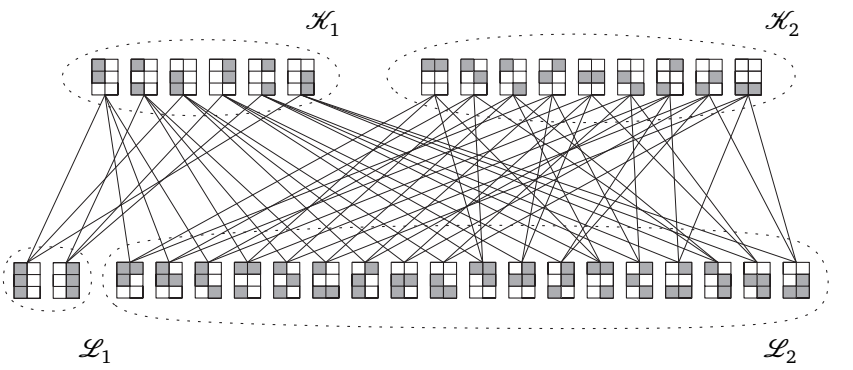


Рис. 30

Утверждение. *При любых i и j все $L \in \mathscr{L}_j$ имеют одинаковое количество d_{ij} соседей в $\mathscr{K}_i$.*

Доказательство утверждения. Пусть $L, L' \in \mathscr{L}_j$. Зафиксируем перестановку π, не ломающую столбцы и такую, что $L' = \pi(L)$. Если $K \in \mathscr{K}_i$, то $\pi(K) \in \mathscr{K}_i$ (согласно альтернативному описанию стеночной эквивалентности), и легко видеть, что $K \mapsto \pi(K)$ задаёт биекцию между соседями множества L, лежащими в $\mathscr{K}_i$, и соседями множества L', лежащими в $\mathscr{K}_i$. □

Теперь на время перейдём в более общую ситуацию. Пусть U, V — непересекающиеся конечные множества, и пусть $(U_1, \ldots, U_r, V_1, \ldots, V_s)$ — разбиение множества $U \cup V$, где $U = U_1 \cup \ldots \cup U_r$ и $V = V_1 \cup \ldots \cup V_s$, причём все U_i и V_j непусты. Далее, пусть G — двудольный граф с множеством вершин $U \cup V$ (все рёбра проходят между U и V).

лентности являются орбитами этого действия. В дальнейшем некоторые утверждения также можно (нужно?) сформулировать в терминах действия групп перестановок, но я решил от этого отказаться, надеясь отпугнуть чуть меньшее количество читателей.

Будем говорить, что разбиение $(U_1, \ldots, U_r, V_1, \ldots, V_s)$ **однородно степени V** относительно G, если выполнено условие утверждения, т. е. все вершины из V_j имеют одинаковое количество d_{ij} соседей из U_i при всех i и j. В этом случае будем называть $D = (d_{ij})_{i=1}^{r}{}_{j=1}^{s}$ **матрицей степени V для данного разбиения** (относительно G).

В ситуации, описанной ранее, имелся двудольный граф с однородным разбиением некоторой степени V. Мы хотим доказать, что $r \leqslant s$, где r — количество частей в разбиении U, а s — количество частей в разбиении V. Следующая лемма даёт достаточное условие, которое мы потом сможем проверить для данного G. По существу условие означает, что V не меньше, чем U, «по линейно-алгебраической причине».

Чтобы сформулировать лемму, рассмотрим $(|U| \times |V|)$-матрицу B (**двудольную матрицу смежности** графа G), строки которой занумерованы вершинами из множества U, столбцы — вершинами из множества V, а элемент b_{uv} имеет вид

$$b_{uv} := \begin{cases} 1 & \text{при } \{u, v\} \in E(G), \\ 0 & \text{в противном случае.} \end{cases}$$

Лемма. *Пусть G — как и выше, двудольный граф; $(U_1, U_2, \ldots, U_r, V_1, V_2, \ldots, V_s)$ — однородное разбиение множества его вершин степени V; B — двудольная матрица смежности графа G, и её строки линейно независимы. Тогда $r \leqslant s$.*

Доказательство леммы. Это сильное утверждение доказывается легко. Покажем, что $(r \times s)$-матрица D степени V имеет линейно независимые строки. Тогда у неё не может быть меньше столбцов, чем строк, так что действительно $r \leqslant s$.

$B =$

	V_1	V_2	V_3	V_4
U_1	$B[U_1, V_1]$	$B[U_1, V_2]$		
U_2				
U_3				$B[U_3, V_4]$

Рис. 31

Пусть $B[U_i, V_j]$ обозначает подматрицу в B, состоящую из элементов b_{uv}, для которых $u \in U_i$ и $v \in V_j$; схематически это показано на рис. 31.

Условие однородности степени V переводится на язык матриц следующим образом: сумма по каждому столбцу матрицы $B[U_i, V_j]$ равна d_{ij}.

Для вектора $\mathbf{x} \in \mathbb{R}^r$ пусть $\widetilde{\mathbf{x}} \in \mathbb{R}^{|U|}$ — вектор, компоненты которого занумерованы вершинами из U и получаются повторением $|U_i|$ раз компоненты x_i для каждого i; таким образом, $\widetilde{x}_u = x_i$ при всех $u \in U_i$, $i = 1, 2, \ldots, r$.

Для этого вектора $\widetilde{\mathbf{x}}$ рассмотрим произведение $\widetilde{\mathbf{x}}^T B$. Его v-я компонента (где $v \in V_j$) равна $\sum\limits_{u \in U} \widetilde{x}_u b_{uv} = \sum\limits_{i=1}^{r} x_i \sum\limits_{u \in U_i} b_{uv} = \sum\limits_{i=1}^{r} x_i d_{ij} = (\mathbf{x}^T D)_j$. Поэтому если $\mathbf{x}^T D = \mathbf{0}$, то $\widetilde{\mathbf{x}}^T B = \mathbf{0}$.

Теперь предположим, что строки матрицы D линейно зависимы, т. е. существует ненулевой вектор $\mathbf{x} \in \mathbb{R}^r$, для которого $\mathbf{x}^T D = \mathbf{0}$. Тогда $\widetilde{\mathbf{x}} \neq \mathbf{0}$, но, как мы только что видели, $\widetilde{\mathbf{x}}^T B = \mathbf{0}$. Однако согласно условию леммы строки матрицы B линейно независимы. Полученное противоречие завершает доказательство. □

Доказательство теоремы. Вернёмся к рассмотренному выше двудольному графу G с множеством вершин $\mathscr{K} \cup \mathscr{L}$ и однородным степени $\mathscr{L}$ разбиением $(\mathscr{K}_1, \ldots, \mathscr{K}_r, \mathscr{L}_1, \ldots, \mathscr{L}_s)$, отвечающим стеночной эквивалентности. Чтобы применить лемму, осталось показать, что строки соответствующей матрицы B линейно независимы.

Этот факт, известный как **теорема Готлиба (Gottlieb)**[1], оказался полезным и в ряде других случаев. В явном виде эта теорема утверждает, что *если в матрице B из нулей и единиц строки занумерованы элементами из $\mathscr{K}$ (всеми k-подмножествами множества $\{1, 2, \ldots, n\}$), столбцы занумерованы элементами из $\mathscr{L}$ (всеми ℓ-подмножествами) при $0 \leqslant k < \ell \leqslant \frac{n}{2}$, а ненулевые элементы отвечают вложениям, то строки линейно независимы.*

Известно несколько доказательств этого факта; здесь мы приведём одно, напоминающее доказательство предыдущей леммы.

Доказательство теоремы Готлиба. Предположим противное: пусть $\mathbf{y}^T B = \mathbf{0}$ для некоторого ненулевого вектора $\mathbf{y}$. Его компоненты занумерованы k-элементными множествами; зафиксируем некоторое $K_0 \in \mathscr{K}$, для которого $y_{K_0} \neq 0$.

[1] Однако это не единственная теорема, связанная с именем Готлиба.

Теперь разделим множества $\mathscr{K}$ и $\mathscr{L}$ на $k+1$ классов в соответствии с размером пересечения с K_0 (это разбиение не имеет ничего общего с разбиением множеств $\mathscr{K}$ и $\mathscr{L}$, рассмотренным ранее, — мы просто используем те же обозначения):

$$\mathscr{K}_i := \{K \in \mathscr{K} : |K \cap K_0| = i\}, \quad i = 0, 1, \ldots, k,$$
$$\mathscr{L}_j := \{L \in \mathscr{L} : |L \cap K_0| = j\}, \quad j = 0, 1, \ldots, k.$$

Каждое $\mathscr{K}_i$ и каждое $\mathscr{L}_j$ непусто — здесь мы используем условие $k < \ell \leqslant \frac{n}{2}$ (например, при $k + \ell > n$ было бы $\mathscr{L}_0 = \varnothing$, поскольку не хватило бы места для ℓ-элементного множества, не пересекающегося с K_0).

На этот раз нам требуется от введённого разбиения однородность степени $\mathscr{K}$ (относительно того же двудольного графа, что и выше, где рёбра отвечают вложениям). Это означает, что каждое $K \in \mathscr{K}_i$ имеет одинаковое количество d_{ij} соседей в множестве $\mathscr{L}_j$. Более подробно, d_{ij} равно количеству способов расширить k-элементное множество K, для которого $|K \cap K_0| = i$, до ℓ-элементного множества $L \supset K$, для которого $|L \cap K_0| = j$. Но ясно, что это количество не зависит от конкретного выбора K. (Можно вычислить d_{ij} явно, но нам это не потребуется.)

При таком определении мы имеем $d_{ij} = 0$ для $i > j$, поэтому матрица D степени $\mathscr{K}$ является верхней треугольной. Кроме того, $d_{ii} \neq 0$ при всех $i = 0, 1, \ldots, k$, так что матрица D невырожденна.

Используя вектор $\mathbf{y}$, найдём такой ненулевой вектор $\mathbf{x} = (x_0, x_1, \ldots, x_k)$, для которого $\mathbf{x}^T D = \mathbf{0}$, что даст противоречие. Подходящий вектор $\mathbf{x}$ получается суммированием компонент вектора $\mathbf{y}$ по классам $\mathscr{K}_i$:

$$x_i := \sum_{K \in \mathscr{K}_i} y_K.$$

Тогда $\mathbf{x} \neq \mathbf{0}$, поскольку класс $\mathscr{K}_k$ содержит лишь K_0 и потому $x_k = y_{K_0} \neq 0$.

Для каждого j имеем

$$0 = \sum_{L \in \mathscr{L}_j} (\mathbf{y}^T B)_L = \sum_{L \in \mathscr{L}_j} \sum_{K \in \mathscr{K}} y_K b_{KL} = \sum_{K \in \mathscr{K}} y_K \sum_{L \in \mathscr{L}_j} b_{KL} =$$
$$= \sum_{i=0}^{k} \sum_{K \in \mathscr{K}_i} y_K d_{ij} = \sum_{i=0}^{k} x_i d_{ij} = (\mathbf{x}^T D)_j.$$

Значит, $\mathbf{x}^T D = \mathbf{0}$, и мы получили обещанное противоречие с невырожденностью матрицы D. Теорема Готлиба доказана. □

Тем самым доказана и основная теорема. □

Другой пример. Читателям, знакомым с понятием изоморфизма графов (см. миниатюру 13), послужит поощрением следующий пример на описанный выше метод: докажите, что если $g_n(k)$ обозначает количество неизоморфных графов с n вершинами и k рёбрами, то последовательность $g_n(0), g_n(1), \ldots, g_n\left(\binom{n}{2}\right)$ унимодальна.

Литература

Как отмечено выше, теорема неявно подразумевалась без доказательства в статье

Cayley A. A second memoir on quantics // Phil. Trans. Roy. Soc. 1856. V. 146. P. 101—126.

Слово «quantic» в заголовке означает в сегодняшней терминологии однородный многочлен от нескольких переменных, и Кэли интересовался теми из них, которые инвариантны относительно линейных преобразований. Первое доказательство теоремы было получено в статье

Sylvester J. J. Proof of the hitherto undemonstrated fundamental theorem of invariants // Philos. Mag. 1878. V. 5. P. 178—188.

Доказательство, сформулированнное в терминах представлений групп и существенно более элементарное, чем предыдущие, получено в работе

Stanley R. P. Some aspects of groups acting on finite posets // J. Combinatorial Theory. Ser. A. 1982. V. 32. P. 132—161.

Мы основывались на изложении в учебнике Бабая и Франкла, упомянутом во введении.

Теорема Готлиба была впервые доказана в работе

Gottlieb D. H. A certain class of incidence matrices // Proc. Amer. Math. Soc 1966. V. 17. P. 1233—1237.

Представленное здесь доказательство — переформулировка рассуждения из работы

Godsil C. D. Tools from linear algebra. Ch. 31 // Handbook of Combinatorics / Eds. R. Graham, M. Grötschel, L. Lovász. Amsterdam: North-Holland, 1995. P. 1705—1748.

Ознакомиться с целочисленными разбиениями можно по книге

Andrews G., Eriksson K. Integer partitions. Cambridge: Cambridge University Press, 2004

(весьма доступный источник) или по запискам лекций Г. Уилфа на сайте `http://www.math.upenn.edu/~wilf/PIMS/PIMSLectures.pdf`.

Миниатюра 24

Совершенные паросочетания и определители

Паросочетанием в графе G называется такое множество рёбер $F \subseteq E(G)$, что любая вершина из G инцидентна не более чем одному ребру из F.

Совершенным паросочетанием называется паросочетание, охватывающее все вершины. Если читатель пожелает, он может отыскать совершенное паросочетание в графе на рис. 32.

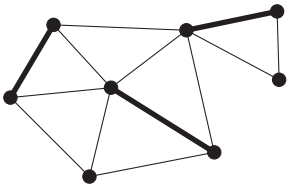


Рис. 32

В миниатюре 22 мы подсчитали совершенные паросочетания в некоторых графах с помощью определителей. Здесь мы применим определители в простом алгоритме, который проверяет, есть ли совершенное паросочетание в данном графе. Наш подход в основе тот же, что и при проверке матричного умножения в миниатюре 11. Мы ограничимся двудольным случаем как более простым.

Рассмотрим двудольный граф G. Его вершины делятся на два класса $\{u_1, u_2, \ldots, u_n\}$ и $\{v_1, v_2, \ldots, v_n\}$, и все рёбра проходят только между классами, но не внутри классов. Размер обоих классов одинаков, так как иначе граф не имел бы совершенного паросочетания. Пусть m обозначает количество рёбер в графе G.

Пусть S_n — множество всех перестановок множества $\{1, 2, \ldots, n\}$. Каждое совершенное паросочетание в графе G однозначно соответствует перестановке $\pi \in S_n$. Можно записать её в виде $\{\{u_1, v_{\pi(1)}\}, \{u_2, v_{\pi(2)}\}, \ldots, \{u_n, v_{\pi(n)}\}\}$.

Выразим наличие совершенного паросочетания с помощью определителя, но не обычной числовой матрицы, а матрицы из *переменных*. Для каждого ребра $\{u_i, v_j\} \in E(G)$ введём переменную x_{ij} (итого m переменных) и зададим $(n \times n)$-матрицу A формулой

$$a_{ij} := \begin{cases} x_{ij} & \text{при } \{u_i, v_j\} \in E(G), \\ 0 & \text{в противном случае.} \end{cases}$$

Определитель матрицы A — многочлен от m переменных x_{ij}. По определению определителя получаем

$$\det(A) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \cdot a_{1,\pi(1)} a_{2,\pi(2)} \dots a_{n,\pi(n)} = \\ = \sum_{\substack{\pi \text{ — совершенное} \\ \text{паросочетание в } G}} \operatorname{sgn}(\pi) \cdot x_{1,\pi(1)} x_{2,\pi(2)} \dots x_{n,\pi(n)}.$$

Лемма. *Многочлен* $\det(A)$ *тождественно равен нулю в точности тогда, когда* G *не имеет совершенного паросочетания.*

Доказательство леммы. Из вышеприведённой формулы ясно, что если G не имеет совершенного паросочетания, то $\det(A)$ — тождественный нуль.

Чтобы показать обратное, зафиксируем перестановку π, которая задаёт совершенное паросочетание, и дадим переменным в $\det(A)$ следующие значения: $x_{i,\pi(i)} := 1$ при $i = 1, 2, \dots, n$, а все остальные x_{ij} равны 0. Тогда $\operatorname{sgn}(\pi) \cdot x_{1,\pi(1)} x_{2,\pi(2)} \dots x_{n,\pi(n)} = \pm 1$.

Для каждой другой перестановки $\sigma \neq \pi$ найдётся i, для которого $\sigma(i) \neq \pi(i)$, поэтому $x_{i,\sigma(i)} = 0$, так что все остальные слагаемые в разложении $\det(A)$ равны 0. Таким образом, для данного выбора x_{ij} мы получаем $\det(A) = \pm 1$. □

Теперь хотелось бы проверить, является ли данный многочлен $\det(A)$ тождественным нулём. У нас нет возможности вычислить этот многочлен явно, поскольку количество его слагаемых равно количеству совершенных паросочетаний в G, которое может иметь экспоненциальный порядок. Но если подставить вместо переменных x_{ij} конкретные числа, то мы легко вычислим определитель, например, методом Гаусса. Так что можно представить себе, что $\det(A)$ доступен нам через чёрный ящик, который выдаёт значение многочлена в любой заданной точке.

Если бы чёрный ящик выдавал значения произвольной функции, то мы убедились бы, что это тождественный нуль, лишь проверив

её значения во всех точках. Но многочлен обладает замечательным свойством: или он равен нулю всюду, или почти нигде. Следующая теорема выражает этот факт количественно.

Теорема (Шварц — Зиппель). *Пусть $\mathbb{K}$ — произвольное поле, d — натуральное число, S — конечное подмножество в $\mathbb{K}$. Тогда для любого ненулевого многочлена $p(x_1, \ldots, x_m)$ степени d от m переменных с коэффициентами из $\mathbb{K}$ количество наборов $(r_1, r_2, \ldots, r_m) \in S^m$, где $p(r_1, r_2, \ldots, r_m) = 0$, не превосходит $d|S|^{m-1}$. Иначе говоря, если r_1, r_2, …, $r_m \in S$ — независимые случайные величины с равномерным распределением, то вероятность равенства $p(r_1, r_2, \ldots, r_m) = 0$ не превосходит $\frac{d}{|S|}$.*

Прежде чем доказывать эту теорему, вернёмся к двудольным паросочетаниям. Предположим, что G имеет совершенное паросочетание и, значит, $\det(A)$ — ненулевой многочлен степени n. Согласно теореме Шварца—Зиппеля, если вычислить $\det(A)$ для значений переменных x_{ij}, независимо выбранных случайным образом из множества $S := \{1, 2, \ldots, 2n\}$, то вероятность получить 0 не превосходит $\frac{1}{2}$.

Но чтобы проверить равенство определителя нулю для данных значений переменных, его нужно вычислить точно. При этом вычислении могут встретиться огромные числа, имеющие порядка n цифр, и тогда арифметические операции станут весьма затратными.

Было бы лучше работать в конечном поле. Простейший способ для этого — выбрать простое число p, $2n \leqslant p < 4n$ (такое число существует согласно теоретико-числовому результату, называемому постулатом Бертрана[1], и его можно вычислить достаточно быстро), и работать в конечном поле $\mathbb{F}_p$ вычетов по модулю p. Тогда арифметические действия выполняются быстро (если заранее заготовить таблицу обратных элементов).

Вычисляя определитель методом Гаусса, получаем вероятностный алгоритм, проверяющий существование совершенного паросочетания в данном двудольном графе за $O(n^3)$ операций. Алгоритм ошибается с вероятностью не больше $\frac{1}{2}$. Как обычно, вероятность неудачи можно понизить до 2^{-k}, повторяя алгоритм k раз.

Можно также вычислить определитель каким-либо алгоритмом быстрого умножения матриц (см. миниатюру 10), и таким способом

[1] А также теоремой Чебышёва. — *Прим. перев.*

получается асимптотически быстрейший из известных алгоритмов для проверки существования совершенного двудольного паросочетания, с временем работы $O(n^{2,376})$.

Но следует откровенно признать, что известен детерминированный алгоритм, который всегда находит максимальное паросочетание за $O(n^{2,5})$ операций, а на практике работает гораздо быстрее. При этом описанный выше алгоритм проверяет существование совершенного паросочетания, но не находит его (однако существуют более сложные его варианты, которые могут и найти паросочетание). С другой стороны, этот алгоритм можно очень эффективно реализовать на параллельных компьютерах, и никакой другой из известных подходов не приводит к параллельным алгоритмам сравнимой скорости.

Доказательство теоремы Шварца—Зиппеля. Проведём индукцию по m. Случай одной переменной очевиден, так как по общеизвестной алгебраической теореме $p(x_1)$ имеет не более d корней. (Это доказывается индукцией по d: если $p(\alpha) = 0$, то можно разделить $p(x)$ на $x - \alpha$, понизив степень.)

Пусть $m > 1$. Предположим, что x_1 появляется с ненулевым коэффициентом хотя бы в одном слагаемом из $p(x_1, \ldots, x_m)$ (в противном случае перенумеруем переменные). Запишем $p(x_1, \ldots, x_m)$ как многочлен от x_1, коэффициенты которого — многочлены от $x_2, \ldots, x_m$:

$$p(x_1, x_2, \ldots, x_m) = \sum_{i=0}^{k} x_1^i p_i(x_2, \ldots, x_m),$$

где k — наибольший показатель при x_1 в $p(x_1, \ldots, x_m)$.

Наборы вида $(r_1, \ldots, r_m)$, где $p(r_1, \ldots, r_m) = 0$, мы разделим на два класса. Обозначим первый класс R_1 и включим в него наборы, для которых $p_k(r_2, \ldots, r_m) = 0$. Поскольку многочлен $p_k(x_2, \ldots, x_m)$ не равен тождественно нулю и имеет степень не выше $d - k$, количество вариантов для $(r_2, \ldots, r_m)$ по предположению индукции не превосходит $(d-k)|S|^{m-2}$, и потому $|R_1| \leqslant (d-k)|S|^{m-1}$.

Другой класс R_2 состоит из остальных наборов, т. е. тех, для которых $p(r_1, r_2, \ldots, r_m) = 0$, но $p_k(r_2, \ldots, r_m) \neq 0$. Их мы подсчитаем так: значения переменных от r_2 до r_m можно выбрать не более чем $|S|^{m-1}$ способами, и если зафиксированы $r_2, \ldots, r_m$, для которых

$$p_k(r_2, \ldots, r_m) \neq 0,$$

то r_1 должно быть корнем многочлена от одной переменной $q(x_1) = p(x_1, r_2, \ldots, r_m)$. Этот многочлен имеет степень (ровно) k, поэтому у него не больше k корней. Значит, второй класс содержит не более $k|S|^{m-1}$ наборов, и потому общее количество наборов не превосходит $d|S|^{m-1}$. На этом шаг индукции закончен, а с ним и доказательство теоремы Шварца—Зиппеля. □

Литература

Идея алгоритма, проверяющего существование совершенного паросочетания с помощью определителей, взята из статьи

Edmonds J. Systems of distinct representatives and linear algebra // J. Res. Nat. Bur. Standards. 1967. V. 71B. P. 241—245.

Существует много работ по алгебраическим алгоритмам для паросочетаний; вот одна из последних (2010 г.):

Harvey N. J. A. Algebraic algorithms for matching and matroid problems // Proc. 47th IEEE Symposium on Foundations of Computer Science (FOCS). 2006. P. 531—542[1].

Теорема (или лемма) Шварца—Зиппеля появилась в статьях

Schwartz J. Fast probabilistic algorithms for verification of polynomial identities // J. ACM 1980. V. 27. P. 701—717

и

Zippel R. Probabilistic algorithms for sparse polynomials // Proc. International Symposium on Symbolic and Algebraic Computation. Berlin: Springer, 1979. (Lecture Notes in Computer Science, V. 72). P. 216—226.

[1] См. также: *Harvey N. J.* Algebraic algorithms for matching and matroid problems // SIAM Journal on Computing. 2009. V. 39, № 2. P. 679—702. — *Прим. перев.*

Миниатюра 25

Как повернуть лестницу над конечным полем

Мы хотим повернуть лестницу длиной 10 м внутри сада (не поднимая её). Какова наименьшая площадь сада, при которой это возможно? Например, на рис. 33 изображён сад, который выглядит вполне экономно в смысле площади (лестница изображена белым отрезком).

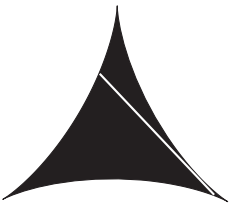


Рис. 33

Этот вопрос обычно называют **задачей Какейи об иголке**; Какейя сформулировал её в терминах вращения иголки, но я никогда не усматривал причин вращать иголку, зато получил весьма запоминающийся опыт, поворачивая длинную и тяжёлую лестницу, поэтому я буду придерживаться этой альтернативной формулировки.

В 1920-х годах Безикович получил один из тех математических результатов, которые явно противоречат интуиции: существуют сады *произвольно малой* площади, всё же допускающие вращение лестницы. Позвольте вкратце описать их красивую конструкцию, хотя она прямо не относится к теме этой книги.

Чтобы лестницу единичной длины можно было повернуть внутри множества X, необходимо, чтобы X содержало отрезок единичной длины каждого направления. Множество, удовлетворяющее этому более слабому требованию, называется **множеством Какейи**; в отличие от задачи о лестнице, это определение очевидным образом обобщается на высшие размерности. Начнём с построения плоского множества Какейи произвольно малой площади (приложив до-

полнительное усилие, можно на самом деле получить и множество Какейи с нулевой мерой).

Рассмотрим треугольник T с высотой 1 и основанием на оси OX. Пусть $k \geqslant 2$ — целое число, и пусть $h \in [0; 1)$. Назовём **k-утоньшением** треугольника T на высоте h следующую процедуру: мы разбиваем его основание на k равных отрезков, разрезаем треугольник T на k треугольников $T_1, \ldots, T_k$ с этими отрезками в качестве оснований и перемещаем каждый из треугольников $T_2, \ldots, T_k$ влево так, чтобы пересечение его контура с контуром T_1 оказалось на высоте h. На рис. 34 показано 3-утоньшение.

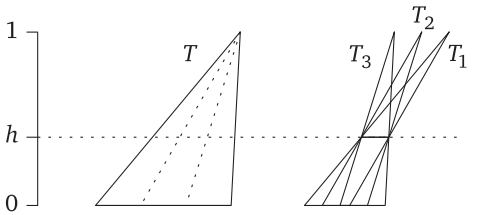


Рис. 34

Более общо, k-утоньшение совокупности треугольников на высоте h означает k-утоньшение каждого из них по отдельности, так что из N треугольников мы получаем kN треугольников.

Построим на плоскости множество малой площади, содержащее отрезки всех направлений, наклон[1] которых не меньше 1 по абсолютной величине (т. е. скорее вертикальные, чем горизонтальные); чтобы получить множество Какейи, нужно добавить второй экземпляр, повёрнутый на 90°.

Выберем большое целое m и построим множество с площадью порядка не выше $O\left(\frac{1}{m}\right)$. Возьмём треугольник с углом 90°, противолежащим горизонтальному основанию, и выполним m-утоньшение на высоте $\frac{1}{m}$, затем на высоте $\frac{2}{m}$ и так далее вплоть до высоты $\frac{m-1}{m}$. На рис. 35 показан пример для $m = 3$.

Пусть B_m обозначает объединение получившихся m^{m-1} тонких треугольников.

Несложно убедиться, что полная длина пересечения множества B_m и горизонтальной прямой на высоте $\frac{i}{m}$, $i = 1, 2, \ldots, m-1$, не пре-

[1] Тангенс угла с лучом OX. — *Прим. перев.*

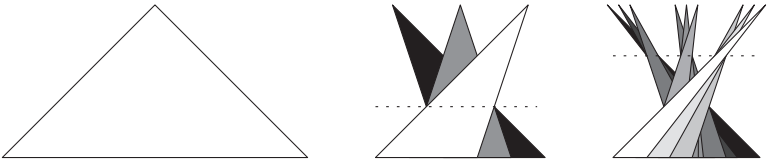


Рис. 35

восходит $\frac{1}{m}$. Труднее показать, что длина пересечения на любой другой высоте также имеет порядок $\frac{1}{m}$. Полное доказательство содержится в литературе, указанной в конце этой миниатюры (честолюбивый читатель может попробовать провести его самостоятельно).

Как можно использовать B_m, чтобы повернуть лестницу? Нужно расширить его так, чтобы лестница могла перемещаться от одного тонкого треугольника к другому. Для этого добавим к B_m «коридоры сдвига», показанные на рис. 36.

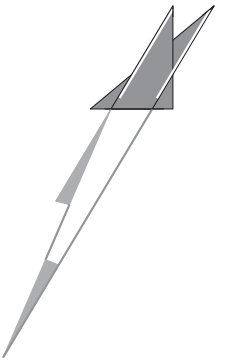


Рис. 36

Тёмно-серые треугольники взяты из B_i, а по более светлому коридору можно перемещать лестницу между двумя отмеченными положениями. Когда мы переносим лестницу на далёкое расстояние, коридоры сдвига добавляют произвольно малую площадь.

Гипотеза Какейи. Таким образом, множество Какейи на плоскости может быть малым и даже иметь меру нуль. При всех $n \geqslant 3$ декартово произведение плоского множества Какейи с мерой нуль на $(n-2)$-мерный шар приводит к множествам Какейи в $\mathbb{R}^n$, также имеющим меру нуль. Однако согласно утверждению, известно-

му как гипотеза Какейи, множества Какейи не могут быть *слишком* маленькими. А именно, множество Какейи K в $\mathbb{R}^n$ должно иметь хаусдорфову размерность n (для читателей, не знакомых с понятием хаусдорфовой размерности: условно говоря, это означает, что нельзя покрыть K множествами малого диаметра намного экономнее, чем, скажем, n-мерный куб).

В то время как задача Какейи об игле носит несколько развлекательный характер, гипотеза Какейи рассматривается как фундаментальная математическая проблема, прежде всего в гармоническом анализе, и она связана с несколькими другими серьёзными задачами. Хотя усилиями многих замечательных математиков получен ряд частичных результатов, проблема всё ещё представляется далёкой от решения (гипотеза Какейи доказана лишь для $n=2$).

Гипотеза Какейи для конечных полей. Недавно, однако, аналог гипотезы Какейи — с заменой поля $\mathbb{R}$ на конечное поле $\mathbb{F}$ — был доказан коротким алгебраическим рассуждением (после более слабых результатов, потребовавших *гораздо* более сложных средств). Множество K в векторном пространстве $\mathbb{F}^n$ является **множеством Какейи**, если оно содержит «прямую» каждого возможного «направления»; это означает, что для любого ненулевого $\mathbf{u}\in\mathbb{F}^n$ найдётся такое $\mathbf{a}\in\mathbb{F}^n$, что $\mathbf{a}+t\mathbf{u}$ принадлежит K при всех $t\in\mathbb{F}$.

Теорема (гипотеза Какейи для конечных полей)**.** *Пусть $\mathbb{F}$ — поле из q элементов. Тогда любое множество Какейи K в $\mathbb{F}^n$ содержит не менее $\binom{q+n-1}{n}$ элементов.*

При фиксированном n и большом q величина $\binom{q+n-1}{n}$ ведёт себя примерно как $\frac{q^n}{n!}$, так что множество Какейи занимает как минимум около $\frac{1}{n!}$ от всего пространства. Таким образом, в отличие от вещественного случая, множество Какейи над конечным полем занимает значительную часть «n-мерного объёма» всего пространства.

Биномиальный коэффициент появляется в силу следующей нетрудной леммы.

Лемма. *Пусть $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_N$ — точки в $\mathbb{F}^n$, где*

$$N < \binom{d+n}{n}.$$

Тогда существует ненулевой многочлен $p(x_1, x_2, \ldots, x_n)$ степени не выше d, для которого $p(\mathbf{a}_i)=0$ при всех i.

Доказательство леммы. Произвольный многочлен степени не выше d от переменных $x_1, x_2, \ldots, x_n$ можно записать в виде

$$p(\mathbf{x}) = \sum_{\alpha_1+\ldots+\alpha_n \leqslant d} c_{\alpha_1,\ldots,\alpha_n} x_1^{\alpha_1} \ldots x_n^{\alpha_n},$$

где $c_{\alpha_1,\ldots,\alpha_n} \in \mathbb{F}$ — некоторые коэффициенты, а суммирование проводится по всем наборам длины n из неотрицательных целых чисел $(\alpha_1, \ldots, \alpha_n)$ с суммой не больше d.

Мы утверждаем, что количество таких наборов $(\alpha_1, \ldots, \alpha_n)$ равно $\binom{d+n}{n}$. Действительно, выбор набора $(\alpha_1, \ldots, \alpha_n)$ равносилен распределению d одинаковых шаров по $n+1$ пронумерованным ящикам (последний ящик предназначен для $d - \alpha_1 - \ldots - \alpha_n$ «неиспользованных» шаров). Простейший способ проверить наше утверждение о количестве распределений — расположить d шаров в ряд, а затем разбить их на группы, вставив между ними n разделителей.

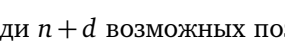


Рис. 37

Таким образом, среди $n+d$ возможных позиций шаров и разделителей мы выбираем n позиций, которые будут заняты разделителями, и производим подсчёт.

Условие вида $p(\mathbf{a}) = 0$ соответствует *однородному* линейному уравнению с неизвестными $c_{\alpha_1,\ldots,\alpha_n}$. Поскольку $N < \binom{n+d}{n}$, у нас меньше уравнений, чем неизвестных, а такая система однородных линейных уравнений всегда имеет ненулевое решение. Поэтому найдётся многочлен, у которого хотя бы один коэффициент отличен от нуля. □

Доказательство теоремы. Предположим противное: пусть $|K| < \binom{q+n-1}{n}$. Тогда согласно лемме существует ненулевой многочлен p степени $d \leqslant q-1$, равный нулю во всех точках из K.

Выберем ненулевое $\mathbf{u} \in \mathbb{F}^n$. Поскольку K — множество Какейи, найдётся $\mathbf{a} \in \mathbb{F}^n$, для которого $\mathbf{a} + t\mathbf{u} \in K$ при всех $t \in \mathbb{F}$. Положим $f(t) := p(\mathbf{a} + t\mathbf{u})$. Это многочлен от одной переменной t степени не выше d, равный нулю при всех q возможных значениях переменной t. А так как многочлен степени d от одной переменной над полем имеет не больше d корней, $f(t)$ тождественно равен нулю. В частности, в нём равен нулю коэффициент при t^d.

Теперь посмотрим, что означает этот коэффициент в терминах исходного многочлена p: он равен $\overline{p}(\mathbf{u})$, где $\overline{p}$ — *однородная часть* многочлена p, т. е. многочлен, полученный из p удалением всех мономов степени строго меньше d. Разумеется, многочлен $\overline{p}$ также ненулевой, так как иначе степень многочлена p была бы меньше, чем d.

Итак, $\overline{p}(\mathbf{u}) = 0$, а так как $\mathbf{u}$ произвольно, $\overline{p}$ равен 0 на всём $\mathbb{F}^n$. Но это противоречит теореме Шварца—Зиппеля из миниатюры 24, согласно которой ненулевой многочлен степени d равен нулю не более чем в $dq^{n-1} \leqslant (q-1)q^{n-1} < |\mathbb{F}^n|$ точках из $\mathbb{F}^n$. Полученное противоречие доказывает теорему. □

Литература

Множества Какейи с нулевой мерой были построены в работе

Besicovitch A. S. Sur deux questions d'integrabilite des fonctions // J. Soc. Phys. Math. 1919. V. 2. P. 105—123.

Узнав про задачу Какейи об игле, Безикович решил её с помощью модификации своего метода в статье

Besicovitch A. S. On Kakeya's problem and a similar one // Math. Zeitschrift. 1928. V. 27. P. 312—320.

Существует несколько упрощений первоначальной конструкции Безиковича (в частности, принадлежащих Перрону и Шёнбергу). Формальное доказательство пригодности конструкции, описанной выше, можно найти в работе

Wolff T. H. Recent work connected with the Kakeya problem B / Ed. H. Rossi // Prospects in Mathematics (Princeton, 1996). Providence: Amer. Math. Soc., 1999. P. 129—162.

По этой статье можно познакомиться также с гипотезой Какейи и некоторыми связанными с ней вопросами и результатами. Другой вариант конструкции, имеющий и совсем другое доказательство, рассмотрен в статье

Besicovitch A. S. The Kakeya problem // Amer. Math. Monthly. 1963. V. 70. P. 697—706.

Доказательство гипотезы Какейи для конечных полей взято из работы

Dvir Z. On the size of Kakeya sets in finite fields // J. Amer. Math. Soc. 2009. V. 22, № 4. P. 1093—1097

(там содержится простое уточнение первоначальной нижней оценки Двира, независимо замеченное Алоном и Тао).

Миниатюра 26

Подсчёт композиций

Рассмотрим следующую алгоритмическую проблему: дано множество P перестановок на множестве $\{1, 2, \ldots, n\}$; мы хотим вычислить мощность множества $P \circ P := \{\sigma \circ \tau \colon \sigma, \tau \in P\}$ всех композиций пар перестановок из P.

Напомним, что **перестановкой** на множестве $\{1, 2, \ldots, n\}$ называется биективное отображение $\sigma \colon \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$. Например, при $n = 4$ можно положить $\sigma(1) = 3$, $\sigma(2) = 2$, $\sigma(3) = 4$ и $\sigma(4) = 1$. Обычно перестановку записывают, перечисляя её значения в строку; в нашем примере будет $\sigma = (3, 2, 4, 1)$. Перестановку можно и загрузить в компьютер в таком виде, т. е. как массив с индексами $\{1, 2, \ldots, n\}$.

Перестановки перемножаются как отображения: чтобы получить композицию (произведение) $\rho := \sigma \circ \tau$ двух перестановок σ и τ, мы сначала применяем τ, а затем σ, т. е. $\rho(i) = \sigma(\tau(i))$. Например, взяв перестановку σ, рассмотренную выше, и $\tau = (2, 3, 4, 1)$, получаем $\sigma \circ \tau = (2, 4, 1, 3)$, тогда как $\tau \circ \sigma = (4, 3, 1, 2) \neq \sigma \circ \tau$. Представляя перестановки в виде массивов, можно вычислить композицию за время $O(n)$.

Попутно напомним, что множество всех перестановок множества $\{1, \ldots, n\}$, наделённое операцией композиции, образует группу, которая называется **симметрической группой** и обозначается S_n. Это важный объект в теории групп — и сам по себе, и потому, что любая конечная группа может быть представлена как подгруппа в S_n при некотором n. Задача эффективного вычисления $|P \circ P|$ — естественный основной вопрос в вычислительной теории групп.

Насколько велико может быть $P \circ P$? Один крайний случай — когда P образует подгруппу в S_n, тогда $\sigma \circ \tau \in P$ при всех $\sigma, \tau \in P$ и $|P \circ P| = |P|$. Другой крайний случай — когда все композиции различны, т. е. $\sigma_1 \circ \tau_1 \neq \sigma_2 \circ \tau_2$ для всех $\sigma_1, \sigma_2, \tau_1, \tau_2 \in P$ и $(\sigma_1, \tau_1) \neq (\sigma_2, \tau_2)$, тогда $|P \circ P| = |P|^2$.

Простейший способ вычислить $|P \circ P|$ состоит в вычислении композиции $\sigma \circ \tau$ для всех $\sigma, \tau \in P$, что даёт список из $|P|^2$ перестановок

за время $O(|P|^2 n)$. В этом списке некоторые перестановки могут появиться несколько раз. Стандартный подход к алгоритму подсчёта *различных* перестановок в таком списке состоит в том, чтобы их лексикографически упорядочить, а затем удалить повторы за один проход по упорядоченному списку. При некоторой изобретательности можно выполнить сортировку за время $O(|P|^2 n)$; мы не будем заниматься подробностями, так как наша цель — обсудить другой алгоритм.

Нелегко найти асимптотически более быстрый алгоритм (чтобы это почувствовать, читатель, разумеется, может попробовать сам). Однако этого можно достичь, комбинируя методы, уже знакомые нам по предыдущим миниатюрам, по крайней мере если мы готовы согласиться с некоторой (пренебрежимо малой) вероятностью ошибки.

Чтобы построить более быстрый алгоритм, прежде всего свяжем композицию перестановок со скалярным произведением определённых векторов. Пусть $x_1, x_2, \ldots, x_n$ и $y_1, y_2, \ldots, y_n$ — переменные, σ — некоторая перестановка. Рассмотрим вектор

$$\mathbf{x}(\sigma) := (x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)});$$

например, при $\sigma = (3, 2, 4, 1)$ имеем $\mathbf{x}(\sigma) = (x_3, x_2, x_4, x_1)$. Аналогично положим $\mathbf{y}(\sigma) := (y_{\sigma(1)}, \ldots, y_{\sigma(n)})$.

Теперь напомним, что τ^{-1} обозначает перестановку, **обратную** к перестановке τ, т. е. единственную перестановку, для которой $\tau^{-1}(\tau(i)) = i$ при всех i. Если, как выше, $\tau = (2, 3, 4, 1)$, то $\tau^{-1} = (4, 1, 2, 3)$.

Посмотрим теперь на скалярное произведение

$$\mathbf{x}(\sigma)^T \mathbf{y}(\tau^{-1}) = x_{\sigma(1)} y_{\tau^{-1}(1)} + \ldots + x_{\sigma(n)} y_{\tau^{-1}(n)};$$

это многочлен (степени 2) от переменных $x_1, \ldots, x_n, y_1, \ldots, y_n$. Все ненулевые коэффициенты этого многочлена равны 1; для определённости будем считать их целыми вещественными числами. Для наших конкретных σ и τ получаем

$$\mathbf{x}(\sigma)^T \mathbf{y}(\tau^{-1}) = x_3 y_4 + x_2 y_1 + x_4 y_2 + x_1 y_3.$$

В многочлене $\mathbf{x}(\sigma)^T \mathbf{y}(\tau^{-1})$ ровно одно слагаемое содержит y_1, ровно одно слагаемое содержит y_2 и т. д. (поскольку τ^{-1} является перестановкой). Какое слагаемое содержит y_1? Можно записать его как $x_{\sigma(k)} y_{\tau^{-1}(k)}$, где k — тот индекс, для которого $\tau^{-1}(k) = 1$; это озна-

чает, что $k = \tau(1)$. Таким образом, слагаемое, содержащее y_1, имеет вид $x_{\sigma(\tau(1))}y_1$. Аналогично слагаемое, содержащее y_i, имеет вид $x_{\sigma(\tau(i))}y_i$. Положив $\rho := \sigma \circ \tau$, можно записать

$$\mathbf{x}(\sigma)^T\mathbf{y}(\tau^{-1}) = \sum_{i=1}^{n} x_{\rho(i)}y_i.$$

Это показывает, что многочлен $\mathbf{x}(\sigma)^T\mathbf{y}(\tau^{-1})$ кодирует композицию $\sigma \circ \tau$ в следующем смысле.

Наблюдение. Пусть σ_1, σ_2, τ_1, τ_2 — перестановки множества $\{1, 2, \ldots, n\}$. Тогда $\mathbf{x}(\sigma_1)^T\mathbf{y}(\tau_1^{-1})$ и $\mathbf{x}(\sigma_2)^T\mathbf{y}(\tau_2^{-1})$ равны (как многочлены) в точности тогда, когда $\sigma_1 \circ \tau_1 = \sigma_2 \circ \tau_2$. □

Пусть $P = \{\sigma_1, \sigma_2, \ldots, \sigma_m\}$ — множество перестановок из нашей исходной задачи. Пусть X — матрица размера $n \times m$, в которой j-й столбец равен вектору $\mathbf{x}(\sigma_j)$, $j = 1, 2, \ldots, m$, а Y — матрица $n \times m$, в которой j-й столбец равен $\mathbf{y}(\sigma_j^{-1})$. Тогда в матричном произведении X^TY в позиции (i, j) стоит многочлен $\mathbf{x}(\sigma_i)^T\mathbf{y}(\sigma_j^{-1})$. Ввиду предыдущего наблюдения *мощность множества $P \circ P$ равно количеству различных элементов в X^TY*.

Может показаться неясным, почему такая странная с виду переформулировка облегчает построение алгоритма по сравнению с исходной задачей вычисления $|P \circ P|$. Однако тут нам на помощь приходят теорема Шварца—Зиппеля из миниатюры 24 и быстрое умножение матриц.

Пусть $s := 4m^4$ (позже мы увидим, почему выбрано это значение) и $S := \{1, 2, \ldots, s\}$. Наш алгоритм для вычисления $|P \circ P|$ будет работать следующим образом.

1. Выберем случайные целые числа $a_1, a_2, \ldots, a_n$ и $b_1, b_2, \ldots, b_n$, распределённые в S равномерно и независимо.

2. Построим матрицу A, которая получается из X подстановкой целого a_i вместо переменной x_i, $i = 1, 2, \ldots, n$. Аналогично пусть B получается из Y заменой каждого y_i на b_i, $i = 1, 2, \ldots, n$. Вычислим произведение $C := A^TB$.

3. Подсчитаем количество различных элементов в C (отсортировав их) и выведем его в качестве ответа.

Лемма. *Число на выходе описанного алгоритма никогда не превосходит $|P \circ P|$, и с вероятностью не меньше $\frac{1}{2}$ оно равно $|P \circ P|$.*

Доказательство. Если два элемента в X^TY — равные многочлены, то им отвечают и равные элементы в A^TB, так что количество различных элементов в A^TB никогда не превосходит $|P \circ P|$.

Пусть теперь элементы в позициях (i_1, j_1) и (i_2, j_2) матрицы X^TY различны как многочлены. Тогда их разность также ненулевой многочлен p степени 2. Согласно теореме Шварца—Зиппеля, если подставить в p вместо переменных элементы из S, выбранные независимо и случайно, то мы получим 0 с вероятностью не больше $2/|S| = 1/(2m^4)$.

Следовательно, любые два неравных элемента из X^TY становятся равными в A^TB с вероятностью не больше $1/(2m^4)$. Но X^TY — матрица размера $m \times m$, так что она заведомо не может содержать больше m^4 пар неравных элементов. Вероятность того, что *какие-нибудь* два неравных элемента из X^TY становятся равными в A^TB, не превосходит $m^4/(2m^4) = \frac{1}{2}$. Значит, с вероятностью не меньше $\frac{1}{2}$ количество неравных элементов в A^TB и в X^TY одинаково. Лемма доказана. □

Лемма показывает, что алгоритм работает корректно с вероятностью не меньше $\frac{1}{2}$. Если запустить алгоритм k раз и взять наибольший из ответов, то вероятность не получить $|P \circ P|$ не превосходит 2^{-k}.

Как быстро может работать программа, реализующая этот алгоритм? Для простоты рассмотрим лишь случай $m = n$, т. е. n перестановок n чисел. Напомним, что прямолинейный алгоритм, упомянутый в начале раздела, требует время порядка n^3.

В только что описанном рандомизированном алгоритме наибольшее время затрачивается на вычисление матричного произведения A^TB. При $m = n$ матрицы A и B квадратные, а их элементы — целые числа, не превосходящие $s = 4n^4$. Как мы отметили в миниатюре 10, такие матрицы теоретически можно перемножить за время $O(n^{2,376})$. Асимптотически это заметный выигрыш по сравнению с $O(n^3)$.

Литература

Yuster R. Efficient algorithms on sets of permutations, dominance, and real-weighted APSP // Proc. 20th Annual ACM-SIAM Symposium on Discrete Algorithms. SIAM, 2009. P. 950—957.

Миниатюра 27

Ассоциативна ли операция?

В математике часто рассматриваются множества, наделённые одной или несколькими бинарными операциями. Наиболее известные примеры — группы, поля, кольца.

Рассмотрим совершенно произвольную **бинарную операцию** $\odot$ на множестве X. Формально $\odot$ — произвольное отображение

$$X \times X \to X.$$

Если говорить менее формально, каждым двум элементам (возможно, совпадающим) $x, y \in X$ ставится в соответствие некоторый элемент $z \in X$, который обозначается $x \odot y$. Алгебраисты иногда изучают бинарные операции на таком уровне общности; множество X вместе с произвольной бинарной операцией называется **группоидом**.

Одно из важнейших свойств бинарных операций — ассоциативность; операция $\odot$ ассоциативна, если равенство

$$(x \odot y) \odot z = x \odot (y \odot z)$$

выполнено для всех $x, y, z \in X$. Практически все бинарные операции в работающей математике ассоциативны; умножение чисел Кэли (октонионов) — выдающееся исключение, которое лишь подтверждает правило[1]. Как только доказана ассоциативность операции в группоиде, его социальный статус повышается и он получает право именоваться **полугруппой**.

Здесь мы рассмотрим алгоритмическую проблему, которая может представлять интерес для алгебраиста, изучающего конечные группоиды и полугруппы: является ли данная бинарная операция $\odot$ на конечном множестве X ассоциативной?

Будем считать, что X содержит n элементов, а операция $\odot$ задана таблицей, строки и столбцы которой занумерованы элементами из X, причём на пересечении строки x и столбца y стоит элемент $x \odot y$. Для $X = \{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\}$ таблица могла бы выглядеть следующим

[1] Можно упомянуть также умножение в лиевых и йордановых алгебрах. — *Прим. перев.*

образом:

⊙	♡	♢	♠	♣
♡	♡	♡	♡	♡
♢	♡	♢	♠	♣
♠	♡	♠	♡	♠
♣	♡	♣	♡	♢

Назовём тройку $(x, y, z) \in X^3$ **ассоциативной**, если выполнено равенство $(x \odot y) \odot z = x \odot (y \odot z)$, и **неассоциативной** в противном случае. Очевидный способ проверки ассоциативности — тестировать каждую тройку $(x, y, z) \in X^3$. Для тройки (x, y, z) требуется два взгляда на таблицу, чтобы найти $(x \odot y) \odot z$, и ещё два взгляда, чтобы вычислить $x \odot (y \odot z)$. Поэтому время работы этого прямолинейного алгоритма имеет порядок n^3.

Приведём остроумный алгоритм с гораздо лучшим временем работы.

Теорема. *Существует вероятностный алгоритм с временем работы не больше $O(n^2)$, входом которого является таблично заданная бинарная операция $\odot$ на множестве из n элементов, а выходом — один из ответов «да» или «нет». Если операция $\odot$ ассоциативна, то ответ всегда «да». Если операция $\odot$ не ассоциативна, то ответ может быть «да» или «нет», но вероятность ответа «да» не превосходит $\frac{1}{2}$.*

Можно сделать вероятность неправильного ответа сколь угодно малой, повторяя алгоритм достаточно много раз, как и для алгоритма из миниатюры 11.

Очевидный рандомизированный алгоритм для проверки ассоциативности состоит в том, чтобы многократно выбирать случайную тройку $(x, y, z) \in X^3$ и проверять её ассоциативность. Но хитрость в том, что ассоциативность не обязательно проявляется на многих тройках. Например, операция, заданная вышеприведённой таблицей, имеет только две неассоциативные тройки, а именно (♣, ♣, ♠) и (♣, ♠, ♣), тогда как всего троек $4^3 = 64$. На самом деле нетрудно построить для каждого $n \geqslant 3$ операцию на множестве из n элементов с единственной неассоциативной тройкой. В этом случае даже после проверки n^2 случайных троек шанс выявить неассоциативность составляет лишь $\frac{1}{n}$, что очень далеко от константы $\frac{1}{2}$ из утверждения теоремы.

Сердцевину более быстрого алгоритма, о котором говорится в теореме, составляет следующая математическая конструкция. Вначале зафиксируем произвольное поле $\mathbb{K}$. Будет удобно принять, что сложение и умножение в нём выполняется за фиксированное время. Нам нужно, чтобы в поле было не меньше шести элементов, так что можно взять в качестве $\mathbb{K}$ поле из 7 элементов (однако, приложив некоторые усилия, можно реализовать алгоритм и для $\mathbb{K}=\mathbb{R}$ и многих других полей).

Перейдём к доказательству теоремы. Рассмотрим векторное пространство $\mathbb{K}^X$, элементы которого — наборы из n элементов поля $\mathbb{K}$, занумерованные элементами из X.

Пусть $\mathbf{e}\colon X \to \mathbb{K}^X$ — следующее отображение. Для каждого $x \in X$ пусть $\mathbf{e}(x)$ — такой вектор из $\mathbb{K}^X$, что в позиции с номером x стоит 1, а в остальных позициях 0. Таким образом, $\mathbf{e}$ задаёт биекцию между X и стандартным базисом в пространстве $\mathbb{K}^X$.

Мы подходим к ключевому пункту конструкции — построению бинарной операции $\boxdot$ на $\mathbb{K}^X$. Говоря неформально, мы продолжим $\odot$ на $\mathbb{K}^X$ линейно. Два произвольных вектора $\mathbf{u}, \mathbf{v} \in \mathbb{K}^X$ можно записать в стандартном базисе как

$$\mathbf{u} = \sum_{x\in X} \alpha_x \mathbf{e}(x), \quad \mathbf{v} = \sum_{y\in X} \beta_y \mathbf{e}(y),$$

где коэффициенты α_x и β_y — элементы из $\mathbb{K}$, однозначно определённые векторами $\mathbf{u}$ и $\mathbf{v}$. Чтобы задать $\mathbf{u} \boxdot \mathbf{v}$, вначале вынесем эти коэффициенты за скобки:

$$\mathbf{u} \boxdot \mathbf{v} = \left(\sum_{x\in X} \alpha_x \mathbf{e}(x)\right) \boxdot \left(\sum_{y\in X} \beta_y \mathbf{e}(y)\right) = \sum_{x,y\in X} \alpha_x \beta_y (\mathbf{e}(x) \boxdot \mathbf{e}(y)).$$

Затем заменим каждое $\mathbf{e}(x) \boxdot \mathbf{e}(y)$ на $\mathbf{e}(x \odot y)$ и получим

$$\mathbf{u} \boxdot \mathbf{v} = \sum_{x,y\in X} \alpha_x \beta_y \mathbf{e}(x \odot y). \tag{1}$$

Правая часть — линейная комбинация векторов базиса, т. е. корректно определённый вектор из $\mathbb{K}^X$, и мы возьмём его в качестве $\mathbf{u} \boxdot \mathbf{v}$ по определению. Разумеется, можно было сразу задать $\boxdot$ посредством формулы (1), но предыдущая выкладка показывает, как прийти к этому определению исходя из идеи, что операция $\boxdot$ должна быть линейным продолжением операции $\odot$.

Легко проверить, что если операция $\odot$ ассоциативна, то $\boxdot$ также ассоциативна (предоставляем это читателю). С другой стороны, если (a, b, c) — неассоциативная тройка относительно $\odot$, то $(\mathbf{e}(a), \mathbf{e}(b), \mathbf{e}(c))$, очевидно, неассоциативная тройка относительно $\boxdot$.

Важнейшая черта этой конструкции, однако, в том, что для $\boxdot$ найдётся гораздо больше неассоциативных троек: даже если для $\odot$ неассоциативная тройка только одна, то для $\boxdot$ их очень много и, как мы увидим, скорее всего мы попадём на одну из них при случайном выборе.

Теперь мы готовы описать алгоритм проверки ассоциативности[1]. Зафиксируем множество $S \subset \mathbb{K}$ из шести элементов.

1. Для каждого $x \in X$ выберем случайные элементы $\alpha_x, \beta_x, \gamma_x \in S$, распределённые равномерно и независимо.
2. Положим $\mathbf{u} := \sum\limits_{x \in X} \alpha_x \mathbf{e}(x)$, $\mathbf{v} := \sum\limits_{y \in X} \beta_y \mathbf{e}(y)$ и $\mathbf{w} := \sum\limits_{z \in X} \gamma_z \mathbf{e}(z)$.
3. Вычислим векторы $(\mathbf{u} \boxdot \mathbf{v}) \boxdot \mathbf{w}$ и $\mathbf{u} \boxdot (\mathbf{v} \boxdot \mathbf{w})$. Если они равны, то алгоритм выдаёт ответ ДА; в противном случае — ответ НЕТ.

Для двух произвольных векторов $\mathbf{u}, \mathbf{v} \in \mathbb{K}^X$ вектор $\mathbf{u} \boxdot \mathbf{v}$ можно вычислить, следуя определению (1), за $O(n^2)$ обращений к таблице операции $\odot$ и $O(n^2)$ операций в поле $\mathbb{K}$. Если считать, что каждая операция в поле $\mathbb{K}$ требует фиксированного времени, то ясно, что алгоритм выполняется за время $O(n^2)$.

Так как операция $\boxdot$ ассоциативна в случае ассоциативной операции $\odot$, ясно также, что для ассоциативной операции алгоритм всегда даст ответ ДА. Чтобы доказать теорему, теперь достаточно убедиться в следующем.

Утверждение. *Если операция $\odot$ не ассоциативна, а $\mathbf{u}, \mathbf{v}, \mathbf{w}$ выбираются случайно, как в описанном алгоритме, то*

$$(\mathbf{u} \boxdot \mathbf{v}) \boxdot \mathbf{w} \neq \mathbf{u} \boxdot (\mathbf{v} \boxdot \mathbf{w})$$

с вероятностью не меньше $\frac{1}{2}$.

Доказательство утверждения. Зафиксируем неассоциативную тройку $(a, b, c) \in X^3$. Будем выбирать $\alpha_x, \beta_y, \gamma_z \in S$ случайным образом согласно алгоритму, причём будем считать, что α_a, β_b и γ_c выбираются последними, когда все остальные $\alpha_x, \beta_y, \gamma_z$ уже зафиксированы. На самом деле мы покажем, что если зафиксировать произвольные значения всех величин $\alpha_x, \beta_y, \gamma_z$, $x \neq a$, $y \neq b$, $z \neq c$, а затем

[1] Напомним, что проверяется ассоциативность тройки $x, y, z \in X$. — *Прим. перев.*

выбрать α_a, β_b и γ_c случайным образом, то вероятность неравенства

$$(\mathbf{u}\boxdot\mathbf{v})\boxdot\mathbf{w}\neq\mathbf{u}\boxdot(\mathbf{v}\boxdot\mathbf{w})$$

будет не меньше $\frac{1}{2}$.

Для этого покажем, что с вероятностью не меньше $\frac{1}{2}$ эти векторы отличаются компонентой с номером

$$r:=(a\odot b)\odot c,$$

т. е. $((\mathbf{u}\boxdot\mathbf{v})\boxdot\mathbf{w})_r\neq(\mathbf{u}\boxdot(\mathbf{v}\boxdot\mathbf{w}))_r$. Чтобы подчеркнуть, что мы рассматриваем α_a, β_b и γ_c как (случайные) переменные, тогда как все остальные $\alpha_x, \beta_y, \gamma_z$ считаются константами, мы запишем

$$f(\alpha_a,\beta_b,\gamma_c):=((\mathbf{u}\boxdot\mathbf{v})\boxdot\mathbf{w})_r,\quad g(\alpha_a,\beta_b,\gamma_c):=(\mathbf{u}\boxdot(\mathbf{v}\boxdot\mathbf{w}))_r.$$

По определению операции $\boxdot$ получаем

$$f(\alpha_a,\beta_b,\gamma_c)=\sum_{x,y,z\in X,(x\odot y)\odot z=r}\alpha_x\beta_y\gamma_z.$$

Таким образом, $f(\alpha_a,\beta_b,\gamma_c)$ — многочлен от α_a, β_b, γ_c степени не выше 3. Поскольку $(a\odot b)\odot c=r$, слагаемое $\alpha_a\beta_b\gamma_c$ появляется с коэффициентом 1 (и потому степень равна 3).

Аналогично получаем

$$g(\alpha_a,\beta_b,\gamma_c)=\sum_{x,y,z\in X,x\odot(y\odot z)=r}\alpha_x\beta_y\gamma_z.$$

Но при этом $a\odot(b\odot c)\neq r$, поскольку (a,b,c) — неассоциативная тройка, и потому коэффициент при $\alpha_a\beta_b\gamma_c$ в многочлене $g(\alpha_a,\beta_b,\gamma_c)$ равен 0.

Теперь можно воспользоваться услугами нашего надёжного помощника — теоремы Шварца—Зиппеля из миниатюры 24: разность $f(\alpha_a,\beta_b,\gamma_c)-g(\alpha_a,\beta_b,\gamma_c)$ является ненулевым многочленом степени 3, поэтому вероятность получить для него значение 0 при подстановке независимых случайных элементов из S вместо переменных $\alpha_a,\beta_b,\gamma_c$ не превосходит $\frac{3}{|S|}=\frac{1}{2}$. Значит, для случайных $\alpha_a,\beta_b,\gamma_c$ мы получим $f(\alpha_a,\beta_b,\gamma_c)\neq g(\alpha_a,\beta_b,\gamma_c)$ с вероятностью не меньше $\frac{1}{2}$. Этим завершено доказательство нашего утверждения, а с ним и теоремы. □

Литература

Rajagopalan S., Schulman L. Verification of Identities // SIAM J. Computing. 2000. V. 29, № 4. P. 1155—1163.

Миниатюра 28

Тайный агент и зонтик

Секретный правительственный агент в тренировочном лагере террористов в пустыне имеет очень ограниченные возможности посылать сообщения. У него пять шарфов: красный, бежевый, зелёный, синий и пурпурный, и каждый день он включает один из них в своё обмундирование. Штабные аналитики определяют цвет его шарфа по фотографии со спутника.

Но так как шарфы не совсем чистые, оказалось, что некоторые пары цветов нельзя надёжно различить. Варианты путаницы показаны на рис. 38.

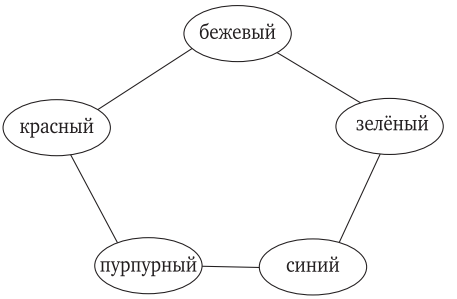


Рис. 38

Например, нельзя надёжно отличить пурпурный ни от синего, ни от красного, но невозможно перепутать пурпурный с бежевым или зелёным.

Чтобы обеспечить надёжность передачи, агент может, например, использовать только синий и красный шарф и, следовательно, посылать каждый день одно из двух возможных сообщений — в терминах информатики один бит. За k дней он сможет передать одно из 2^k возможных сообщений.

Среди каждых трёх шарфов есть два, которые можно перепутать, так что может показаться, что нет возможности передать за день больше одного бита. Но есть способ лучше! За два последователь-

ных дня агент может послать одно из пяти сообщений, например, следующим образом.

	Первый день	Второй день
Сообщение 1	красный	красный
Сообщение 2	бежевый	зелёный
Сообщение 3	зелёный	пурпурный
Сообщение 4	синий	бежевый
Сообщение 5	пурпурный	синий

В самом деле, читатель легко проверит, что никакую из этих двухдневных комбинаций нельзя перепутать с другой. Поэтому агент за k дней (при чётном k) может передать одно из $5^{k/2} = (\sqrt{5})^k$ возможных сообщений, так что эффективность в расчёте на день возросла с 2 до $\sqrt{5}$.

Можно ли ещё больше поднять эффективность, используя, скажем, трёхдневные или десятидневные комбинации? Это трудная математическая задача. Ответ отрицательный, и приведённое ниже замечательное доказательство — единственное известное.

Сначала сформулируем задачу на математическом языке (и обобщим её). Рассмотрим некоторый **алфавит** S; в нашем случае S состоит из пяти возможных цветов шарфа. Некоторые пары символов из S можно перепутать (иначе говоря, они *взаимозаменимы*), и это изображается графом $G = (S, E)$, где пары взаимозаменимых символов из S соединены рёбрами. Для случая пяти шарфов этот граф изображён на рис. 38: это цикл длины 5, обозначаемый C_5.

Рассмотрим два сообщения длины k, имеющие вид $a_1a_2\ldots a_k$ и $b_1b_2\ldots b_k$. В терминах теории кодирования это слова длины k над алфавитом S; см. миниатюру 5. Эти сообщения взаимозаменимы в точности тогда, когда a_i взаимозаменимо с b_i (в том смысле, что $a_i = b_i$ или $\{a_i, b_i\} \in E$) при всех $i = 1, 2, \ldots, k$.

Пусть $\alpha_k(G)$ — максимальный размер множества сообщений длины k, не содержащего взаимозаменимой пары. В частности, $\alpha_1(G)$ — максимальный размер **независимого множества** в графе G, т. е. множества вершин, в котором никакие две вершины не соединены рёбрами. Эта величина обычно обозначается $\alpha(G)$. В нашем примере $\alpha_1(C_5) = \alpha(C_5) = 2$. Из таблицы видно, что $\alpha_2(C_5) \geqslant 5$, причём

на самом деле выполнено равенство, и это весьма частный случай результата, который мы собираемся доказать.

Шенноновская ёмкость графа G определяется следующим образом:

$$\Theta(G) := \sup\bigl\{\alpha_k(G)^{1/k} : k = 1, 2, \ldots\bigr\}.$$

Она выражает максимальную возможную эффективность передачи одного символа из сообщения. При достаточно большом k агент может послать одно из примерно $\Theta(C_5)^k$ возможных сообщений за k дней, но не больше. Верна следующая

Теорема. *Справедливо равенство* $\Theta(C_5) = \sqrt{5}$.

Доказательство теоремы. Прежде всего заметим, что $\alpha_k(G)$ равно максимальному размеру независимого множества некоторого подходящего графа. Его множеством вершин является S^k, т. е. его вершины — все возможные сообщения (слова) длины k, причём две вершины $a_1a_2\ldots a_k$ и $b_1b_2\ldots b_k$ соединены ребром, если они взаимозаменимы. Обозначим этот граф через G^k и будем называть его **сильным произведением** k экземпляров графа G. Сильное произведение $H \cdot H'$ двух произвольных графов H и H' определяется следующим образом:

$$\begin{aligned} V(H \cdot H') &= V(H) \times V(H'), \\ E(H \cdot H') &= \{\{(u,u'),(v,v')\} : \ (u = v \text{ или } \{u,v\} \in E(H)) \\ &\qquad\qquad \text{и одновременно} \\ &\qquad\qquad (u' = v' \text{ или } \{u',v'\} \in E(H'))\}. \end{aligned}$$

Итак, для оценки $\Theta(C_5)$ сверху нам нужно ограничить максимальный размер независимых множеств в каждом из графов C_5^k. Установим два общих факта, связывающих независимые множества в графах с определёнными системами векторов. Пусть $H = (V, E)$ — произвольный граф. **Ортогональным представлением** графа H называется отображение $\rho : V \to \mathbb{R}^n$ для некоторого n, которое сопоставляет каждой вершине $v \in V(H)$ *единичный* вектор $\rho(v)$ (т. е. $\|\rho(v)\| = 1$), причём выполнено следующее.

> Если две различные вершины u, v *не связаны* ребром, то соответствующие векторы *ортогональны*. На языке формул из того, что $\{u, v\} \notin E$ следует, что $\langle \rho(u), \rho(v) \rangle = 0$.

(Здесь $\langle ., . \rangle$ обозначает стандартное скалярное произведение в $\mathbb{R}^n$.)

Чтобы доказать нашу основную теорему, потребуется интересное ортогональное представление ρ_{LU} графа C_5 в $\mathbb{R}^3$ — «зонтик Ловаса». Представим себе сложенный зонтик с пятью рёбрами единичной длины, трость которого — вектор $\mathbf{e}_1 = (1, 0, 0)$. Будем медленно открывать зонтик, пока все пары несмежных рёбер не станут ортогональными (см. рис. 39).

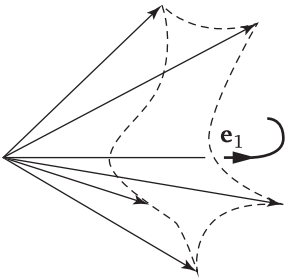


Рис. 39

В этот момент рёбра задают единичные векторы $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_5$. Сопоставляя каждому вектору $\mathbf{v}_i$ вершину графа C_5 с номером i, получаем ортогональное представление ρ_{LU}. Угол раскрытия зонтика вычисляется без труда: $\langle \mathbf{v}_i, \mathbf{e}_1 \rangle = 5^{-1/4}$, что нам скоро потребуется.

Каждое ортогональное представление графа G даёт следующую верхнюю границу для $\alpha(G)$.

Лемма А. *Пусть H — граф, ρ — его ортогональное представление. Тогда $\alpha(H) \leqslant \vartheta(H, \rho)$, где*

$$\vartheta(H, \rho) := \max_{v \in V(H)} \frac{1}{\langle \rho(v), \mathbf{e}_1 \rangle^2}.$$

Доказательство леммы А. Построение ортогонального представления ρ с минимальным $\vartheta(H, \rho)$ имеет следующий геометрический смысл: мы хотим упаковать все единичные векторы $\rho(v)$ в сферическую шапку с центром $\mathbf{e}_1$ и наименьшим возможным радиусом.

Векторы сопротивляются такой упаковке, поскольку пары, отвечающие отсутствию рёбер, должны быть ортогональны. В частности, ортонормированную систему образуют векторы, отвечающие независимому множеству в H, и для такой системы минимальный радиус шапки можно вычислить точно.

В формальном доказательстве используется тот факт, что для произвольной ортонормированной системы векторов

$(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m)$ в некотором пространстве $\mathbb{R}^n$ и для произвольного вектора $\mathbf{u}$ выполнено неравенство

$$\sum_{i=1}^{m} \langle \mathbf{v}_i, \mathbf{u} \rangle^2 \leqslant \|\mathbf{u}\|^2.$$

Действительно, данную систему $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m)$ можно расширить до ортонормированного базиса $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ пространства $\mathbb{R}^n$, добавив ещё $n-m$ подходящих векторов $(\mathbf{v}_{m+1}, \mathbf{v}_{m+2}, \ldots, \mathbf{v}_n)$. Тогда i-я компонента вектора $\mathbf{u}$ будет равна $\langle \mathbf{v}_i, \mathbf{u} \rangle$, откуда по теореме Пифагора получаем $\|\mathbf{u}\|^2 = \sum_{i=1}^{n} \langle \mathbf{v}_i, \mathbf{u} \rangle^2$. Нужное неравенство получается отбрасыванием последних $n-m$ слагаемых в правой части.

Если теперь $I \subseteq V(H)$ — независимое множество в графе H, то, как отмечено выше, векторы $\rho(v)$, $v \in I$, образуют ортонормированную систему, так что

$$\sum_{v \in I} \langle \rho(v), \mathbf{e}_1 \rangle^2 \leqslant \|\mathbf{e}_1\|^2 = 1.$$

Значит, существует $v \in I$, для которого $\langle \rho(v), \mathbf{e}_1 \rangle^2 \leqslant \frac{1}{|I|}$, и потому $\vartheta(H, \rho) \geqslant |I|$. □

Используя лемму А и зонтик Ловаса, получаем

$$\alpha(C_5) \leqslant \vartheta(C_5, \rho_{\mathrm{LU}}) = \sqrt{5}.$$

Это (ещё) не потрясающий результат, так как все знают, что $\alpha(C_5) = 2$. Потребуется добавить к нему следующую лемму, которая показывает, что ортогональные представления хорошо себя ведут по отношению к сильному произведению.

Лемма В. *Пусть H_1, H_2 — графы, ρ_i — ортогональное представление графа H_i при $i = 1, 2$. Тогда существует ортогональное представление ρ сильного произведения $H_1 \cdot H_2$, для которого*

$$\vartheta(H_1 \cdot H_2, \rho) = \vartheta(H_1, \rho_1) \cdot \vartheta(H_2, \rho_2).$$

Применяя лемму В к сильному произведению k экземпляров графа C_5 индукцией по k получим

$$\alpha(C_5^k) \leqslant \vartheta(C_5, \rho_{\mathrm{LU}})^k = \sqrt{5}^k,$$

а значит, $\Theta(C_5) \leqslant \sqrt{5}$ откуда и будет следовать утверждение теоремы.

Доказательство леммы B. Вспомним операцию **тензорного произведения**, уже использованную в миниатюре 18. Тензорным произведением двух векторов $\mathbf{x} \in \mathbb{R}^m$ и $\mathbf{y} \in \mathbb{R}^n$ называется вектор из $\mathbb{R}^{mn}$, обозначаемый $\mathbf{x} \otimes \mathbf{y}$, компоненты которого равны $x_i y_j$ при $i = 1, 2, \ldots, m$ и $j = 1, 2, \ldots, n$. Например, если $\mathbf{x} = (x_1, x_2, x_3)$ и $\mathbf{y} = (y_1, y_2)$, то

$$\mathbf{x} \otimes \mathbf{y} = (x_1 y_1, x_2 y_1, x_3 y_1, x_1 y_2, x_2 y_2, x_3 y_2) \in \mathbb{R}^6.$$

Нам потребуется следующий факт, рутинное доказательство которого оставляем читателю:

$$\langle \mathbf{x} \otimes \mathbf{y}, \mathbf{x}' \otimes \mathbf{y}' \rangle = \langle \mathbf{x}, \mathbf{x}' \rangle \cdot \langle \mathbf{y}, \mathbf{y}' \rangle \tag{1}$$

для произвольных $\mathbf{x}, \mathbf{x}' \in \mathbb{R}^m$, $\mathbf{y}, \mathbf{y}' \in \mathbb{R}^n$.

Теперь можно построить ортогональное представление ρ сильного произведения $H_1 \cdot H_2$, о котором говорится в лемме. Вершины графа $H_1 \cdot H_2$ — пары (v_1, v_2), $v_1 \in V(H_1)$, $v_2 \in V(H_2)$. Положим

$$\rho((v_1, v_2)) := \rho_1(v_1) \otimes \rho_2(v_2).$$

С помощью равенства (1) можно легко проверить, что ρ — ортогональное представление графа $H_1 \cdot H_2$, причём выполнено равенство $\vartheta(H_1 \cdot H_2, \rho) = \vartheta(H_1, \rho_1) \cdot \vartheta(H_2, \rho_2)$. Доказательство леммы B завершено. □

Тем самым теорема доказана. □

Замечания. Величина

$$\vartheta(G) = \inf\{\vartheta(G, \rho) : \rho \text{ — ортогональное представление графа } G\}$$

называется **тета-функцией Ловаса** графа G. Как мы видели, она даёт верхнюю границу для $\alpha(G)$ — числа независимости графа. Нетрудно доказать, что она также обеспечивает нижнюю оценку для **хроматического числа** дополнения к графу G — иначе говоря, для минимального количества полных подграфов, которым можно покрыть G. Вычисление числа независимости или хроматического числа данного графа — трудная алгоритмическая задача (NP-полная), но, к удивлению, $\vartheta(G)$ можно вычислить за полиномиальное время (точнее, аппроксимировать с любой заданной точностью). В силу этого и нескольких других замечательных свойств тета-функция Ловаса очень важна.

Шенноновская ёмкость — гораздо более трудный орешек. Для её вычисления, хотя бы приближённого, не известно *вообще никакого*

алгоритма, полиномиального или нет. И не приходится долго искать нерешённый случай — неизвестно уже $\Theta(C_7)$! Если бы у агента было семь шарфов, никто не смог бы назвать ему наилучший способ передачи сообщений.

Литература

Lovász L. On the Shannon capacity of a graph // IEEE Trans. Inform. Th. 1979. V. 25. P. 1—7.

Миниатюра 29

Шенноновская ёмкость объединения: повесть о двух полях

Здесь мы продолжим тему миниатюры 28 — шенноновскую ёмкость графа. Однако для удобства мы повторим соответствующие определения. Чтобы понять мотивировку понятия шенноновской ёмкости, полезно также прочитать начало миниатюры 28.

Вначале напомним, что если G — некоторый граф, то $\alpha(G)$ обозначает максимальный размер независимого множества в нём, т. е. такого множества $I \subseteq V(G)$, что никакие две вершины в I не соединены ребром. **Сильное произведение** $H \cdot H'$ графов H и H' имеет множество вершин $V(H) \times V(H')$, причём две вершины из этого множества, которые можно обозначить (u, u') и (v, v'), соединены ребром, если $u = v$ или $\{u, v\} \in E(H)$ и одновременно $u' = v'$ или $\{u', v'\} \in E(H')$.

Шенноновская ёмкость графа G обозначается $\Theta(G)$ и по определению равна

$$\Theta(G) := \sup\bigl\{\alpha(G^k)^{1/k} \colon k = 1, 2, \ldots\bigr\},$$

где G^k обозначает сильное произведение k экземпляров графа G.

Шенноновская сложность очень важна в теории кодирования и долгое время изучалась в теории графов с большим интересом, но она до сих пор остаётся одним из самых загадочных свойств графов. Цель этого раздела — доказать удивительный результат, относящийся к поведению шенноновской сложности при операции дизъюнктного объединения графов.

Неформально говоря, **дизъюнктное объединение** графов G и H, обозначаемое $G + H$, — это граф, полученный «прикладыванием» графа G к H. Формально определить дизъюнктное объединение легко, если множества вершин $V(G)$ и $V(H)$ не пересекаются; тогда можно просто положить $V(G + H) := V(G) \cup V(H)$ и $E(G + H) := E(G) \cup E(H)$. Однако в общем случае G и H могут иметь общие вершины, их множества вершин могут даже совпадать. В этом случае нужно вначале построить изоморфную копию H' графа H, для

которой $V(G) \cap V(H') = \varnothing$, а затем положить

$$V(G+H) := V(G) \cup V(H'), \quad E(G+H) := E(G) \cup E(H').$$

(при этом граф $G+H$ определяется лишь с точностью до изоморфизма, но для наших целей это как раз подходит).

Вот приятное, но не совсем тривиальное упражнение, и мы даже не побуждаем читателя его выполнять: доказать, что

$$\Theta(G+H) \geqslant \Theta(G) + \Theta(H) \tag{1}$$

для любых двух графов G и H.

На языке теории кодирования, см. миниатюру 28, величина $\Theta(G)$ равна количеству различимых сообщений «в расчёте на символ», которые можно передать посредством (произвольно длинных) сообщений из символов алфавита $V(G)$, и аналогично для $\Theta(H)$. Тогда неравенство (1) означает, что если никакой символ из алфавита $V(G)$ нельзя перепутать с символом из алфавита $V(H)$ и если можно посылать сообщения, составленные из символов обоих алфавитов, то количество различимых сообщений «в расчёте на символ» не меньше $\Theta(G) + \Theta(H)$. Читатель, вероятно, согласится, что это звучит вполне правдоподобно, если не интуитивно очевидно.

Однако столь же правдоподобно или интуитивно очевидно выглядит следующее утверждение: в соотношении (1) всегда должно выполняться равенство (что и предполагал Шеннон). Но это оказалось неверно, и именно этот результат мы выше анонсировали как удивительный.

Теорема. *Существуют графы G и H, для которых*

$$\Theta(G+H) > \Theta(G) + \Theta(H).$$

Для доказательства мы подготовим два инструмента: первый потребуется, чтобы ограничить $\Theta(G+H)$ снизу, а второй — чтобы ограничить $\Theta(G)$ и $\Theta(H)$ сверху. Первый инструмент — следующая простая лемма.

Лемма. *Пусть G — граф с m вершинами, $\overline{G}$ — его дополнение, т. е. граф на множестве вершин $V(G)$, в котором две различные вершины u, v смежны в точности тогда, когда они не смежны в G. Тогда*

$$\Theta(G+\overline{G}) \geqslant \sqrt{2m}.$$

Доказательство леммы. В силу определения шенноновской ёмкости достаточно найти независимое множество размера $2m$ в сильном произведении $(G+\overline{G})^2$.

Пусть $v_1, v_2, \ldots, v_m$ — вершины графа G, а $v_1', v_2', \ldots, v_m'$ — вершины изоморфной копии графа $\overline{G}$, используемой при образовании дизъюнктного объединения $G + \overline{G}$. Положим

$$I := \{(v_1, v_1'), (v_2, v_2'), \ldots, (v_m, v_m')\} \cup \{(v_1', v_1), (v_2', v_2), \ldots, (v_m', v_m)\}.$$

Тогда I независимо в $(G + \overline{G})^2$. Действительно, (v_i, v_i') и (v_j', v_j) не смежны, поскольку v_i и v_j' не смежны в $G + \overline{G}$, а (v_i, v_i') и (v_j, v_j'), $i \neq j$, не смежны[1], поскольку или v_i и v_j не смежны в G, или v_i' и v_j' не смежны в (изоморфной копии графа) $\overline{G}$. Лемма доказана. □

Функциональные представления. Второй инструмент — алгебраический, он нужен, чтобы ограничить $\Theta(.)$ сверху. Пусть $\mathbb{K}$ — некоторое поле (например, $\mathbb{R}$, $\mathbb{Q}$ или $\mathbb{F}_2$), а $G = (V, E)$ — некоторый граф. **Функциональное представление** $\mathscr{F}$ графа G над $\mathbb{K}$ определяют следующие объекты:

- основное множество X (произвольное множество, не обязательно как-то связанное с G или $\mathbb{K}$),
- для каждой вершины $v \in V$ — элемент $c_v \in X$,
- для каждой вершины $v \in V$ — функция $f_v : X \to \mathbb{K}$,

причём должны выполняться следующие условия:

(i) $f_v(c_v) \neq 0$ для каждого $v \in V$,

(ii) если u, v — различные и *не смежные* вершины графа G, то

$$f_u(c_v) = 0.$$

(Если u и v смежны, то $f_u(c_v)$ может быть каким угодно.)

Положим $\mathscr{F} = (X, (c_v, f_v)_{v \in V})$. (Ортогональное представление графа G, см. миниатюру 28, также естественно интерпретируется как его функциональное представление — читатель может это проверить.)

Размерность $\dim \mathscr{F}$ функционального представления $\mathscr{F}$ — это размерность подпространства, порождённого всеми функциями f_v, $v \in V$, в векторном пространстве $\mathbb{K}^X$ всех функций $X \to \mathbb{K}$. (Как обычно, функции складываются поточечно: $(f + g)(x) = f(x) + g(x)$, а также поточечно умножаются на элементы из $\mathbb{K}$.)

Предложение. *Если G имеет функциональное представление размерности d над некоторым полем $\mathbb{K}$, то $\Theta(G) \leqslant d$.*

[1] И, разумеется, по той же причине не смежны (v_i', v_i) и (v_j', v_j). — *Прим. перев.*

Это предложение немедленно вытекает из определения шенноновской ёмкости и следующих двух утверждений.

Утверждение A. *Если G имеет функциональное представление $\mathscr{F} = (X, (c_v, f_v)_{v\in V})$ над некоторым полем $\mathbb{K}$, то $\alpha(G) \leqslant \dim \mathscr{F}$.*

Утверждение B. *Пусть граф $G = (V, E)$ имеет функциональное представление $\mathscr{F}$ над некоторым полем $\mathbb{K}$, а $G' = (V', E')$ имеет функциональное представление $\mathscr{F}'$ над тем же $\mathbb{K}$. Тогда сильное произведение $G \cdot G'$ имеет функциональное представление над $\mathbb{K}$ размерности не выше $\dim \mathscr{F} \cdot \dim \mathscr{F}'$.*

Доказательство утверждения A. Достаточно показать, что если множество $I \subseteq V(G)$ независимо, то функции f_v, $v \in I$, линейно независимы.

Это делается вполне стандартным образом. Предположим, что

$$\sum_{v\in I} t_v f_v = 0 \tag{2}$$

для некоторых скаляров t_v, $v \in I$ (нуль в правой части — это функция, равная 0 при каждом $x \in X$). Зафиксируем $u \in V$ и оценим левую часть равенства (2) в точке c_u. Поскольку никакие две различные вершины $u, v \in I$ не соединены ребром, имеем $f_v(c_u) = 0$ при $v \neq u$, откуда следует, что $\sum\limits_{v\in I} t_v f_v(c_u) = t_u f_u(c_u)$. Поскольку $f_u(c_u) \neq 0$, имеем $t_u = 0$, а так как u произвольно, функции f_v линейно независимы, как и утверждалось. □

Доказательство утверждения B. Начнём с того, что вполне естественным образом определим функциональное представление $\mathscr{G}$ графа $G \cdot G'$ (которое можно рассматривать как тензорное произведение представлений $\mathscr{F}$ и $\mathscr{F}'$). Пусть $\mathscr{F} = (X, (c_v, f_v)_{v\in V})$ и $\mathscr{F}' = (X', (c'_{v'}, f'_{v'})_{v'\in V'})$. Основным множеством для $\mathscr{G}$ является $X \times X'$. Вершины из $G \cdot G'$ имеют вид $(v, v') \in V \times V'$, и мы полностью зададим $\mathscr{G}$, положив

$$c_{(v,v')} = (c_v, c'_{v'}) \in X \times X', \quad f_{(v,v')} := f_v \otimes f'_{v'},$$

где $f_v \otimes f'_{v'}$ обозначает функцию $X \times X' \to \mathbb{K}$ вида $(f_v \otimes f'_{v'})(x, x') := f_v(x) f'_{v'}(x')$. Непосредственно проверяется, что такое $\mathscr{G}$ действительно удовлетворяет аксиомам (i) и (ii) функционального представления (предоставляем это читателю).

Остаётся проверить, что $\dim \mathscr{G} \leqslant \dim \mathscr{F} \cdot \dim \mathscr{F}'$. Это также не составляет труда: если все f_v — линейные комбинации базисных функций $b_1, \ldots, b_d$, а $f'_{v'}$ — линейные комбинации функций $b'_1, \ldots, b'_{d'}$, то

почти очевидно, что каждая функция $f_v \otimes f'_{v'}$ является линейной комбинацией функций вида $b_i \otimes b'_j$, $i = 1, 2, \ldots, d$, $j = 1, 2, \ldots, d'$. (Можно проверить, что $\dim \mathscr{G}$ на самом деле равно $\dim \mathscr{F} \cdot \dim \mathscr{F}'$.) □

Доказательство теоремы. Нам осталось построить соответствующие графы G и H и применить подготовленные инструменты. Известно несколько подходящих конструкций, и некоторые из них показывают, что $\Theta(G+H)$ в действительности может быть *намного* больше, чем $\Theta(G)+\Theta(H)$. Здесь мы для простоты приведём лишь одну очень конкретную конструкцию, для которой $\Theta(G+H)$ лишь «несколько больше», чем $\Theta(G)+\Theta(H)$.

Пусть s — целочисленный параметр; далее мы установим, что в доказательстве теоремы достаточно взять $s = 16$. Все вершины графа G — трёхэлементные подмножества в множестве $\{1, 2, \ldots, s\}$, и две такие вершины A и B соединены ребром, если $|A \cap B| = 1$. (Графы такого рода, где вершинами являются множества, а рёбра определяются мощностью их пересечений, служат очень интересными примерами во многих теоретико-графовых вопросах.)

В качестве H возьмём дополнение $\overline{G}$ графа G.

Прежде всего, G имеет $\binom{s}{3}$ вершин, так что $\Theta(G+\overline{G}) \geqslant \sqrt{2\binom{s}{3}}$ согласно лемме.

Теперь определим подходящие функциональные представления. В случае графа G используем поле $\mathbb{F}_2$, а в качестве основного множества X возьмём $\mathbb{F}_2^s$, так что его элементами являются s-компонентные векторы из нулей и единиц. Если $A \in V(G)$ — вершина, т. е. трёхэлементное множество, то пусть $\mathbf{c}_A$ — его характеристический вектор: $(\mathbf{c}_A)_i = 1$ при $i \in A$ и $(\mathbf{c}_A)_i = 0$ при $i \notin A$. Наконец, функция $f_A \colon \mathbb{F}_2^s \to \mathbb{F}_2$ имеет вид $f_A(\mathbf{x}) = \sum\limits_{i \in A} x_i$ (со сложением в $\mathbb{F}_2$, т. е. по модулю 2).

Убедимся, что это действительно функциональное представление графа G. Заметим, что $f_A(\mathbf{c}_B)$ равно $|A \cap B|$ по модулю 2. В частности, $f_A(\mathbf{c}_A) = 1 \neq 0$. Если теперь вершины $A \neq B$ не смежны в G, то $|A \cap B|$ может быть равно 2 или 0, и в этом случае $f_A(\mathbf{c}_B) = 0$.

Размерность этого функционального представления не превосходит s, поскольку каждое f_A является линейной комбинацией координатных функций $\mathbf{x} \mapsto x_i$. Следовательно (согласно доказанному предложению), $\Theta(G) \leqslant s$.

Для $\overline{G}$ используем очень похожее функциональное представление, но над другим полем, например $\mathbb{R}$ (можно взять любое другое

поле характеристики, отличной от 2). А именно, положим $X' := \mathbb{R}^s$, пусть снова $\mathbf{c}'_A$ — характеристический вектор множества A (рассматриваемый в этот раз как вещественный вектор), и пусть $f'_A(\mathbf{x}) := \left(\sum_{i\in A} x_i\right) - 1$. Тогда $f'_A(\mathbf{c}'_B) = |A\cap B| - 1$, откуда $f'_A(\mathbf{c}'_A) = 2 \neq 0$, а для вершин $A \neq B$, не смежных в $\overline{G}$, получаем $|A\cap B| = 1$ и $f'_A(\mathbf{c}'_B) = 0$, что и требовалось. Размерность представления в этот раз не превосходит $s+1$ (в дополнение к координатным функциям $\mathbf{x}\mapsto x_i$ нужно также включить в базис константу -1), откуда получаем $\Theta(\overline{G}) \leqslant s+1$.

Для завершения доказательства выберем s достаточно большим, чтобы было $\sqrt{2\binom{s}{3}} > 2s+1$. Вычисление показывает, что наименьшее подходящее s равно 16. Тогда каждый из графов G и $\overline{G}$ имеет 560 вершин. □

Замечание. Интересно сравнить рассмотренные здесь функциональные представления с ортогональными представлениями из миниатюры 28. Эти понятия по существу похожи, так же как и доказательства, что оба они дают верхние оценки для $\Theta(G)$. Однако функциональные представления могут дать только целочисленные оценки, поэтому они не могут обеспечить, например, что $\Theta(C_5) \leqslant \sqrt{5}$. С другой стороны, ортогональные представления не выглядят подходящими для доказательства из этого раздела, поскольку в нём существенно использование двух различных полей, как мы сейчас покажем.

В самом деле, рассуждая как при доказательстве леммы, можно получить оценку $\alpha(G\cdot\overline{G}) \geqslant m$ для любого графа G с m вершинами. Таким образом, если $\mathscr{F}$ — функциональное представление графа G, а $\mathscr{F}'$ — функциональное представление графа $\overline{G}$ над тем же полем, то $(\dim\mathscr{F})(\dim\mathscr{F}') \geqslant m$ согласно утверждениям A и B. Следовательно, $\dim\mathscr{F} + \dim\mathscr{F}' \geqslant 2\sqrt{m}$ (по неравенству между средним арифметическим и средним геометрическим), и потому функциональные представления над одним и тем же полем не могут дать верхнюю оценку для $\Theta(G) + \Theta(\overline{G})$, меньшую чем $\sqrt{2m}$, что согласно лемме является нижней оценкой для $\Theta(G+\overline{G})$.

Литература

Alon N. The Shannon capacity of a union // Combinatorica. 1998. V. 18. P. 301—310.

Наше доказательство приводит к более слабому результату и при этом несколько проще.

Миниатюра 30

Равносторонние множества

Равносторонним множеством в пространстве $\mathbb{R}^d$ называется множество точек $\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_n$, в котором расстояния между всеми парами различных точек $\mathbf{p}_i, \mathbf{p}_j$ одинаковы.

Мы намеренно не сказали, какое расстояние имеем в виду. Это сыграет ключевую роль в данном разделе. Если рассматривать самое привычное *евклидово* расстояние, то нетрудно доказать, что равностороннее множество в $\mathbb{R}^d$ может содержать $d+1$ точек, но не больше.

Попутно напомним классическое доказательство, что больше $d+1$ таких точек быть не может. Его метод очень напоминает миниатюру 6. Обозначим точки через $\mathbf{p}_1, \ldots, \mathbf{p}_{n+1}$. После параллельного сдвига можно считать, что $\mathbf{p}_{n+1} = \mathbf{0}$, а после растяжения — что расстояния в парах точек равны 1. Построим матрицу Грама G, состоящую из скалярных произведений: $g_{ij} = \langle \mathbf{p}_i, \mathbf{p}_j \rangle$. Из условия равносторонности получаем, что $G = \frac{1}{2}(I_n + J_n)$, где I_n — единичная матрица, а J_n — матрица из единиц, поэтому $\operatorname{rank}(G) = n$. С другой стороны, $G = P^T P$, где P — матрица размера $d \times n$, в которой i-й столбец равен вектору $\mathbf{p}_i$ при каждом i, поэтому $\operatorname{rank}(G) \leqslant d$, откуда $n \leqslant d$.

(А кстати, как доказать строго, что равностороннее множество из $(d+1)$ точек возможно? Подходят, например, векторы стандартного базиса $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_d$ плюс точка $(-t, -t, \ldots, -t)$ при подходящем $t > 0$: даже если нет желания вычислять нужное t, легко убедиться в его существовании по соображениям непрерывности.)

Другие виды расстояний. Равносторонние множества становятся гораздо непонятнее, когда рассматриваются другие определения расстояний в $\mathbb{R}^d$.

Сначала, в качестве поучительного примера, рассмотрим метрику ℓ_∞ («эль-бесконечность»), когда расстояние между двумя точками $\mathbf{x}, \mathbf{y} \in \mathbb{R}^d$ определяется как $\|\mathbf{x} - \mathbf{y}\|_\infty = \max\{|x_i - y_i| : i = 1, 2, \ldots, d\}$. Тогда «куб» $\{0, 1\}^d$ является равносторонним множеством из 2^d то-

чек! (Для метрики ℓ_∞ в $\mathbb{R}^d$ этот случай оказывается максимально возможным, но в эту тему мы не хотим здесь углубляться.)

На самом деле мы намерены сосредоточиться на **метрике $\boldsymbol{\ell_1}$**, имеющей вид

$$\|\mathbf{x}-\mathbf{y}\|_1 = |x_1-y_1|+|x_2-y_2|+\ldots+|x_d-y_d|.$$

Вот пример равностороннего множества из $2d$ точек для этого случая: $\{\mathbf{e}_1, -\mathbf{e}_1, \mathbf{e}_2, -\mathbf{e}_2, \ldots, \mathbf{e}_d, -\mathbf{e}_d\}$. Согласно популярному предположению это максимум того, что можно получить, но примерно до 2001 г. не было известно никакой верхней оценки, кроме (экспоненциальной!) 2^d-1.

Приведём остроумное доказательство полиномиальной верхней оценки $O(d^4)$. Доказательство наилучшей на данный момент верхней оценки $O(d\log d)$ использует ряд дополнительных идей и гораздо более технично.

Теорема. *Для любого $d\geqslant 1$ любое множество в $\mathbb{R}^d$, равностороннее в метрике ℓ_1, содержит не больше $100d^4$ точек.*

Изложенное ниже доказательство содержит интересный поворот: чтобы найти оценку для *строго* равносторонних множеств при «неудобном» расстоянии ℓ_1, мы используем множества, *приблизительно* равносторонние при «удобном» евклидовом расстоянии. Вот инструмент, который для этого потребуется.

Лемма (о приближённом вложении)**.** *Для каждых двух натуральных чисел d, q существует такое отображение*

$$f_{d,q}\colon [0;1]^d \to \mathbb{R}^{dq},$$

что для любых $\mathbf{x}, \mathbf{y}\in[0;1]^d$ выполнены неравенства

$$\|\mathbf{x}-\mathbf{y}\|_1 - \frac{2d}{q} \leqslant \frac{1}{q}\|f_{d,q}(\mathbf{x})-f_{d,q}(\mathbf{y})\|^2 \leqslant \|\mathbf{x}-\mathbf{y}\|_1 + \frac{2d}{q}.$$

Подчеркнём, что в терминальном пространстве $\mathbb{R}^{dq}$ мы берём *квадрат* евклидова расстояния. Если вместо этого потребовать, чтобы ℓ_1-расстояние $\|\mathbf{x}-\mathbf{y}\|_1$ было достаточно близко к евклидову расстоянию между образами для всех $\mathbf{x}, \mathbf{y}$, то задача становится неразрешимой.

Наше доказательство леммы довольно бесхитростно. Более изощрёнными методами можно значительно понизить размерность терминального пространства (что приводит к улучшению оценки $O(d^4)$ в теореме).

Доказательство леммы. Сначала рассмотрим случай $d=1$. Для $x\in[0;1]$ определим $f_{1,q}(x)$ как вектор размерности q из нулей и единиц, начинающийся с $\lfloor qx\rfloor$ единиц, за которыми следуют $q-\lfloor qx\rfloor$ нулей. Тогда $\|f_{1,q}(x)-f_{1,q}(y)\|^2$ — количество позиций, где одна из величин $f_{1,q}(x)$, $f_{1,q}(y)$ равна 1, а другая 0. Это количество равно $\big|\lfloor qx\rfloor-\lfloor qy\rfloor\big|$ и отличается от $q|x-y|$ не больше чем на 2. Этим доказан случай $d=1$.

Для $d>1$ определим $f_{d,q}(\mathbf{x})$ как вектор размерности dq, составленный из $f_{1,q}(x_1)$, $f_{1,q}(x_2)$,..., $f_{1,q}(x_d)$. Нужная оценка очевидна из одномерного случая. □

Приближённо равносторонние множества. Если дано равностороннее множество в $\mathbb{R}^d$ с метрикой ℓ_1, то с помощью только что доказанной леммы мы получаем (при подходящих значениях параметров) приближённо равностороннее множество в *евклидовом* пространстве некоторой более высокой размерности. Покажем теперь, что такие приближённо равносторонние множества не могут быть слишком большими; вот здесь и выходит на сцену линейная алгебра. Доказательство основано на следующем результате, представляющем самостоятельный интерес.

Лемма о ранге. *Пусть A — вещественная симметрическая ненулевая $(n\times n)$-матрица. Тогда*

$$\operatorname{rank}(A)\geqslant\frac{\big(\sum\limits_{i=1}^{n}a_{ii}\big)^2}{\sum\limits_{i,j=1}^{n}a_{ij}^2}.$$

Доказательство леммы о ранге. Из линейной алгебры мы знаем, что матрица A из условия леммы имеет n вещественных собственных значений $\lambda_1,\lambda_2,\ldots,\lambda_n$. Если $\operatorname{rank}(A)=r$, то ровно r из λ_i отличны от нуля; можно считать, что $\lambda_i\neq0$ при $1\leqslant i\leqslant r$ и $\lambda_i=0$ при $i>r$.

Запишем неравенство Коши—Буняковского—Шварца

$$\Big(\sum_{i=1}^{r}x_iy_i\Big)^2\leqslant\Big(\sum_{i=1}^{r}x_i^2\Big)\Big(\sum_{i=1}^{r}y_i^2\Big)$$

для $x_i=\lambda_i$, $y_i=1$. Получаем $\Big(\sum\limits_{i=1}^{r}\lambda_i\Big)^2\leqslant r\sum\limits_{i=1}^{r}\lambda_i^2$. Разделив на $\sum\limits_{i=1}^{r}\lambda_i^2$, приходим к следующему неравенству для ранга в терминах соб-

ственных значений:

$$\operatorname{rank}(A) \geqslant \frac{\left(\sum\limits_{i=1}^{n} \lambda_i\right)^2}{\sum\limits_{i=1}^{n} \lambda_i^2}. \qquad (1)$$

(Фактически суммирование проведено вплоть до n, поскольку λ_{r+1}, …, λ_n равны 0.)

Последнее неравенство можно превратить в неравенство из леммы о ранге за три простых шага. Во-первых, сумма всех собственных значений матрицы A равна её *следу*, т. е. $\sum\limits_{i=1}^{n} \lambda_i = \sum\limits_{i=1}^{n} a_{ii}$ (стандартный факт из линейной алгебры). Это обеспечивает нужный числитель в формуле (1). Во-вторых, как можно вспомнить или непосредственно проверить, собственные значения матрицы A^2 равны $\lambda_1^2, \ldots, \lambda_n^2$, и потому $\sum\limits_{i=1}^{n} \lambda_i^2 = \operatorname{trace}(A^2)$. В-третьих, как нетрудно вычислить

$$\operatorname{trace}(A^2) = \sum_{i,j=1}^{n} a_{ij}^2.$$

Это приводит к нужному виду знаменатель. □

Следствие. *Пусть A — симметричная $(n \times n)$-матрица, причём $a_{ii} = 1$, $i = 1, 2, \ldots, n$, и $|a_{ij}| \leqslant \frac{1}{\sqrt{n}}$ для всех $i \neq j$. Тогда* $\operatorname{rank}(A) \geqslant \frac{n}{2}$. □

Предложение (о приближённо равносторонних множествах)**.** *Пусть $\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_n \in \mathbb{R}^d$ — такие точки, что при всех $i \neq j$ выполнены неравенства*

$$1 - \frac{1}{\sqrt{n}} \leqslant \|\mathbf{p}_i - \mathbf{p}_j\|^2 \leqslant 1 + \frac{1}{\sqrt{n}}.$$

Тогда $n \leqslant 2(d+2)$. (*Отметим, что ради технического удобства оценивается* квадрат *евклидова расстояния.*)

Доказательство предложения. Пусть A — матрица размера $n \times n$ с элементами $a_{ij} = 1 - \|\mathbf{p}_i - \mathbf{p}_j\|^2$. Из условий предложения сразу следует, что для A выполнено условие предыдущего следствия, поэтому $\operatorname{rank}(A) \geqslant \frac{n}{2}$.

Остаётся оценить $\operatorname{rank}(A)$ сверху в терминах размерности d. Здесь мы действуем как в миниатюре 15. При $i = 1, 2, \ldots, n$ пусть $f_i : \mathbb{R}^d \to \mathbb{R}$ — функция, заданная формулой $f_i(\mathbf{x}) = 1 - \|\mathbf{x} - \mathbf{p}_i\|^2$; таким образом, i-я строка матрицы A имеет вид $\big(f_i(\mathbf{p}_1), f_i(\mathbf{p}_2), \ldots, f_i(\mathbf{p}_n)\big)$.

Можно записать

$$f_i(\mathbf{x}) = 1 - \|\mathbf{x}\|^2 - \|\mathbf{p}_i\|^2 + 2(p_{i1}x_1 + p_{i2}x_2 + \ldots + p_{id}x_d),$$

где p_{ik} обозначает k-ю компоненту вектора $\mathbf{p}_i$. Тогда становится ясно, что каждое f_i является линейной комбинацией следующих $d+2$ функций: константы 1, функции $\mathbf{x} \mapsto \|\mathbf{x}\|^2$ и «координатных функций» $\mathbf{x} \mapsto x_k$, $k = 1, 2, \ldots, d$. Поэтому векторное пространство, натянутое на f_i, имеет размерность не выше $d+2$, и это размерность пространства строк матрицы A. Значит, $\operatorname{rank}(A) \leqslant d+2$, и предложение доказано. □

Доказательство теоремы. Предположим противное: пусть существует равностороннее множество в пространстве $\mathbb{R}^d$ с метрикой ℓ_1, содержащее не менее $100d^4$ точек. Удалив, если нужно, некоторые точки, можно считать, что точек ровно $n := 100d^4$.

Масштабируем множество так, чтобы расстояния между точками стали равными $\frac{1}{2}$, и сдвинем его так, чтобы одна из точек получила координаты $\left(\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2}\right)$. Тогда множество будет целиком содержаться в кубе $[0; 1]^d$.

Используем лемму о приближённом вложении при $q := 40d^3$. Применив к нашему множеству отображение $f_{d,q}$, получаем множество из n точек в $\mathbb{R}^{dq}$, в котором квадраты всех попарных евклидовых расстояний находятся между $\frac{q}{2} - 2d$ и $\frac{q}{2} + 2d$. Умножив на $\sqrt{\frac{2}{q}}$, получаем приближённо равностороннее множество, где квадраты евклидовых расстояний между точками находятся между $1 - \frac{4d}{q}$ и $1 + \frac{4d}{q}$. Поскольку $\frac{4d}{q} = \frac{1}{10d^2} = \frac{1}{\sqrt{n}}$, можно применить предложение о приближённо равносторонних множествах, согласно которому $n \leqslant 2(dq+2)$. Получили противоречие, поскольку $n = 100d^4$, но $2(dq+2) = 2(40d^4+2) < 100d^4$. Теорема доказана. □

Литература

Alon N., Pudlák P. Equilateral sets in l_p^n // Geometric and Functional Analysis. 2003. V. 13. P. 467—482.

Наше изложение с использованием приближённого вложения несколько другое.

Миниатюра 31

Дешёвый разрез с помощью собственных векторов

Во многих практических приложениях мы рассматриваем большой граф G и хотим отрезать часть вершин, удалив как можно меньше рёбер. В случае большого куска можно согласиться на удаление большего количества рёбер, чем в случае маленького, что схематически показано на рис. 40.

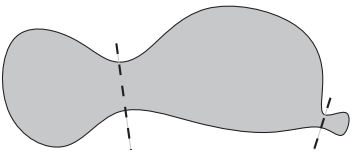


Рис. 40

Представим себе, что удаление одного ребра имеет единичную стоимость и мы хотим отрезать часть вершин, не более половины, уплатив наименьшую возможную цену *за одну вершину*.

Эта задача тесно связана с парадигмой *разделяй и властвуй* в разработке алгоритмов. Например, в таких областях, как компьютерная графика, системы автоматизированного проектирования, получение медицинских изображений, мы имеем дело с двумерной поверхностью, представленной в виде *треугольной сетки* (см. рис. 41).

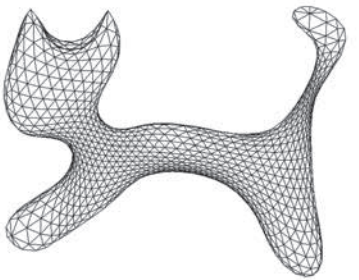


Рис. 41

Для различных вычислений часто требуется разделить большую сетку на более мелкие части, связанные между собой как можно меньше.

Более абстрактно: вершины графа G могут соответствовать неким объектам, рёбра — выражать их зависимости или взаимодействия, и мы опять хотим разделить задачу на меньшие подзадачи с малым количеством взаимосвязей.

Разреженное разрезание. Сформулируем задачу более строго. Пусть G — данный граф с множеством вершин V, $|V| = n$, и множеством рёбер E. Назовём разбиение множества V на два непустых подмножества A и $V \setminus A$ **разрезом** и обозначим через $E(A, V \setminus A)$ множество всех рёбер в G, связывающих вершину из A с вершиной из $V \setminus A$.

«Цену за вершину» при отрезании множества A можно в этом контексте определить как $\Phi(A, V \setminus A) := |E(A, V \setminus A)|/|A|$, считая, что $|A| \leqslant \frac{n}{2}$. Мы будем работать с другой, но тесно связанной величиной: назовём **плотностью** разреза $(A, V \setminus A)$ величину

$$\varphi(A, V \setminus A) := n \cdot \frac{|E(A, V \setminus A)|}{|A| \cdot |V \setminus A|}$$

(она в n раз больше отношения количеств рёбер, соединяющих A и $V \setminus A$ в графе G и в полном графе на множестве V). Поскольку $|A| \cdot |V \setminus A|$ находится между $\frac{1}{2}n|A|$ и $n|A|$ (мы снова считаем, что $|A| \leqslant \frac{n}{2}$), всегда выполнены неравенства $\Phi(A, V \setminus A) \leqslant \varphi(A, V \setminus A) \leqslant \leqslant 2\Phi(A, V \setminus A)$. Так что нет большой разницы, искать разрез, минимизирующий Φ или φ, и мы выберем последнее.

Итак, пусть φ_G обозначает наименьшую возможную плотность разреза в графе G. Мы хотим найти **самый разреженный разрез**, т. е. разрез плотности φ_G.

Известно, что эта задача вычислительно трудна (NP-полна), и для неё предложены различные приближённые алгоритмы. Один такой алгоритм, точнее класс алгоритмов, называется *спектральным разбиением* и использует собственные векторы некоторой матрицы, ассоциированной с данным графом. Он широко и успешно применяется на практике, а благодаря современным методам вычисления собственных значений он работает достаточно быстро даже в случае больших графов.

Прежде чем приступать к формулировке алгоритма, необходимо заметить следующее. В некоторых приложениях на самом деле

интересен не самый разреженный разрез, а *приближённо сбалансированный* разреженный разрез, т. е. отрезающий не меньше, скажем, трети всех вершин. Для этой цели можно использовать наш алгоритм итеративно: мы многократно отрезаем части, возможно и небольшие, пока не соберём хотя бы треть всех вершин. Можно показать, что итерирование хорошего алгоритма для отыскания самого разреженного разреза приводит к хорошему приближённо сбалансированному разрезу. Не будем углубляться в подробности, так как это отвлекло бы от основной темы.

Теперь начнём подготовку к построению алгоритма.

Матрица Лапласа. Для удобства занумеруем вершины графа G числами $1, 2, \ldots, n$. Определим **матрицу Лапласа** L графа G (она также использовалась в миниатюре 21) как $(n\times n)$-матрицу с элементами ℓ_{ij} вида

$$\ell_{ij} := \begin{cases} \deg(i) & \text{при } i = j, \\ -1 & \text{при } \{i,j\} \in E(G), \\ 0 & \text{в остальных случаях,} \end{cases}$$

где $\deg(i)$ — количество соседей (степень) вершины i в G.

Нам потребуется следующее тождество, выполненное для каждого $\mathbf{x}\in\mathbb{R}^n$:

$$\mathbf{x}^T L\mathbf{x} = \sum_{\{i,j\}\in E} (x_i - x_j)^2. \tag{1}$$

В самом деле,

$$\mathbf{x}^T L\mathbf{x} = \sum_{i,j=1}^{n} \ell_{ij} x_i x_j = \sum_{i=1}^{n} \deg(i) x_i^2 - 2 \sum_{\{i,j\}\in E} x_i x_j,$$

правая часть упрощается до $\sum\limits_{\{i,j\}\in E} (x_i - x_j)^2$, и мы получаем равенство (1).

Правая часть равенства (1) всегда неотрицательна, так что матрица L является положительно полуопределённой. Поэтому у неё n неотрицательных вещественных собственных значений, которые мы запишем в порядке неубывания как $\mu_1 \leqslant \mu_2 \leqslant \ldots \leqslant \mu_n$.

Поскольку сумма каждой строки в L равна 0, получаем $L\mathbf{1} = \mathbf{0}$ (где $\mathbf{1}$ — вектор из единиц), т. е. $\mu_1 = 0$ является собственным значением с собственным вектором $\mathbf{1}$. Ключевую роль в описанном далее алгоритме, как и в многих других теоретико-графовых задачах,

играет второе собственное значение μ_2 (иногда его называют *собственным значением Фидлера* графа G).

Спектральное разбиение. Алгоритм для отыскания разреженного разреза работает следующим образом.

1. Для данного графа G вычислить собственный вектор $\mathbf{u}$, принадлежащий второму (в порядке неубывания) собственному значению μ_2 матрицы Лапласа.

2. Упорядочить компоненты вектора $\mathbf{u}$ в порядке убывания. Пусть π — перестановка, для которой $u_{\pi(1)} \geqslant u_{\pi(2)} \geqslant \ldots \geqslant u_{\pi(n)}$.

3. Положить $A_k := \{\pi(1), \pi(2), \ldots, \pi(k)\}$. Среди разрезов

$$(A_k, V \setminus A_k), \quad k = 1, 2, \ldots, n-1,$$

выбрать имеющий наименьшую плотность.

Теорема. *Следующее верно для любого графа G*:

(i) $\varphi_G \geqslant \mu_2$;

(ii) *описанный алгоритм всегда находит разрез с плотностью не больше*

$$4\sqrt{d_{\max}\mu_2},$$

где $d_{\max}$ — наибольшая степень вершины в G; в частности, $\varphi_G \leqslant 4\sqrt{d_{\max}\mu_2}$.

Замечания. Эта теорема имеет фундаментальное значение, которое далеко не ограничивается алгоритмом спектрального разбиения. Например, она играет ключевую роль при построении экспандеров (расширяющих графов)[1].

Константу 4 в п. (ii) можно улучшить, проведя более тщательное рассуждение. Разница между верхней оценкой для φ_G из п. (i) и нижней оценкой из п. (ii) может быть большой, но обе оценки по существу неулучшаемы. А именно, для одних графов нижняя оценка близка к точной, а для других достигается верхняя.

Для планарных графов, в которых степень вершин ограничена константой, — например, для сетки-кошки на рис. 41 — известно, что $\mu_2 = O\left(\frac{1}{n}\right)$ (доказательство выходит за рамки этой книги), поэтому алгоритм спектрального разбиения всегда находит разрез

[1] Пункт (ii) часто называют *неравенством Чигера—Алона—Мильмана*, имея в виду, что неравенство Чигера является аналогичным «непрерывным» результатом в геометрии римановых многообразий.

плотности $O(n^{-1/2})$. Эта плотность — с точностью до постоянного множителя наименьшая возможная, для многих планарных графов (например, рассмотрим квадратную решётку). Аналогичные результаты известны для нескольких других классов графов.

Доказательство п. (i) теоремы. Будем называть вектор $\mathbf{x}\in\mathbb{R}^n$ **непостоянным**, если он не пропорционален вектору $\mathbf{1}$.

Для непостоянного $\mathbf{x}\in\mathbb{R}^n$ положим

$$Q(\mathbf{x}) := n\cdot\frac{\sum\limits_{\{i,j\}\in E}(x_i-x_j)^2}{\sum\limits_{1\leqslant i<j\leqslant n}(x_i-x_j)^2}.$$

Пусть $(A, V\setminus A)$ — разрез в графе G, а $\mathbf{c}_A$ — характеристический вектор множества A (его i-я компонента равна 1 при $i\in A$ и равна 0 в противном случае). Тогда $Q(\mathbf{c}_A)$ равно плотности разреза $(A, V\setminus A)$, так что φ_G равно минимуму $Q(\mathbf{x})$ по всем непостоянным векторам $\mathbf{x}\in\{0,1\}^n$.

Теперь покажем, что μ_2 равно минимуму $Q(\mathbf{x})$ по более широкому множеству векторов, а именно

$$\mu_2 = \min\{Q(\mathbf{x}) : \mathbf{x}\in\mathbb{R}^n \text{ непостоянен}\} \tag{2}$$

(в информатике в этом случае говорят, что μ_2 является *релаксацией* для φ_G). Разумеется, тогда $\varphi_G\geqslant\mu_2$.

Поскольку $Q(\mathbf{x}) = Q(\mathbf{x}+t\mathbf{1})$ для всех $t\in\mathbb{R}$, можно заменить множество (2) на

$$\mu_2 = \min\{Q(\mathbf{x}) : \mathbf{x}\in\mathbb{R}^n\setminus\{\mathbf{0}\},\ \langle\mathbf{x},\mathbf{1}\rangle = 0\}.$$

Утверждение. *Если* $\mathbf{x}$ *и* $\mathbf{1}$ *ортогональны, то знаменатель дроби* $Q(\mathbf{x})$ *равен* $n\|\mathbf{x}\|^2$.

Доказательство утверждения. Знаменатель дроби $Q(\mathbf{x})$ равен сумме величин $(x_i-x_j)^2$ по всем рёбрам полного графа на вершинах $\{1, 2, \ldots, n\}$. Его матрица Лапласа равна $nI_n - J_n$. Из тождества (1) для матрицы Лапласа тогда следует, что

$$\sum_{1\leqslant i<j\leqslant n}(x_i-x_j)^2 = \mathbf{x}^T(nI_n-J_n)\mathbf{x} = n\|\mathbf{x}\|^2,$$

так как $J_n\mathbf{x}=\mathbf{0}$ по предположению. Утверждение доказано. □

Таким образом, теперь можно заменить множество (2) на

$$\mu_2 = \min\bigl\{\mathbf{x}^T L\mathbf{x} : \|\mathbf{x}\| = 1,\ \langle\mathbf{1},\mathbf{x}\rangle = 0\bigr\}. \tag{3}$$

Но это стандартный факт из линейной алгебры (для частного случая) — *минимаксная характеризация собственных значений* (или *теорема Куранта—Фишера*). Его легко и проверить: разложим $\mathbf{x}$ по ортонормированному базису из собственных векторов матрицы L и соответственно выразим $\mathbf{x}^T L\mathbf{x}$; предоставим это читателю. Отметим лишь, что из доказательства следует также, что минимум в формуле (3) достигается на собственном векторе матрицы L, принадлежащем μ_2, — это будет полезно в дальнейшем. На этом завершается доказательство п. (i) теоремы. □

В доказательстве п. (ii) один из главных шагов — следующая

Лемма. *Пусть* $A_k = \{1, 2, \ldots, k\}$, *и пусть* α — *такое вещественное число, что каждый из разрезов* $(A_k, V \setminus A_k)$, $k = 1, 2, \ldots, n$, *имеет плотность не меньше* α. *Пусть* $\mathbf{z} \in \mathbb{R}^n$ — *такой вектор, что* $z_1 \geqslant z_2 \geqslant \ldots \ldots \geqslant z_n$. *Тогда*

$$\sum_{\{i,j\}\in E, i<j} (z_i - z_j) \geqslant \frac{\alpha}{n} \sum_{1\leqslant i<j\leqslant n} (z_i - z_j). \tag{4}$$

Доказательство леммы. В левой части неравенства (4) запишем каждое $z_i - z_j$ в виде

$$(z_i - z_{i+1}) + (z_{i+1} - z_{i+2}) + \ldots + (z_{j-1} - z_j).$$

Сколько раз слагаемое $z_k - z_{k+1}$ появляется в получившейся сумме? Ответ равен количеству таких рёбер $\{i, j\} \in E$, что $i \leqslant k < j$, т. е. равен $|E(A_k, V \setminus A_k)|$. Таким образом,

$$\sum_{\{i,j\}\in E, i<j} (z_i - z_j) = \sum_{k=1}^{n-1} (z_k - z_{k+1}) \cdot |E(A_k, V \setminus A_k)|.$$

Точно так же получаем $\sum\limits_{1\leqslant i<j\leqslant n} (z_i - z_j) = \sum\limits_{k=1}^{n-1} (z_k - z_{k+1}) |A_k| \cdot |V \setminus A_k|$. Осталось применить предположение о плотности: $|E(A_k, V \setminus A_k)| \geqslant \geqslant \frac{\alpha}{n} |A_k| \cdot |V \setminus A_k|$ при всех k. □

Доказательство п. (ii) теоремы. Ради простоты обозначений перенумеруем вершины графа G так, что $u_1 \geqslant u_2 \geqslant \ldots \geqslant u_n$, где $\mathbf{u}$ — собственный вектор из алгоритма (тогда $\pi(i) = i$ при всех i).

Пусть α — плотность разреза, полученного по алгоритму; мы хотим доказать, что $\alpha \leqslant 4\sqrt{d_{\max}\mu_2}$. При доказательстве п. (i) мы получили $\mu_2 = Q(\mathbf{u}) = \big(\sum\limits_{\{i,j\}\in E} (u_i - u_j)^2\big) / \|\mathbf{u}\|^2$, поэтому достаточно дока-

зать неравенство

$$\alpha\|\mathbf{u}\| \leqslant 4\Big(d_{\max}\sum_{\{i,j\}\in E}(u_i-u_j)^2\Big)^{1/2}. \tag{5}$$

Мы получим это неравенство из предыдущей леммы при подходящих $\mathbf{z}$, $z_1 \geqslant z_2 \geqslant \ldots \geqslant z_n$. Выбор правильного $\mathbf{z}$ — возможно, самый хитроумный шаг доказательства; он может выглядеть волшебством, но последующие выкладки покажут его смысл.

Для начала положим $\mathbf{v} := \mathbf{u} - u_{\lceil n/2\rceil}\mathbf{1}$, т. е. сдвинем все координаты так, что теперь $v_i \geqslant 0$ при $i \leqslant \frac{n}{2}$ и $v_i \leqslant 0$ при $i > \frac{n}{2}$. Имея в виду дальнейшее, отметим, что $\|\mathbf{v}\| \geqslant \|\mathbf{u}\|$ (поскольку $\mathbf{u}$ и $\mathbf{1}$ ортогональны).

Будем считать, что $\sum\limits_{i\colon 1\leqslant i\leqslant n/2} v_i^2 \geqslant \sum\limits_{i\colon n/2<i\leqslant n} v_i^2$; в противном случае нужно лишь использовать в доказательстве $-\mathbf{u}$ вместо $\mathbf{u}$ (что заведомо не влияет на результат работы алгоритма).

Теперь зададим $\mathbf{w}$, положив $w_i := \max(v_i, 0)$; таким образом, $\mathbf{w}$ начинается с первой половины вектора $\mathbf{v}$, за которой следуют нули. По предположению, сделанному в предыдущем абзаце, $\|\mathbf{w}\|^2 \geqslant \geqslant \frac{1}{2}\|\mathbf{v}\|^2 \geqslant \frac{1}{2}\|\mathbf{u}\|^2$.

Наконец, зададим $\mathbf{z}$, положив $z_i := w_i^2$, и подставим его в неравенство из леммы (для удобства переставив его части):

$$\frac{\alpha}{n}\sum_{1\leqslant i<j\leqslant n}(w_i^2-w_j^2) \leqslant \sum_{\{i,j\}\in E, i<j}(w_i^2-w_j^2). \tag{6}$$

Мы оценим обе части и в итоге получим (5).

Сначала займёмся правой частью (6). Разложив на множители: $w_i^2 - w_j^2 = (w_i - w_j)(w_i + w_j)$ и применив неравенство Коши—Буняковского—Шварца $\sum\limits_{i=1}^n a_i b_i \leqslant \big(\sum\limits_{i=1}^n a_i^2\big)^{1/2}\big(\sum\limits_{i=1}^n b_i^2\big)^{1/2}$ при $a_i = w_i - w_j$, $b_i = w_i + w_j$, получаем:

$$\begin{aligned}\sum_{\{i,j\}\in E, i<j}(w_i^2-w_j^2) &\leqslant \Big(\sum_{\{i,j\}\in E}(w_i-w_j)^2\Big)^{\frac12}\Big(\sum_{\{i,j\}\in E}(w_i+w_j)^2\Big)^{\frac12} \leqslant\\ &\leqslant \Big(\sum_{\{i,j\}\in E}(v_i-v_j)^2\Big)^{\frac12}\Big(\sum_{\{i,j\}\in E}2(w_i^2+w_j^2)\Big)^{\frac12} \leqslant\\ &\leqslant \Big(\sum_{\{i,j\}\in E}(u_i-u_j)^2\Big)^{\frac12}\sqrt{2d_{\max}}\,\|\mathbf{w}\|.\end{aligned}$$

Остаётся разобраться с левой частью (6), что совсем просто:

$$\sum_{1\leqslant i<j\leqslant n}(w_i^2-w_j^2)\geqslant\sum_{1\leqslant i\leqslant n/2}\sum_{n/2<j\leqslant n}(w_i^2-w_j^2)=$$
$$=\sum_{1\leqslant i\leqslant n/2}\sum_{n/2<j\leqslant n}w_i^2\geqslant\frac{n}{2}\|\mathbf{w}\|^2.$$

Соединив это с неравенством (6), вышеприведённой оценкой для его правой части и неравенством $\|\mathbf{w}\|\geqslant\dfrac{\|\mathbf{u}\|}{\sqrt{2}}$, выведенным раньше, получаем (5). Пункт (ii) теоремы доказан. □

Литература

Непрерывный аналог теоремы получен в работе

Cheeger J. A lower bound for the smallest eigenvalue of the Laplacian // Problems in analysis (Papers dedicated to Salomon Bochner, 1969). Princeton, NJ: Princeton Univ. Press, 1970. P. 195—199.

Дискретный вариант доказан в статьях

Alon N., *Milman V. D.* λ_1, isoperimetric inequalities for graphs, and superconcentrators // J. Combin. Theory. Ser. B. 1985. V. 38, № 1. P. 73—88,

и

Alon N. Eigenvalues and expanders // Combinatorica. 1986. V. 6, № 2. P. 83—96

и независимо в статье

Dodziuk J. Difference equations, isoperimetric inequality and transience of certain random walks // Trans. Amer. Math. Soc. 1984. V. 284, № 2. P. 787—794.

Несколько иное доказательство пункта (ii) теоремы можно найти, например, в превосходном обзоре

Hoory S., *Linial N.*, *Wigderson A.* Expander graphs and their applications // Bull. Amer. Math. Soc. (N.S.). V.2006. 43, № 4. P. 439—561.

Оно короче, но на мой взгляд выглядит ещё чуть «волшебнее», чем приведённое выше. Несколько другой интересный подход, когда проводится анализ некоторого рандомизированного алгоритма, предложен в работе

Trevisan L. Max cut and the smallest eigenvalue // SIAM Journal on Computing. 2012. V. 41. P. 1769—1786.

Результат о втором собственном значении для планарных графов взят из статьи

Spielman D. A., *Teng S.-H.* Spectral partitioning works: planar graphs and finite element meshes // Linear Algebra Appl. 2007. V. 421, № 2. P. 284—305.

Обобщение и новое доказательство дано в работе

Biswal P., *Lee J. R.*, *Rao S.* Eigenvalue bounds, spectral partitioning, and metrical deformations via flows // J. ACM. 2010. V. 57, № 3. Art. 13, 23.

Приближённые алгоритмы построения разреженного разреза составляют область активных исследований.

Миниатюра 32

Вращение куба

Вначале сформулируем две красивые геометрические теоремы. Поскольку они потребуются лишь как мотивировка, мы не будем рассматривать их доказательства, в которых требуются методы алгебраической топологии. Пусть

$$S^{n-1} = \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\| = 1\}$$

— единичная сфера в пространстве $\mathbb{R}^n$, где

$$\|\mathbf{x}\| = \sqrt{x_1^2 + x_2^2 + \ldots + x_n^2}$$

обозначает евклидову норму. Например, S^2 — обычная двумерная единичная сфера в трёхмерном пространстве.

(T1) *Для каждой непрерывной функции* $f : S^2 \to \mathbb{R}$ *существуют такие три взаимно ортогональных единичных вектора* $\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3$, *что* $f(\mathbf{p}_1) = f(\mathbf{p}_2) = f(\mathbf{p}_3)$.

(T2) *Пусть* $\alpha \in (0; 2]$, *а* $f : S^{n-1} \to \mathbb{R}^{n-1}$ *— произвольное непрерывное отображение. Тогда существуют две точки* $\mathbf{p}, \mathbf{q} \in S^n$ *на евклидовом расстоянии* α *друг от друга, для которых* $f(\mathbf{p}) = f(\mathbf{q})$. *Наглядное описание: в каждый данный момент на поверхности Земли существуют два места с одинаковой температурой и одинаковым атмосферным давлением на расстоянии ровно* 1234 *км друг от друга.*

Вероятно, теорема (T2) побудила Бронислава Кнастера поставить в 1947 г. следующий вопрос.

Вопрос Кнастера. *Верно ли, что для любого непрерывного отображения* $f : S^{n-1} \to \mathbb{R}^m$, *где* $n - 1 \geqslant m \geqslant 1$, *и любого множества* K *из* $n - m + 1$ *точек на сфере* S^{n-1} *существует вращение* ρ *пространства* $\mathbb{R}^n$ *вокруг начала координат, при котором во всех точках повёрнутого множества* ρK *значение* f *одинаково*?

Легко видеть, что положительный ответ на вопрос Кнастера при всех m, n включает теоремы (T1) и (T2) как частные случаи. Например, вторая теорема относится в точности к случаю $m = n - 1$ в вопросе Кнастера.

Однако утверждение из вопроса Кнастера выполняется, к сожалению, *не* при всех n, m, как было обнаружено в 1980-х годах. На самом деле оно *почти никогда* не выполняется: к настоящему моменту известны контрпримеры для всех таких n и m, что $n-1>m\geqslant 2$, а также когда $m=1$ и n достаточно велико[1].

Здесь мы рассмотрим контрпример для последнего из упомянутых случаев, а именно для $m=1$ (и подходящего большого n). Этот контрпример был найден лишь в 2003 г., когда уже были разобраны почти все остальные случаи.

Теорема. *Существуют целое n, непрерывная функция*

$$f\colon S^{n-1}\to\mathbb{R}$$

и множество $K\subset S^{n-1}$ из n точек такие, что для любого вращения ρ пространства $\mathbb{R}^n$ вокруг начала координат функция f принимает на ρK не менее двух различных значений.

Функция f в данном случае очень проста, а именно

$$f(\mathbf{x})=\|\mathbf{x}\|_\infty:=\max\{|x_1|,|x_2|,\ldots,|x_n|\}.$$

Сложность состоит в построении множества K и доказательстве нужного свойства.

Геометрические наводящие соображения, на самом деле не обязательные. Ясно, что максимум функции f на S^{n-1} равен 1 и достигается в точках $\pm\mathbf{e}_1,\ldots,\pm\mathbf{e}_n$. Приложив небольшие усилия, находим, что минимум функции f на S^{n-1} равен $n^{-1/2}$ и достигается в точках вида $(\pm n^{-1/2},\pm n^{-1/2},\ldots,\pm n^{-1/2})$.

Теперь рассмотрим функцию $f(\mathbf{x})=\|\mathbf{x}\|_\infty$ на всём $\mathbb{R}^n$. Тогда множество $\{\mathbf{x}\in\mathbb{R}^n\colon\|\mathbf{x}\|_\infty=1\}$ — поверхность единичного куба $[-1,1]^n$. Более общо, множество уровня $\{\mathbf{x}\in\mathbb{R}^n\colon\|\mathbf{x}\|_\infty=t\}$ — поверхность растянутого единичного куба $[-t,t]^n$. Итак, если K — некоторое множество на S^{n-1}, то найти такое вращение ρ, что f постоянна на ρK, — значит найти коэффициент растяжения t и вращение растянутого единичного куба $[-t,t]^n$ такие, что всё K лежит на поверхности куба, полученного при вращении (см. рис. 42).

В доказательстве теоремы в качестве K взято дизъюнктное объединение двух множеств K_1 и K_2. Они строятся таким образом, что если K_1 лежит на поверхности полученного куба, то коэффициент

[1] Однако вопрос сохраняет силу: остаётся понять, для каких множеств K утверждение выполняется. Этот вопрос очень интересен и весьма далёк от разрешения.

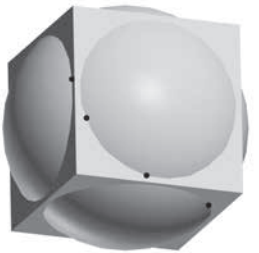


Рис. 42

растяжения t должен быть *большим* (геометрически это означает, что точки из K_1 должны располагаться далеко от углов куба), тогда как для K_2 коэффициент растяжения должен быть *малым* (точки из K_2 должны быть близки к углам куба). Поэтому K_1 и K_2 не могут одновременно лежать на поверхности одного и того же растянутого и повёрнутого куба.

Предварительные шаги. В теореме рассматривается множество точек K на $(n-1)$-мерной единичной сфере, а также результаты его вращений ρK. В доказательстве будет удобнее работать с множеством $\overline{K}$ на единичной сфере S^{d-1} подходящей меньшей размерности. Тогда вместо вращений мы рассмотрим **изометрии** $\varphi\colon \mathbb{R}^d \to \mathbb{R}^n$, т. е. линейные отображения, для которых $\|\varphi(\mathbf{x})\| = \|\mathbf{x}\|$ при всех $\mathbf{x}\in\mathbb{R}^d$. Если φ_0 — такая изометрия, то $K := \varphi_0(\overline{K})$ — некоторое множество точек на S^{n-1}, а множества $\varphi(\overline{K})$ для всех остальных изометрий $\varphi\colon \mathbb{R}^d \to \mathbb{R}^n$ — это в точности результаты всевозможных поворотов множества K (а также их зеркальные отражения — но для доказательства теоремы зеркальные отражения не будут нужны).

Нам потребуется ещё одно определение. Пусть $X \subseteq \mathbb{R}^n$ — некоторое множество, $\delta > 0$ — вещественное число. Множество $N \subseteq X$ называется **δ-плотным в X**, если для каждого $\mathbf{x}\in X$ существует такое $\mathbf{y}\in N$, что $\|\mathbf{x}-\mathbf{y}\| \leqslant \delta$.

Лемма К1. (i) *Пусть $\varphi\colon \mathbb{R}^d \to \mathbb{R}^n$ — некоторая изометрия. Тогда существует $\mathbf{x}\in S^{d-1}$, для которого $\|\varphi(\mathbf{x})\|_\infty \geqslant \sqrt{\frac{d}{n}}$.*

(ii) *Пусть при этом множество $\overline{K}_1 \subset S^{d-1}$ является $\frac{1}{2}$-плотным на S^{d-1}. Тогда существует $\overline{\mathbf{p}}\in\overline{K}_1$, для которого $\|\varphi(\overline{\mathbf{p}})\|_\infty \geqslant \frac{1}{2}\sqrt{\frac{d}{n}}$.*

Доказательство леммы К1. Начнём с пункта (i). Пусть A — матрица изометрии φ в стандартном базисе, т. е. i-м столбцом матрицы A является вектор $\varphi(\mathbf{e}_i)\in\mathbb{R}^n$, $i=1, 2, \ldots, d$. Поскольку φ сохраняет евклидову норму, столбцы матрицы A — единичные векторы в $\mathbb{R}^n$, и потому

$$\sum_{i=1}^{n}\sum_{j=1}^{d} a_{ij}^2 = d. \tag{1}$$

Пусть $\mathbf{a}_i\in\mathbb{R}^d$ обозначает i-ю *строку* матрицы A. Если $\mathbf{x}\in\mathbb{R}^d$, то i-я компонента в $\varphi(\mathbf{x})$ равна скалярному произведению $\langle\mathbf{a}_i, \mathbf{x}\rangle$, а значит, $\|\varphi(\mathbf{x})\|_\infty = \max\{|\langle\mathbf{a}_i, \mathbf{x}\rangle| : i=1, 2, \ldots, n\}$.

Далее, равенство (1) означает, что $\sum\limits_{i=1}^{n}\|\mathbf{a}_i\|^2 = d$, поэтому найдётся i_0, для которого $\|\mathbf{a}_{i_0}\| \geqslant \sqrt{\frac{d}{n}}$. Положив $\mathbf{x} := \mathbf{a}_{i_0}/\|\mathbf{a}_{i_0}\|$, получаем $\|\varphi(\mathbf{x})\|_\infty \geqslant \langle\mathbf{a}_{i_0}, \mathbf{x}\rangle = \|\mathbf{a}_{i_0}\| \geqslant \sqrt{\frac{d}{n}}$, чем доказан п. (i).

Теперь перейдём к п. (ii), который на самом деле и потребуется в дальнейшем. Доказательство окажется чуть сложнее, чем могло показаться на первый взгляд.

В условиях п. (ii) положим $M := \sup\{\|\varphi(\mathbf{x})\|_\infty : \mathbf{x}\in S^{d-1}\}$, и пусть $\mathbf{x}_0\in S^{d-1}$ — точка, в которой достигается это значение[1]. В силу п. (i) получаем $M \geqslant \sqrt{\frac{d}{n}}$.

Поскольку множество $\overline{K}_1$ является $\frac{1}{2}$-плотным, найдётся точка $\overline{\mathbf{p}}\in\overline{K}_1$, для которой $\|\mathbf{x}_0 - \overline{\mathbf{p}}\| \leqslant \frac{1}{2}$. Если случайно окажется, что $\overline{\mathbf{p}} = \mathbf{x}_0$, то результат получен, поэтому можно считать, что $\overline{\mathbf{p}} \neq \mathbf{x}_0$. Пусть

$$\mathbf{v} := (\mathbf{x}_0 - \overline{\mathbf{p}})/\|\mathbf{x}_0 - \overline{\mathbf{p}}\| \in S^{d-1}$$

— единичный вектор в направлении $\mathbf{x}_0 - \overline{\mathbf{p}}$. Тогда $\|\varphi(\mathbf{v})\|_\infty \leqslant M$ по выбору M, и потому $\|\varphi(\mathbf{x}_0 - \overline{\mathbf{p}})\|_\infty \leqslant \frac{1}{2}M$. Применяя неравенство треугольника для нормы $\|.\|_\infty$, получаем

$$\|\varphi(\overline{\mathbf{p}})\|_\infty \geqslant \|\varphi(\mathbf{x}_0)\|_\infty - \|\varphi(\mathbf{x}_0 - \overline{\mathbf{p}})\|_\infty \geqslant M - \frac{1}{2}M = \frac{1}{2}M \geqslant \frac{1}{2}\sqrt{\frac{d}{n}}.$$

Пункт (ii) доказан. □

[1] Супремум достигается, поскольку S^{d-1} — компакт. Читатели, не владеющие понятием компактности, могут рассмотреть точку $\mathbf{x}_0$, для которой, скажем, $\|\varphi(\mathbf{x}_0)\|_\infty \geqslant 0{,}99M$, что заведомо возможно. Тогда константы в доказательстве следует немного изменить.

Лемма К2. *Пусть $\overline{K}_2$ — множество из m различных точек единичной окружности $S^1 \subset \mathbb{R}^2$. Если для некоторого числа t существует такая изометрия $\varphi\colon \mathbb{R}^2 \to \mathbb{R}^n$, что $\|\varphi(\overline{\mathbf{p}})\|_\infty = t$ при всех $\overline{\mathbf{p}} \in \overline{K}_2$, то $t \leqslant \sqrt{8/m}$.*

Доказательство леммы К2. Начнём так же, как при доказательстве леммы К1, положив на этот раз $d = 2$: A является матрицей отображения φ, а $\mathbf{a}_i \in \mathbb{R}^2$ — её i-я строка. Согласно равенству (1) имеем $\sum\limits_{i=1}^{n} \|\mathbf{a}_i\|^2 = 2$. Мы хотим получить нижнюю оценку для левой части в терминах m и t.

Поскольку i-я координата вектора $\varphi(\overline{\mathbf{p}})$ равна $\langle \mathbf{a}_i, \overline{\mathbf{p}} \rangle$, условие

$$\|\varphi(\overline{\mathbf{p}})\|_\infty = t$$

для всех $\overline{\mathbf{p}} \in \overline{K}_2$ можно переформулировать следующим образом.

(С1) Для каждого $\overline{\mathbf{p}} \in \overline{K}_2$ существует $i = i(\overline{\mathbf{p}})$, для которого $|\langle \mathbf{a}_i, \overline{\mathbf{p}} \rangle| = t$.

(С2) При всех $\overline{\mathbf{p}} \in \overline{K}_2$ и всех i выполнено неравенство $|\langle \mathbf{a}_i, \overline{\mathbf{p}} \rangle| \leqslant t$.

Из условия (С1) вытекает, что

$$\text{если } i = i(\overline{p}),\ \overline{\mathbf{p}} \in \overline{K}_2, \quad \text{то } \|\mathbf{a}_i\| \geqslant t. \tag{2}$$

Действительно, $\overline{\mathbf{p}}$ — единичный вектор, поэтому $|\langle \mathbf{y}, \overline{\mathbf{p}} \rangle| \leqslant \|\mathbf{y}\|$ при всех $\mathbf{y}$ и из равенства $|\langle \mathbf{a}_i, \overline{\mathbf{p}} \rangle| = t$ следует, что $\|\mathbf{a}_i\| \geqslant t$.

Остаётся показать, что существует *много* различных таких i, что $i = i(\overline{\mathbf{p}})$ для некоторого $\overline{\mathbf{p}} \in \overline{K}_2$. Воспользуемся тем, что каждое данное i может служить в качестве $i(\overline{\mathbf{p}})$ не более чем для четырёх различных точек $\overline{\mathbf{p}}$. Это можно увидеть из рис. 43.

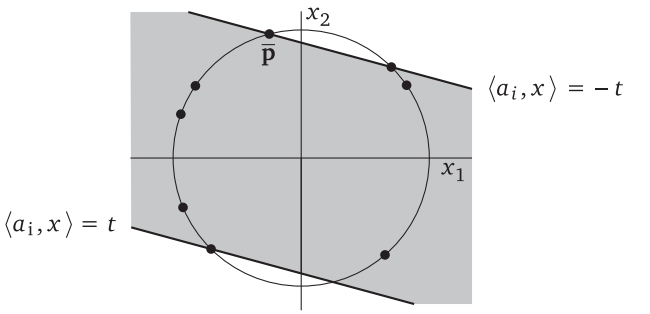


Рис. 43

Условие $i = i(\overline{\mathbf{p}})$ означает, что точка $\overline{\mathbf{p}}$ лежит на одной из прямых $\{\mathbf{x} \in \mathbb{R}^2\colon \langle \mathbf{a}_i, \mathbf{x} \rangle = t\}$ и $\{\mathbf{x} \in \mathbb{R}^2\colon \langle \mathbf{a}_i, \mathbf{x} \rangle = -t\}$, а из условия (С2) следует,

что все точки из $\overline{K}_2$ лежат в полосе между этими двумя параллельными прямыми. Тогда граница такой полосы может содержать не больше четырёх точек из $\overline{K}_2$ (в действительности одна, если $\overline{K}_2$ расположено достаточно общим образом).

Следовательно, среди $\mathbf{a}_i$ имеется не менее $\frac{m}{4}$ различных векторов с евклидовой нормой не меньше t, и потому $\sum_{i=1}^{n} \|\mathbf{a}_i\|^2 \geqslant \frac{t^2 m}{4}$. Так как мы уже знаем, что левая часть равна 2, получаем утверждение леммы K2. □

Два способа построения δ-плотных множеств. Последняя недостающая компонента доказательства теоремы — способ построения не слишком большого $\frac{1}{2}$-плотного множества $\overline{K}_1$ на сфере S^{d-1}, как в лемме K1(ii). Точнее, достаточно убедиться, что для любого $d \geqslant 1$ существует такое $\overline{K}_1$, имеющее размер не больше $g(d)$ для подходящей функции g.

Это хорошо известный геометрический факт. Один несколько неуклюжий, но быстрый способ его доказательства исходит из того, что целочисленная решётка $\mathbb{Z}^d$ является $\sqrt{d}$-плотной в $\mathbb{R}^d$ (на самом деле $\frac{1}{2}\sqrt{d}$-плотной). Растянув её в $\frac{1}{4\sqrt{d}}$ раз и взяв пересечение с кубом $[-1, 1]^d$, получим в этом кубе $\frac{1}{4}$-плотное множество N_0 размера не больше $(8\sqrt{d}+1)^d$. Затем для каждой точки $\mathbf{x} \in N_0$ на расстоянии не больше $\frac{1}{4}$ от S^{d-1} выберем точку $\mathbf{y} \in S^{d-1}$ на расстоянии не больше $\frac{1}{4}$ от $\mathbf{x}$, и пусть $N \subset S^{d-1}$ состоит из всех таких $\mathbf{y}$. Нетрудно проверить, что N является $\frac{1}{2}$-плотным на S^{d-1}. Отсюда получаем для $g(d)$ порядок $d^{O(d)}$.

Другое доказательство, «из учебника», использует «жадный» алгоритм и соображения объёма. Выберем первую точку $\mathbf{p}_1$ на сфере S^{d-1} произвольно. Когда уже выбраны $\mathbf{p}_1, \ldots, \mathbf{p}_{i-1}$, выберем $\mathbf{p}_i$ на S^{d-1} на расстоянии не меньше $\frac{1}{2}$ от $\mathbf{p}_1, \ldots, \mathbf{p}_{i-1}$. Этот процесс останавливается, когда нельзя выбрать следующую точку, т. е. получилось $\frac{1}{2}$-плотное множество. Чтобы оценить количество m точек, полученных таким способом, заметим, что все шары радиуса $\frac{1}{4}$ с центром $\mathbf{p}_i$ не пересекаются и содержатся в шаре радиуса $\frac{5}{4}$ с центром $\mathbf{0}$. Таким образом, суммарный объём маленьких шаров не превосходит

объёма большого шара, откуда получаем $m \leqslant 5^d$. Эта оценка лучше, чем при рассуждении в терминах решёток.

Доказательство теоремы. Выберем чётное $n \geqslant 2g(100)$. Пусть множество $\overline{K}_1$ размера не больше $\frac{n}{2}$ является $\frac{1}{2}$-плотным на S^{99}, и пусть $\overline{K}_2$ — множество из $\frac{n}{2}$ точек на S^1. Положим $K := K_1 \cup K_2$, где $K_1, K_2 \subset S^{n-1}$ — образы множеств $\overline{K}_1$ и $\overline{K}_2$ соответственно при изометриях.

Лемма K1(ii) показывает, что для любого вращения ρ существует такая точка $\mathbf{p} \in \rho K_1$, что $\|\mathbf{p}\|_\infty \geqslant \frac{1}{2}\sqrt{\frac{100}{n}} > 4n^{-1/2}$. С другой стороны, если вращение ρ таково, что $\|\mathbf{p}\|_\infty$ равно одному и тому же t для всех $\mathbf{p} \in \rho K_2$, то $t \leqslant \sqrt{16/n} = 4n^{-1/2}$ по лемме K2. Поэтому $K = K_1 \cup K_2$ нельзя повернуть так, чтобы все его точки имели одну и ту же норму $\|.\|_\infty$. □

Литература

Kashin B. S., Szarek S. J. The Knaster problem and the geometry of high-dimensional cubes // C. R. Acad. Sci. Paris, 2003. V. 336. P. 931—936.

Теорема (T2) обобщает широко известную теорему Борсука—Улама и доказана в работе

Hopf H. Eine Verallgemeinerung bekannter Abbildungs- und Überdeckungssätze // Portugaliae Math. 1944. V. 4. P. 129—139.

Теорема (T1) взята из заметки

Kakutani S. A proof that there exists a circumscribing cube around any bounded closed convex set in $\mathbb{R}^3$ // Ann. Math. 1942. V. 43. P. 739—741.

Это частный случай теоремы Ямабе и Юдзобо, согласно которой если $m = 1$, а K — конфигурация из n попарно ортогональных векторов на S^{n-1}, то вопрос Кнастера имеет положительный ответ.

Миниатюра 33

Пары множеств и внешние произведения

Докажем ещё одну теорему о свойствах пересечений множеств.

Теорема. *Пусть* $A_1, A_2, \ldots, A_n$ *— множества из* k *элементов,* $B_1, B_2, \ldots, B_n$ *— множества из* ℓ *элементов, и пусть*

(i) $A_i \cap B_i = \varnothing$ *при всех* $i = 1, 2, \ldots, n$,

(ii) $A_i \cap B_j \neq \varnothing$ *при условии* $1 \leqslant i < j \leqslant n$.

Тогда $n \leqslant \binom{k+\ell}{k}$.

Легко понять, откуда появляется $\binom{k+\ell}{k}$: пусть

$$X := \{1, 2, \ldots, k+\ell\},$$

список $A_1, A_2, \ldots, A_n$ состоит из всех k-элементных подмножеств в X, и пусть $B_i := X \setminus A_i$ при каждом i. Тогда A_i и B_i удовлетворяют условиям теоремы и $n = \binom{k+\ell}{k}$.

Может показаться неожиданным, что нельзя построить больше множеств, удовлетворяющих условиям (i) и (ii), даже если использовать гораздо большее основное множество (заметим, что теорема не накладывает ограничений на количество элементов в объединении множеств A_i и B_i; она ограничивает лишь их собственный размер и характер их пересечений).

Сформулированная теорема и подобные ей применялись при доказательстве многих интересных результатов в теории графов и гиперграфов, комбинаторной геометрии и теоретической информатике; говорят даже о *методе пар множеств*. Однако мы не будем обсуждать эти приложения. Мы включили эту теорему в основном из-за метода её доказательства, в котором затрагивается замечательный математический объект — внешняя алгебра векторного пространства.

Этп теорема известна в литературе как **несимметричная теорема Боллобаша**. Боллобаш вначале доказал более слабый (симметричный) вариант, где условие (ii) усилено до следующего:

(ii′) $A_i \cap B_j \neq \varnothing$ при всех $i, j = 1, 2, \ldots, n$, $i \neq j$.

У этого варианта есть короткое вероятностное доказательство (или, если угодно, доказательство двойным подсчётом). Однако для несимметричного варианта известны лишь линейно-алгебраические доказательства. Одно из них использует полиномиальный метод (который мы встречали в различных видах в миниатюрах 15, 16, 17), а другое изложенное вслед за первым служит простым примером ещё одного мощного метода.

Начнём с простого утверждения о существовании сколь угодно большого множества векторов «в общем положении».

Утверждение. *Для любого $d \geqslant 1$ и любого $m \geqslant 1$ существуют такие векторы $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m \in \mathbb{R}^d$, что среди них любые d или меньше векторов линейно независимы.*

Доказательство утверждения. Произвольно выберем m различных ненулевых вещественных чисел $t_1, t_2, \ldots, t_m$ и положим

$$\mathbf{v}_i := (t_i, t_i^2, \ldots, t_i^d)$$

(это точки на так называемой **кривой моментов** в $\mathbb{R}^d$).

Поскольку эта конструкция симметрична, достаточно проверить линейную независимость векторов $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_d$ (мы считаем, что $m \geqslant d$, так как иначе результат тривиален). Так что положим

$$\sum_{j=1}^{d} \alpha_j \mathbf{v}_j = \mathbf{0}.$$

Тогда

$$\sum_{j=1}^{d} \alpha_j t_i^j = 0 \quad \text{при всех } i,$$

т. е. $t_1, \ldots, t_d$ являются корнями многочлена

$$p(x) := \alpha_d x^d + \alpha_{d-1} x^{d-1} + \ldots + \alpha_1 x.$$

Но 0 также является его корнем, так что всего получается $d+1$ различных корней, а так как многочлен $p(x)$ имеет степень не выше d, он тождественно равен нулю. Значит, $\alpha_1 = \alpha_2 = \ldots = \alpha_d = 0$.

Можно также доказать линейную независимость векторов $\mathbf{v}_i$ с помощью определителя Вандермонда (обычно он вычисляется во вводных курсах линейной алгебры).

Ещё одно доказательство легко проводится по индукции, если поверить, что $\mathbb{R}^d$ не является объединением конечного множества $(d-1)$-мерных линейных подпространств. (Но строгое обоснование

этого факта, пожалуй, не проще, чем доказательство, приведённое выше.) □

О перестановках и знаках. Напомним, что знак перестановки

$$\pi\colon \{1, 2, \ldots, d\} \to \{1, 2, \ldots, d\}$$

можно определить как $\operatorname{sgn}(\pi) = (-1)^{\operatorname{inv}(\pi)}$, где $\operatorname{inv}(\pi) = |\{(i, j)\colon 1 \leqslant i < j \leqslant d \text{ и } \pi(i) > \pi(j)\}|$ — количество **инверсий** в перестановке π.

Пусть d — фиксированное целое число, $\mathbf{s} = (s_1, s_2, \ldots, s_k)$ — последовательность целых чисел из множества $\{1, 2, \ldots, d\}$. Определим знак последовательности $\mathbf{s}$, как выше:

$$\operatorname{sgn}(\mathbf{s}) := \begin{cases} (-1)^{\operatorname{inv}(\mathbf{s})}, & \text{если все числа в } \mathbf{s} \text{ различны,} \\ 0 & \text{в противном случае,} \end{cases}$$

где $\operatorname{inv}(\mathbf{s}) = |\{(i, j)\colon 1 \leqslant i < j \leqslant k \text{ и } s_i > s_j\}|$.

Если рассматривать перестановку π как последовательность

$$(\pi(1), \ldots, \pi(d)),$$

то оба определения знака, разумеется, совпадают.

Внешняя алгебра конечномерного векторного пространства. В 1844 г. Герман Грассман, школьный учитель в Штеттине (в то время — город в Пруссии, затем в Германии, а ныне в Польше под названием Щецин), опубликовал книгу, предложив новое алгебраическое обоснование геометрии. Построив основы линейной алгебры более-менее так, как мы знаем их сегодня, он ввёл понятие «внешнего произведения» векторов, чтобы сделать возможным унифицированное бескоординатное рассмотрение длин, площадей и объёмов. Его революционные математические открытия не были оценены при его жизни (он стал известен как лингвист), но позже они были дополнены и частично переоткрыты другими. Они принадлежат к числу важнейших основ современной математики и имеют много приложений, например, в дифференциальной геометрии, алгебраической геометрии и физике.

Здесь мы построим **внешнюю алгебру** (другое название — **грассманова алгебра**) конечномерного пространства минимальными средствами (не самым концептуальным образом), проверяя лишь свойства, нужные для доказательства сформулированной выше теоремы.

Предложение. *Пусть V — векторное пространство*[1] *размерности d. Тогда существуют счётная последовательность $W_0, W_1, W_2, \ldots$ векторных пространств (на самом деле существенны лишь $W_0, \ldots, W_d$) и бинарная операция $\wedge$ («внешнее произведение,» или «произведение-крышка») на множестве $W_0 \cup W_1 \cup W_2 \cup \ldots$ со следующими свойствами.*

(EA1) *Справедливо равенство* $\dim W_k = \binom{d}{k}$. *В частности, W_1 изоморфно V, а $W_k = \{\mathbf{0}\}$ при $k > d$.*

(EA2) *Если* $\mathbf{u} \in W_k$, $\mathbf{v} \in W_\ell$, *то* $\mathbf{u} \wedge \mathbf{v} \in W_{k+\ell}$.

(EA3) *Внешнее произведение* **ассоциативно**, *т. е.*

$$(\mathbf{u} \wedge \mathbf{v}) \wedge \mathbf{w} = \mathbf{u} \wedge (\mathbf{v} \wedge \mathbf{w}).$$

(EA4) *Внешнее произведение* **билинейно**, *т. е.*

$$(\alpha\mathbf{u} + \beta\mathbf{v}) \wedge \mathbf{w} = \alpha(\mathbf{u} \wedge \mathbf{w}) + \beta(\mathbf{v} \wedge \mathbf{w}),$$
$$\mathbf{u} \wedge (\alpha\mathbf{v} + \beta\mathbf{w}) = \alpha(\mathbf{u} \wedge \mathbf{v}) + \beta(\mathbf{u} \wedge \mathbf{w}).$$

(EA5) *внешнее произведение отражает линейную зависимость следующим образом: для любых $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_d \in W_1$ условие*

$$\mathbf{v}_1 \wedge \mathbf{v}_2 \wedge \ldots \wedge \mathbf{v}_d = \mathbf{0}$$

выполнено в точности тогда, когда $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_d$ линейно зависимы.

Доказательство предложения. Пусть $\mathscr{F}_k$ обозначает множество всех k-элементных подмножеств в $\{1, 2, \ldots, d\}$. Для каждого $k = 0, 1, \ldots, d$ зафиксируем $\binom{d}{k}$-мерное векторное пространство W_k, где $W_i \cap W_j = \varnothing$ при $i \neq j$. В каждом W_k зафиксируем произвольный базис (состоящий из $\binom{d}{k}$ векторов) и обозначим его векторы $b_{K_1}, b_{K_2}, \ldots$, где $K_1, K_2, \ldots, K_{\binom{d}{k}}$ — множества из $\mathscr{F}_k$, занумерованные в некотором фиксированном порядке. Другими словами, поставим базис в биективное соответствие с $\mathscr{F}_k$, так, чтобы базисный вектор $\mathbf{b}_K$ соответствовал $K \in \mathscr{F}_k$. Таким образом, $\mathbf{b}_K$ становится *названием* базисного вектора, которое будет удобнее в качестве

[1] Над любым полем, но нам потребуется лишь вещественный случай.

обозначения, чем обычное индексирование базиса числами 1, 2, … Разумеется, положим $W_{d+1} = W_{d+2} = \ldots = \{\mathbf{0}\}$.

Вначале определим внешнее произведение для базисных векторов. Пусть $K, L \subseteq \{1, 2, \ldots, d\}$, где $s_1 < s_2 < \ldots < s_k$ — элементы множества K в порядке возрастания, а $t_1 < \ldots < t_\ell$ — элементы множества L в порядке возрастания. Положим

$$\mathbf{b}_K \wedge \mathbf{b}_L := \begin{cases} \operatorname{sgn}((s_1, s_2, \ldots, s_k, t_1, t_2, \ldots, t_\ell))\mathbf{b}_{K\cup L} & \text{при } k+\ell \leqslant d, \\ \mathbf{0} \in W_{k+\ell} & \text{при } k+\ell > d. \end{cases}$$

Отметим, что при $K \cap L \neq \varnothing$ выполнено равенство $\mathbf{b}_K \wedge \mathbf{b}_L = \mathbf{0}$, поскольку тогда в последовательности $(s_1, s_2, \ldots, s_k, t_1, t_2, \ldots, t_\ell)$ какой-то член повторится и, следовательно, знак последовательности равен 0. Знаки выглядят громоздко, но они важны для хорошего поведения внешнего произведения относительно линейной независимости, т. е. для выполнения свойства (EA5).

Распространим операцию $\wedge$ на все векторы по билинейности: если $\mathbf{u} \in W_k$, $\mathbf{v} \in W_\ell$, то представим их в соответствующих базисах как $\mathbf{u} = \sum\limits_{K\in\mathscr{F}_k} \alpha_K \mathbf{b}_K$, $\mathbf{v} = \sum\limits_{L\in\mathscr{F}_\ell} \beta_L \mathbf{b}_L$ и положим

$$\mathbf{u} \wedge \mathbf{v} := \sum_{K\in\mathscr{F}_k, L\in\mathscr{F}_\ell} \alpha_K \beta_L (\mathbf{b}_K \wedge \mathbf{b}_L).$$

Теперь свойства (EA1), (EA2) и (EA4) (билинейность) очевидны.

Что касается ассоциативности (EA3), достаточно проверить её для векторов базиса, т. е. проверить равенство

$$(\mathbf{b}_K \wedge \mathbf{b}_L) \wedge \mathbf{b}_M = \mathbf{b}_K \wedge (\mathbf{b}_L \wedge \mathbf{b}_M) \tag{1}$$

для всех K, L, M. Интересен случай, когда K, L, M попарно не пересекаются и $|K| + |L| + |M| \leqslant d$. Очевидно, тогда обе части (1) имеют вид $\pm\mathbf{b}_{K\cup L\cup M}$ и остаётся проверить, что знаки совпадают.

Для этого обозначим через $s_1 < \ldots < s_k$ элементы множества K в порядке возрастания, и пусть аналогичное верно для $t_1 < \ldots < t_\ell$ и L, а также для $z_1 < \ldots < z_m$ и M. Подсчитав инверсии в соответствующих последовательностях, находим, что

$$(\mathbf{b}_K \wedge \mathbf{b}_L) \wedge \mathbf{b}_M = (-1)^N \mathbf{b}_{K\cup L\cup M},$$

где

$$N = \operatorname{inv}((s_1, \ldots, s_k, t_1, \ldots, t_\ell)) + \operatorname{inv}((s_1, \ldots, s_k, z_1, \ldots, z_m)) + \\ + \operatorname{inv}((t_1, \ldots, t_\ell, z_1, \ldots, z_m)),$$

и для правой части равенства (1) получаем то же самое.

Далее, если какие-то из множеств K, L, M пересекаются или $k + \ell + m > d$, то легко проверить, что обе части равенства (1) равны $\mathbf{0} \in W_{k+\ell+m}$. Наконец, если равенство (1) проверено, то ассоциативность в общем случае проверяется чисто технически — нужно лишь разложить три рассматриваемых вектора по соответствующим базисам, преобразовать обе части по билинейности и применить равенство (1).

Остаётся доказать свойство (EA5) — наиболее интересный пункт, где выбор знака наконец «превращается из проклятия в благословение».

Возьмём произвольные $\mathbf{v}_1, \ldots, \mathbf{v}_d \in W_1$ и разложим их по базису $\mathbf{b}_{\{1\}}, \ldots, \mathbf{b}_{\{d\}}$ пространства W_1:

$$\mathbf{v}_i = \sum_{j=1}^{d} a_{ij} \mathbf{b}_{\{j\}}.$$

С учётом билинейности и ассоциативности получаем

$$\mathbf{v}_1 \wedge \mathbf{v}_2 \wedge \ldots \wedge \mathbf{v}_d = \sum_{j_1, j_2, \ldots, j_d = 1}^{d} a_{1j_1} a_{2j_2} \ldots a_{dj_d} \mathbf{b}_{\{j_1\}} \wedge \mathbf{b}_{\{j_2\}} \wedge \ldots \wedge \mathbf{b}_{\{j_d\}}.$$

По определению внешнего произведения базисных векторов, в правой части равны нулю все слагаемые, в которых совпадают какие-то два j_i. Остаётся сумма по всем наборам из d попарно различных j_i — иначе говоря, по всем перестановкам множества $\{1, 2, \ldots, d\}$:

$$\mathbf{v}_1 \wedge \ldots \wedge \mathbf{v}_d = \sum_{\pi} a_{1\pi(1)} a_{2\pi(2)} \ldots a_{d\pi(d)} \mathbf{b}_{\{\pi(1)\}} \wedge \mathbf{b}_{\{\pi(2)\}} \wedge \ldots \wedge \mathbf{b}_{\{\pi(d)\}}.$$

Рассуждая очень похоже на проверку ассоциативности, находим, что $\mathbf{b}_{\{\pi(1)\}} \wedge \mathbf{b}_{\{\pi(2)\}} \wedge \ldots \wedge \mathbf{b}_{\{\pi(d)\}} = \operatorname{sgn}(\pi) \mathbf{b}_{\{1,2,\ldots,d\}}$. Тогда последняя сумма превращается в $\det(A) \mathbf{b}_{\{1,2,\ldots,d\}}$, что равно $\mathbf{0}$ в точности тогда, когда $\mathbf{v}_i$ линейно зависимы. Предложение доказано. □

Практически без труда можно распространить свойство (EA5) на любое количество векторов; таким образом, $\mathbf{v}_1, \ldots, \mathbf{v}_n \in W_1$ линейно зависимы в точности тогда, когда их внешнее произведение равно $\mathbf{0}$ (нам это не потребуется, но не упомянуть об этом представляется неправильным).

Доказательство теоремы. Пусть $d := k + \ell$. Рассмотрим внешнюю алгебру пространства $\mathbb{R}^d$ с такими, как в предложении, векторными пространствами $W_0, W_1, \ldots$ и операцией $\wedge$. Без потери общно-

сти можно считать, что

$$A_1 \cup \ldots \cup A_n \cup B_1 \cup \ldots \cup B_n = \{1, 2, \ldots, m\}$$

для некоторого целого m. Зафиксируем m векторов $\mathbf{v}_1, \ldots \mathbf{v}_m \in W_1 \cong \mathbb{R}^d$, находящихся в общем положении в смысле доказанного выше утверждения (любые d или меньше из этих векторов линейно независимы). Отметим, что m может быть значительно больше, чем d.

Пусть $A \subseteq \{1, 2, \ldots, m\}$ — произвольное подмножество; запишем его элементы по возрастанию: $i_1 < i_2 < \ldots < i_r$, где $r = |A|$. Положим

$$\mathbf{w}_A := \mathbf{v}_{i_1} \wedge \mathbf{v}_{i_2} \wedge \ldots \wedge \mathbf{v}_{i_r}.$$

Таким образом, $\mathbf{w}_A \in W_r$.

Пусть $A, B \subseteq \{1, 2, \ldots, m\}$, причём $|A| + |B| = d$. Тогда в силу свойств (EA3) и (EA5) имеем

$$\mathbf{w}_A \wedge \mathbf{w}_B = \begin{cases} \pm \mathbf{w}_{A \cup B} \neq \mathbf{0} & \text{при } A \cap B = \varnothing, \\ \mathbf{0} & \text{при } A \cap B \neq \varnothing. \end{cases}$$

Мы утверждаем, что n векторов $\mathbf{w}_{A_1}, \mathbf{w}_{A_2}, \ldots, \mathbf{w}_{A_n} \in W_k$ линейно независимы. Это докажет теорему, поскольку

$$\dim(W_k) = \binom{d}{k} = \binom{k+\ell}{k}.$$

Итак, пусть $\sum_{i=1}^{n} \alpha_i \mathbf{w}_{A_i} = \mathbf{0}$. Предположим, что для некоторого j мы уже знаем, что $\alpha_i = 0$ при всех $i > j$ (для $j = n$ это условие бессодержательно). Покажем, что тогда и $\alpha_j = 0$. Для этого рассмотрим внешнее произведение $\mathbf{0} \wedge \mathbf{w}_{B_j} = \mathbf{0}$ и запишем его как

$$\mathbf{0} \wedge \mathbf{w}_{B_j} = \left(\sum_{i=1}^{n} \alpha_i \mathbf{w}_{A_i} \right) \wedge \mathbf{w}_{B_j} = \sum_{i=1}^{n} \alpha_i (\mathbf{w}_{A_i} \wedge \mathbf{w}_{B_j}) = \alpha_j (\mathbf{w}_{A_j} \wedge \mathbf{w}_{B_j}),$$

поскольку $\mathbf{w}_{A_i} \wedge \mathbf{w}_{B_j} = 0$ при $i < j$ (так как $A_i \cap B_j \neq \varnothing$), $\alpha_i = 0$ при $i > j$ по предположению индукции и $\mathbf{w}_{A_j} \wedge \mathbf{w}_{B_j} \neq \mathbf{0}$, поскольку $A_j \cap B_j = \varnothing$. Отсюда $\alpha_j = 0$, и теорема доказана. □

Геометрия внешнего произведения с первого взгляда. Некоторые примеры внешнего произведения в малых размерностях связаны с общеизвестными фактами. Вначале положим $d = 2$ и отождествим W_1 с $\mathbb{R}^d$ таким образом, чтобы базис $(\mathbf{b}_{\{1\}}, \mathbf{b}_{\{2\}})$ соответствовал стандартному ортонормированному базису $(\mathbf{e}_1, \mathbf{e}_2)$. Тогда

можно показать, что $\mathbf{u} \wedge \mathbf{v} = \pm a \cdot \mathbf{e}_1 \wedge \mathbf{e}_2$, где a — площадь параллелограмма, натянутого на $\mathbf{u}$ и $\mathbf{v}$ (см. рис. 44).

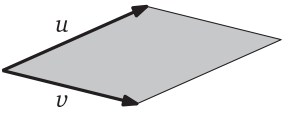


Рис. 44

В пространстве $\mathbb{R}^3$ после аналогичного отождествления W_1 с $\mathbb{R}^3$ оказывается, что $\mathbf{u} \wedge \mathbf{v}$ тесно связано с *векторным произведением* векторов $\mathbf{u}$ и $\mathbf{v}$ (часто используемым в физике), причём $\mathbf{u} \wedge \mathbf{v} \wedge \mathbf{w} = \pm a \cdot \mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3$, где a — объём параллелепипеда, натянутого на $\mathbf{u}, \mathbf{v}$ и $\mathbf{w}$. Последний факт, разумеется, служит примером на общее правило; в пространстве $\mathbb{R}^d$ объём параллелепипеда, натянутого на $\mathbf{v}_1, \ldots, \mathbf{v}_d \in \mathbb{R}^d$, равен $|\det(A)|$, где A — матрица, столбцами которой являются $\mathbf{v}_i$, и мы уже установили, что

$$\mathbf{v}_1 \wedge \ldots \wedge \mathbf{v}_d = \det(A) \cdot \mathbf{e}_1 \wedge \ldots \wedge \mathbf{e}_d.$$

Это лишь первые указания на очень богатый геометрический смысл внешнего произведения. В общем случае можно считать, что $\mathbf{v}_1 \wedge \ldots \wedge \mathbf{v}_k \in W_k$ представляет, с точностью до скалярного множителя, k-мерное подпространство в $\mathbb{R}^d$, натянутое на $\mathbf{v}_1, \ldots, \mathbf{v}_k$. Однако, безусловно, не все векторы из W_k отвечают при этом k-мерным подпространствам; можно представлять себе W_k как «замыкание», которое превращает совокупность всех k-мерных подпространств в векторное пространство.

Литература

Теорема Боллобаша была доказана в работе

Bollobás B. On generalized graphs // Acta Math. Acad. Sci. Hung. 1965. V. 16. P. 447—452.

Первое применение внешней алгебры в комбинаторике принадлежит Ловасу:

Lovász L. Flats in matroids and geometric graphs // Combinatorial Surveys (Proc. Sixth British Combinatorial Conf., Royal Holloway Coll., Egham, 1977). London: Academic Press, 1977. P. 45—86.

Эта статья содержит вариант теоремы Боллобаша для векторных подпространств, и из доказательства легко следует несимметричная теорема Боллобаша. Но похоже, что в явном виде эта теорема впервые появилась в заметке

Frankl P. An extremal problem for two families of sets // European J. Combin. 1982. V. 3, № 2. P. 125—127,

где она доказана с помощью *симметричных* тензорных произведений (притом что внешнее произведение можно интерпретировать как *антисимметричное* тензорное произведение). Метод, использующий внешние произведения, был также открыт независимо Калаи и с огромным успехом применён в изучении выпуклых политопов и геометрически заданных симплициальных комплексов:

Kalai G. Intersection patterns of convex sets // Israel J. Math. 1984. V. 48. P. 161—174.

Туза дал обзор применений метода пар множеств в двух статьях, из которых вторая:

Tuza Zs. Applications of the set-pair method in extremal problems, II // Combinatorics, Paul Erdős is eighty. Budapest: J. Bolyai Math. Soc., 1996. (Bolyai Society Mathematical Studies; V. 2). P. 459—490

охватывает более широкую тему.

Предметный указатель