ВСЯ

КОНКУРС
ПО СОЗДАНИЮ
НОВЫХ УЧЕБНИКОВ

ЛАУРЕАТ

МИНИСТЕРСТВА
ОБРАЗОВАНИЯ
РОССИИ

М. Л. Краснов
А. И. Киселев
Г. И. Макаренко
Е. В. Шикин
В. И. Заляпин
А. Ю. Эвнин

ВЫСШАЯ МАТЕМАТИКА 7

- Теория чисел
- Общая алгебра
- Комбинаторика
- Теория Пойа
- Теория графов
- Паросочетания
- Матроиды

Теория ▸ Примеры

URSS

ВСЯ ВЫСШАЯ МАТЕМАТИКА

М. Л. Краснов
А. И. Киселев
Г. И. Макаренко
Е. В. Шикин
В. И. Заляпин
А. Ю. Эвнин

7

Рекомендовано
Министерством образования
Российской Федерации
в качестве учебника для студентов
высших технических учебных заведений

МОСКВА
URSS

ББК 22.1я73

**Краснов Михаил Леонтьевич, Киселев Александр Иванович,
Макаренко Григорий Иванович, Шикин Евгений Викторович,
Заляпин Владимир Ильич, Эвнин Александр Юрьевич**

Вся высшая математика: Учебник. Т. 7. — М.: КомКнига, 2006. — 208 с.

ISBN 5-484-00521-3

Предлагаемый учебник впервые вышел в свет в виде двухтомника сначала на английском и испанском языках в 1990 году, а затем на французском. Он пользуется большим спросом за рубежом.

В 1999 году книга стала лауреатом конкурса по созданию новых учебников Министерства образования России.

Этот учебник адресован студентам высших учебных заведений (в первую очередь будущим инженерам и экономистам) и охватывает практически все разделы математики, но при этом представляет собой не набор разрозненных глав, а единое целое.

Седьмой том включает в себя материал по теории чисел, комбинаторике и теории графов. В первых двух главах тома рассматриваются элементы теории чисел и общей алгебры. Вводимые при этом понятия широко используются в других главах, в частности при изложении теории Пойа, позволяющей решать задачи пересчета объектов с точностью до того или иного отношения эквивалентности. В главе, посвященной комбинаторике, помимо начальных сведений о выборках излагается принцип включения-исключения, эффективно работающий при решении классических комбинаторных задач. Здесь также описывается аппарат производящих функций — мощное средство комбинаторного анализа. В заключительных главах вводятся основные понятия теории графов и матроидов, описываются некоторые эффективные алгоритмы.

Издательство «КомКнига». 117312, г. Москва, пр-т 60-летия Октября, 9.
Подписано к печати 09.03.2006 г. Формат 70×100/16. Печ. л. 13. Зак. № 2331.
Отпечатано в типографии ООО ПФ «Полиграфист». 160001, г. Вологда, ул. Челюскинцев, 3.

ISBN 5-484-00521-3

НАУЧНАЯ И УЧЕБНАЯ ЛИТЕРАТУРА
E-mail: URSS@URSS.ru
Каталог изданий в Интернете:
http://URSS.ru
Тел./факс: 7 (495) 135-42-16
URSS Тел./факс: 7 (495) 135-42-46

3384 ID 31314
9 785484 005215

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

В предыдущих книгах нашего издания развитие основных событий в большей или меньшей степени было связано с ключевой идеей *близости*, математическое осмысление которой привело к ошеломляющему каскаду самых разнообразных результатов. И хотя эта идея еще весьма далека от исчерпания, существует широкий пласт математических задач, в которых она не работает. Значительную по объему долю в этом пласте составляют задачи, в которых изучаются свойства множеств, состоящих из конечного числа элементов. Число элементов в таких множествах может быть разным — от нескольких единиц до многих степеней десяти — $10^{10}, 10^{10^{10}}, \ldots$.

Истоки некоторых из этих задач и методы их решения отделены от нас сотнями и даже тысячами лет. Появление других было стимулировано развитием вычислительных средств, стремительно расширяющиеся возможности которых сами служат источником все новых и новых задач.

Нарастающий интерес вызвал к жизни новое понятие — *дискретная математика*. Понимаемая в широком смысле дискретная математика включает в себя теорию чисел, общую алгебру, математическую логику, комбинаторный анализ, теорию графов, теорию кодирования, целочисленное программирование, теорию функциональных систем и др.

Дискретность (от латинского *discretus* — разделенный, прерывистый) нередко противопоставляют непрерывности. Однако при решении сложных практических задач дискретные и непрерывные подходы работают совместно и весьма эффективно, взаимно обогащая друг друга.

В 1998 году издательство «Мир» выпустило книгу Р. Грэхема, Д. Кнута и О. Паташника «Конкретная математика» (*Concrete mathematics*), термин

CONCRETE

в названии которой образован слиянием слов

CONtinious и *disCRETE*.

Основная задача этого тома — дать читателю рабочее представление о технике оперирования с дискретными объектами, аналогичной технике для объектов непрерывных.

Наша цель скромней: мы лишь хотим познакомить читателя с некоторыми элементами дискретной математики.

В первых двух главах тома рассматриваются элементы теории чисел и общей алгебры. Вводимые при этом понятия широко используются в других главах,

в частности при изложении теории Пойа, позволяющей решать задачи пересчета объектов с точностью до того или иного отношения эквивалентности. В главе, посвященной комбинаторике, помимо начальных сведений о выборках излагается принцип включения-исключения, эффективно работающий при решении классических комбинаторных задач. Здесь также описывается аппарат производящих функций — мощное средство комбинаторного анализа. В заключительных главах вводятся основные понятия теории графов и матроидов, описываются некоторые эффективные алгоритмы.

Глава LXVI

ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ

Откуда взялись числа, не знает никто. Этнографы объездили все страны вдоль и поперек и нашли народы, которым вполне хватает «один», «два» и «много». А между тем, у них есть и изысканное искусство, и тончайшие мифы, и нетривиальные ремесла. Видимо, эти народы так и не столкнулись с проблемами, для разрешения которых было необходимо заметное расширение числового диапазона. Они такие же люди, как и мы, только без этого «один», «два», «три» и так далее, вплоть до натурального ряда чисел.

Магия натуральных чисел необычайно притягательна. Она привлекает внимание не только увлеченных модной нынче нумерологией, но и заражает выдающиеся умы. Леонард Эйлер, Карл Фридрих Гаусс, Георг Фридрих Бернхард Риман и многие другие, чьи имена читатель уже встречал в самых разных разделах томах нашей серии, серьезно занимались проблемами высшей арифметики, или, как ее принято называть сейчас, теории чисел, в которой к настоящему времени накопилось значительное количество недоказанных утверждений (несмотря на впечатляющие успехи).

Обманчиво простая формулировка Великой теоремы Ферма породила столь большую и разношерстную армию желающих ее доказать, что профессиональные математики, обращавшиеся к этой проблеме, предпочитали скрывать свои усилия по ее доказательству. Это в полной мере относится и к Эндрю Уайлсу, сумевшему обосновать всем очевидный ответ около десяти лет назад. Насколько важен этот результат для науки, сказать трудно — на этот счет существуют разные точки зрения. Но то обстоятельство, что найденное доказательство совсем не просто, признают все.

В этой главе мы знакомим читателя с некоторыми понятиями теории чисел, с несложным инструментарием, позволяющим показать целый ряд замечательных свойств натуральных чисел, и рассказываем об одном из применений классических результатов теории чисел к решению чрезвычайно актуальной проблемы защиты информации (создании надежных шифров).

§ 1. Теорема о делении с остатком

Пусть a и b — целые числа. Если существует такое целое число q, что $a = bq$, то говорят: a *делится на* b, или a *кратно* b, или b *делит* a, или b — *делитель* a; при этом пользуются обозначениями $a \vdots b$ или $b \mid a$.

Теорема 1 (теорема о делении с остатком). *Пусть* $a \in \mathbb{Z}$, $b \in \mathbb{N}$. *Тогда*

$$\exists!\, q, \quad r \in \mathbb{Z}, \quad a = bq + r, \quad 0 \leqslant r < b.$$

◀ *Существование.* Пусть bq — наибольшее из чисел, кратных b и не превосходящих a. Тогда выполняется двойное неравенство $bq \leqslant a < b(q+1)$, а, значит, и $0 \leqslant a - bq < b$. Теперь если положить $r = a - bq$, то одновременно будем иметь: $a = bq + r$, $0 \leqslant r < b$.

Единственность. Пусть $a = bq_1 + r_1$ и $a = bq_2 + r_2$. Вычитая из первого равенства второе, получаем: $0 = b(q_1 - q_2) + r_1 - r_2$, или $b(q_1 - q_2) = r_2 - r_1$, откуда следует, что $r_1 - r_2$ делится на b. С другой стороны, из неравенств $0 \leqslant r_1 < b$ и $0 \leqslant r_2 < b$ вытекает неравенство $|r_1 - r_2| < b$. Сопоставляя два полученных факта, заключаем, что $r_1 - r_2 = 0$. Тогда $b(q_1 - q_2) = 0$, и так как $b \neq 0$ (b — *натуральное* число), то $q_1 = q_2$. Итак, любые два представления числа a в виде $a = bq + r$ совпадают. Единственность доказана. ►

Замечание. Числа q и r из формулировки доказанной теоремы называют соответственно *частным* и *остатком от деления* a на b.

§ 2. Наибольший общий делитель. Алгоритм Евклида

В этом параграфе все числа предполагаются натуральными.

Обозначим через $D(a)$ множество всех делителей числа a, а через $D(a_1, a_2, \ldots, a_n)$ — множество всех общих делителей чисел $a_1, a_2, \ldots, a_n$. Таким образом,

$$D(a_1, a_2, \ldots, a_n) = \bigcap_{i=1}^{n} D(a_i).$$

Заметим, что это множество конечно и не пусто (по крайней мере, оно содержит 1), поэтому в нем есть наибольший элемент, который будем обозначать $(a_1, a_2, \ldots a_n)$ и называть *наибольшим общим делителем* чисел $a_1, a_2, \ldots, a_n$.

Натуральные числа a и b называются *взаимно простыми*, если их наибольший общий делитель равен 1. Очевидно следующее утверждение.

Лемма 1. $a \vdots b \Leftrightarrow (a, b) = b$.

Лемма 2. *Пусть* $a = bq + r$, $0 < r < b$. *Тогда* $(a, b) = (b, r)$.

◀ Пусть $x \in D(a, b)$. Тогда $a \vdots x$, $b \vdots x$ и $r = a - bq \vdots x$. Таким образом, $x \in D(b, r)$.

Пусть теперь $x \in D(b, r)$. Тогда $b \vdots x$, $r \vdots x$ и $a = bq + r \vdots x$. Таким образом, $x \in D(a, b)$.

Доказано равенство множеств $D(b, r) = D(a, b)$, а, значит, и их максимальных элементов. Поэтому $(b, r) = (a, b)$, что и требовалось доказать. ►

Пусть a не делится на b. Тогда имеет место представление a в виде $a = bq_0 + r_1$, $0 < r_1 < b$. По лемме 2 $(a, b) = (b, r_1)$. Если b не делится на r_1, то имеем: $b = r_1q_1 + r_2$, $0 < r_2 < r_1$ и $(b, r_1) = (r_1, r_2)$. Продолжив данный процесс (а он называется *алгоритмом Евклида*), получим последовательность остатков (r_i), это — убывающая последовательность натуральных чисел. Она не может быть бесконечной, поэтому найдется остаток r_n, являющийся делителем предыдущего остатка r_{n-1}. Итак, выполняются следующие соотношения:

$$\begin{aligned}
a &= bq_0 + r_1, && 0 < r_1 < b; && (a, b) = (b, r_1);\\
b &= r_1q_1 + r_2, && 0 < r_2 < r_1; && (b, r_1) = (r_1, r_2);\\
r_1 &= r_2q_2 + r_3, && 0 < r_3 < r_2; && (r_1, r_2) = (r_2, r_3);\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
r_{n-2} &= r_{n-1}q_{n-1} + r_n, && 0 < r_n < r_{n-1}; && (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n);\\
r_{n-1} &= r_nq_n; && && (r_{n-1}, r_n) = r_n.
\end{aligned}$$

(Последнее равенство справедливо в силу леммы 1.)

Цепочка равенств

$$(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = r_n$$

доказывает следующую теорему.

Теорема 2. *Наибольший общий делитель двух чисел равен последнему ненулевому остатку в алгоритме Евклида, примененному к данным числам.*

Пример. Для нахождения (288, 126) применим алгоритм Евклида к числам 288 и 126:

288	126	
126	36	2
36	18	3
0	2	

Последний ненулевой остаток равен 18; поэтому (288, 126) = 18.

Теорема 3. *Наибольший общий делитель двух чисел делится на любой из общих делителей этих чисел.*

◄ Пусть $a \vdots x$, $b \vdots x$; $r_1, \ldots, r_n$ — остатки, возникающие при работе алгоритма Евклида. Тогда

$$r_1 = (a - bq_0) \vdots x, \quad r_2 = (b - r_1q_1) \vdots x, \quad \ldots, \quad r_n = (r_{n-2} - r_{n-1}q_{n-1}) \vdots x.$$

В силу предыдущей теоремы $r_n = (a, b)$. Таким образом, $(a, b) \vdots x$, что и требовалось доказать. ►

2.1. Свойства наибольшего общего делителя

1. $(a, b) = (b, a)$.
2. $(ma, mb) = m(a, b)$.

   ◀ Все равенства, возникающие при работе алгоритма Евклида, почленно умножаются на m при переходе от пары $\langle a, b\rangle$ к паре $\langle ma, mb\rangle$. ▶
3. *Если a и b взаимно просты, то* $(ac, b) = (c, b)$.

   ◀ Пусть $x \in D(ac, b)$. Тогда $ac \vdots x$, $b \vdots x$, $bc \vdots x$, т.е. $x \in D(ac, bc)$. По теореме 3 $(ac, bc) \vdots x$, и, в силу предыдущего свойства, $c(a, b) \vdots x$, но по условию $(a, b) = 1$. Таким образом, $c \vdots x$ и $x \in D(b, c)$. Пусть теперь $x \in D(b, c)$. Тогда $b \vdots x$, $c \vdots x$, $ac \vdots x$ и $x \in D(ac, b)$. Доказано, что $D(ac, b) = D(c, b)$, откуда следует требуемое. ▶
4. *Если числа a_1 и a_2 взаимно просты с b, то тем же свойством обладает и их произведение, т.е.* $(a_1, b) = 1, (a_2, b) = 1 \Rightarrow (a_1a_2, b) = 1$.
   Это свойство вытекает из предыдущего.
5. *Пусть для* $i = 1, 2, \ldots, n$ $(a_i, b) = 1$. *Тогда* $\left(\prod\limits_{i=1}^{n} a_i, b\right) = 1$.

   Свойство легко доказать индукцией по n с помощью предыдущего свойства.
6. *Если* $\forall i, j$ $(a_i, b_j) = 1$, *то* $\left(\prod a_i, \prod b_j\right) = 1$.
   Следует из свойств 1 и 5.
7. $(a_1, a_2, \ldots, a_n) = \big((\ldots((a_1, a_2), a_3), \ldots), a_n\big)$.
   Для доказательства достаточно использовать соотношение

$$D(a_1, a_2, \ldots, a_n) = D(a_1) \cap D(a_2) \cap \ldots \cap D(a_n)$$

   и свойство ассоциативности пересечения множеств.

§ 3. $(k^a - 1, k^b - 1) = k^{(a,b)} - 1$

Вновь все числа, рассматриваемые в этом параграфе, предполагаются натуральными.

Пусть $k \geqslant 2$. Докажем справедливость формулы, вынесенной в заголовок параграфа.

Рассмотрим сначала случай, когда a кратно b. Имеем при этом $a = bq$ и $(a, b) = b$ (по лемме 1). Доказываемое равенство приобретает вид $(k^a - 1, k^b - 1) = k^b - 1$ и равносильно тому, что $k^a - 1$ кратно $k^b - 1$. С помощью алгебраического тождества

$$y^n - 1 = (y - 1)(y^{n-1} + y^{n-2} + \ldots + y + 1)$$

получаем, что $k^a - 1 = k^{bq} - 1 = (k^b)^q - 1$ делится на $k^b - 1$.

Пусть теперь a не делится на b, т.е. $a = bq + r$, $0 < r < b$. Имеем:

$$k^a - 1 = k^{bq+r} - 1 = k^r(k^{bq} - 1) + k^r - 1.$$

Как показано выше, $k^{bq} - 1$ делится на $k^b - 1$. Кроме того, $0 < k^r - 1 < k^b - 1$. Таким образом, остаток от деления $k^a - 1$ на $k^b - 1$ равен $k^r - 1$. Поэтому по лемме 2 $(k^a - 1, k^b - 1) = (k^b - 1, k^r - 1)$. Используя соотношения алгоритма Евклида

$a = bq_0 + r_1$, $b = r_1q_1 + r_2$, $r_1 = r_2q_2 + r_3, \ldots, r_{n-2} = r_{n-1}q_{n-1} + r_n$, $r_{n-1} = q_nr_n$, получаем цепочку равенств $(k^a - 1, k^b - 1) = (k^b - 1, k^{r_1} - 1) = (k^{r_1} - 1, k^{r_2} - 1) = \ldots = (k^{r_{n-1}} - 1, k^{r_n} - 1) = k^{r_n} - 1 = k^{(a,b)} - 1$. Сопоставляя начало и конец этой цепочки, получаем требуемое.

Пример. $(288, 216) = 18 \Rightarrow (3^{288} - 1, 3^{216} - 1) = 3^{18} - 1$.

Важным следствием доказанного соотношения является следующее утверждение.

Если m и n взаимно просты, то взаимно простыми будут и числа $2^m - 1$ и $2^n - 1$.

Действительно, $(m, n) = 1 \Rightarrow (2^m - 1, 2^n - 1) = 2^{(m,n)} - 1 = 2^1 - 1 = 1$.

§ 4. Простые числа. Основная теорема арифметики

Натуральное число, большее 1, называется *простым*, если оно имеет ровно два делителя — 1 и само себя.

Натуральное число, большее 1, не являющееся простым, называется *составным*.

1 не является ни простым, ни составным числом.

Отметим, что число является простым тогда и только тогда, когда оно взаимно просто со всеми меньшими натуральными числами.

Теорема 4. *Множество простых чисел бесконечно.*

◄ Предположим, что $F = \{n_1, n_2, \ldots, n_k\}$ — множество *всех* простых чисел ($n_1 = 2$, $n_2 = 3$, $n_3 = 5, \ldots$). Очевидно, что числа из F попарно взаимно просты; в силу последнего утверждения предыдущего параграфа при $i \neq j$ числа $2^{n_i} - 1$ и $2^{n_j} - 1$ также взаимно просты. Выберем теперь для каждого $i = 1, 2, \ldots, k$ какой-нибудь *простой* делитель p_i числа $2^{n_i} - 1$; числа $p_1, p_2, \ldots, p_k$ будут попарно различны. В результате образуется множество $G = \{p_1, p_2, \ldots, p_k\}$ простых чисел ($p_1 = 3$, $p_2 = 7$, $p_3 = 31, \ldots$). Все элементы G — суть *нечетные* числа. Поскольку множества F и G содержат поровну элементов, $2 \in F$ и $2 \notin G$, делаем вывод, что в G найдется число, не входящее в F. Пришли к противоречию. Теорема доказана. ►

Теорема 5 (основная теорема арифметики). *Любое натуральное число, большее 1, представимо в виде произведения простых чисел. Такое представление единственно с точностью до порядка сомножителей.*

◄ Существование и единственность указанного представления для простых чисел очевидно. Доказательство теоремы для составных чисел проводится методом математической индукции.

Пусть a — составное число. Предположим, что все натуральные числа от 2 до $a - 1$ раскладываются, и притом единственным образом, в произведение простых чисел.

Докажем *существование* соответствующего разложения и для a. Наименьший делитель a, больший 1, обозначим p. Очевидно, p — простое число. Для некоторого натурального числа a_1 имеем $a = a_1 \cdot p$, причем $a_1 < a$. По предположению индукции a_1 раскладывается на простые множители, поэтому тем же свойством обладает и число a.

Единственность. Пусть существуют два разложения составного числа a на простые множители:

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_n = q_1 \cdot q_2 \cdot \ldots \cdot q_m. \qquad (1)$$

Если $p_i \neq q_j$ для всех i и j, то имеем $\forall\, i, j \quad (p_i, q_j) = 1$ и по свойству 6 из § 2

$$a = (a, a) = (p_1 \cdot p_2 \cdot \ldots \cdot p_n, q_1 \cdot q_2 \cdot \ldots \cdot q_m) = 1,$$

что противоречит неравенству $a > 1$. Значит, для некоторых i и $j \quad p_i = q_j$. Пусть $a = a_1 \cdot p_i$. Сокращая части равенства (1) на общий множитель $p_i = q_j$, получим два разложения для числа a_1. Поскольку $a_1 < a$, эти разложения совпадают. Отсюда следует и единственность представления числа a в виде произведения простых чисел. Теорема доказана. ►

Представление натурального числа в виде

$$a = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r},$$

где $p_1, p_2, \ldots, p_r$ — попарно различные простые числа, называют *каноническим разложением* числа a.

§ 5. Сравнения и их свойства

В этом параграфе все числа предполагаются целыми.

Пусть m — натуральное число. Говорят, что a *сравнимо с* b *по модулю* m, если их разность $a - b$ делится на m. При этом используется запись $a \equiv b (\mathrm{mod}\, m)$.

Например, $7 \equiv 1 (\mathrm{mod}\, 3)$; $12 \equiv -2 (\mathrm{mod}\, 7)$.

Очевидно, что

$$a \equiv b (\mathrm{mod}\, m) \quad \Leftrightarrow \quad \exists\, t \in \mathbb{Z} \quad a = b + mt.$$

Докажем следующее простое

Предложение. $a \equiv b (\mathrm{mod}\, m)$ *тогда и только тогда, когда* a *и* b *имеют одинаковые остатки от деления на* m.

◄ Пусть a и b при делении на m дают остатки r_1 и r_2 соответственно:

$$a = mq_1 + r_1, \quad 0 \leqslant r_1 < m; \quad b = mq_2 + r_2, \quad 0 \leqslant r_2 < m.$$

Если $a \equiv b (\mathrm{mod}\, m)$, то $(a - b) \vdots m$, т.е. $(m(q_1 - q_2) + r_1 - r_2) \vdots m$, откуда $(r_1 - r_2) \vdots m$. С другой стороны, поскольку $0 \leqslant r_1, r_2 < m$, имеем $|r_1 - r_2| < m$. Сопоставляя два последних утверждения, получаем, что $r_1 - r_2 = 0$, поэтому $r_1 = r_2$.

Обратно, при $r_1 = r_2$ справедливо $a - b = m(q_1 - q_2) \vdots m$. ►

Заметим, что всякое число сравнимо по модулю m со своим остатком от деления на m.

Свойства сравнений

1. $a \equiv a (\mathrm{mod}\, m)$ (рефлексивность).
2. $a \equiv b (\mathrm{mod}\, m) \Rightarrow b \equiv a (\mathrm{mod}\, m)$ (симметричность).
3. $a \equiv b (\mathrm{mod}\, m), b \equiv c (\mathrm{mod}\, m) \Rightarrow a \equiv c (\mathrm{mod}\, m)$ (транзитивность).

   ◄ Если $(a-b) \vdots m$, $(b-c) \vdots m$, то и $a-c=(a-b)+(b-c) \vdots m$. ►
4. $a_1 \equiv b_1 (\mathrm{mod}\, m)$, $a_2 \equiv b_2 (\mathrm{mod}\, m) \Rightarrow a_1 + a_2 \equiv b_1 + b_2 (\mathrm{mod}\, m)$.

   ◄ Если $(a_1 - b_1) \vdots m$, $(a_2 - b_2) \vdots m$, то
   $(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) \vdots m$. ►
5. $a_1 \equiv b_1 (\mathrm{mod}\, m)$, $a_2 \equiv b_2 (\mathrm{mod}\, m) \Rightarrow a_1 \cdot a_2 \equiv b_1 \cdot b_2 (\mathrm{mod}\, m)$.

   ◄ Числа a_1 и a_2 можно представить в виде $a_1 = b_1 + mt_1$ и $a_2 = b_2 + mt_2$; поэтому $a_1a_2 - b_1b_2 = (b_1 + mt_1)(b_2 + mt_2) - b_1b_2 = (b_1t_2 + t_2b_1 + mt_1t_2)m \vdots m$. ►

   Таким образом, *сравнения по одинаковому модулю можно почленно складывать и умножать.*
6. $a \equiv b (\mathrm{mod}\, m) \Rightarrow ca \equiv cb (\mathrm{mod}\, m)$.
   Это свойство — следствие свойств 1, 5.
7. $a \equiv b (\mathrm{mod}\, m)$, $n \in \mathbb{N} \Rightarrow a^n \equiv b^n (\mathrm{mod}\, m)$.
   Следствие предыдущего свойства.
8. Если $a \equiv b (\mathrm{mod}\, m)$ и $P(x)$ — многочлен с целыми коэффициентами, то $P(a) \equiv P(b) (\mathrm{mod}\, m)$.
   Следствие свойств 4, 6, 7.

Примеры решения задач

1) Доказать, что любое натуральное число сравнимо с суммой своих цифр по модулю 9.

   ◄ Пусть натуральное число k имеет десятичную запись $k = \overline{a_{n-1}a_{n-2}\ldots a_1a_0}$. Рассмотрим многочлен $P(x) = \sum\limits_{i=0}^{n-1} a_i \cdot x^i$, чьи коэффициенты суть цифры числа k. Очевидно, что $k = P(10)$, $P(1) = \sum\limits_{i=0}^{n-1} a_i$.

   Поскольку $10 \equiv 1 (\mathrm{mod}\, 9)$, в силу свойства 8 получаем $P(10) \equiv P(1) (\mathrm{mod}\, 9)$, что и требовалось доказать.

   Частным случаем доказанного утверждения является известный из средней школы признак делимости на 9. Аналогично доказывается, что любое натуральное число сравнимо с суммой своих цифр по модулю 3. ►

2) Вывести признак делимости на 11.

   Пусть, как и выше, $k = \overline{a_{n-1}a_{n-2}\ldots a_1a_0}$, $P(x) = \sum\limits_{i=0}^{n-1} a_i \cdot x^i$. Так как $10 \equiv -1 (\mathrm{mod}\, 11)$, имеем $k = P(10) \equiv P(-1) (\mathrm{mod}\, 11)$. Заметим, что

   $$P(-1) = a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^{n-1} a_{n-1}.$$

   Таким образом, число делится на 11 тогда и только тогда, когда делится на 11 знакочередующаяся сумма его цифр.

3) Десятичная запись числа состоит из 95 единиц и нескольких нулей. Может ли оно быть квадратом некоторого натурального числа?

◄ Пусть k — данное число. Как отмечалось выше, число сравнимо с суммой своих цифр по модулю 3. Поэтому $k \equiv 95 (\mathrm{mod}\, 3) \equiv 2 (\mathrm{mod}\, 3)$.
Выясним теперь, какие остатки может давать квадрат натурального числа n от деления на 3. Имеет место один из трех случаев: n сравнимо с 0, 1 или 2 по модулю 3.
Если $n \equiv 0 (\mathrm{mod}\, 3)$, то $n^2 \equiv 0 (\mathrm{mod}\, 3)$;
если $n \equiv 1 (\mathrm{mod}\, 3)$, то $n^2 \equiv 1 (\mathrm{mod}\, 3)$;
если $n \equiv 2 (\mathrm{mod}\, 3)$, то $n^2 \equiv 4 \equiv 1 (\mathrm{mod}\, 3)$.
Таким образом, квадрат натурального числа не может давать остаток 2 от деления на 3; ответ на вопрос задачи отрицательный. ►

4) Докажите самостоятельно, что квадрат натурального числа при делении на 4 может иметь остатки только 0 или 1.

5) Доказать, что $(3^{30} - 2^{30}) \vdots 7$.

◄ Действительно, $3^{30} = 27^{10} \equiv (-1)^{10} \equiv 1 (\mathrm{mod}\, 7)$; $2^{30} = 8^{10} \equiv 1^{10} \equiv 1 (\mathrm{mod}\, 7)$, откуда вытекает требуемое. ►

6) Доказать, что для любого натурального n $(5^{2n+3} + 3^{n+3} \cdot 2^n) \vdots 19$.

◄ $5^{2n+3} = 125 \cdot 25^n \equiv 11 \cdot 6^n (\mathrm{mod}\, 19)$. $3^{n+3} \cdot 2^n = 27 \cdot 6^n \equiv 8 \cdot 6^n (\mathrm{mod}\, 19)$. Складывая сравнения, получаем: $5^{2n+3} + 3^{n+3} \cdot 2^n \equiv 19 \cdot 6^n \equiv 0 (\mathrm{mod}\, 19)$, что и требовалось. ►

7) Доказать, что для любого натурального n
$13 \cdot (-50)^n + 17 \cdot 40^n - 30 \vdots 1989$.

◄ Разложим 1989 на множители: $1989 = 9 \cdot 13 \cdot 17$. Обозначим $a_n = 13 \cdot (-50)^n + 17 \cdot 40^n - 30$. Докажем, что a_n делится на 9, 13 и 17. Действительно, $a_n \equiv 4 \cdot 4^n + (-1) \cdot 4^n - 3 \equiv 3 \cdot (4^n - 1) (\mathrm{mod}\, 9)$. Поскольку $4^n - 1 \equiv 1^n - 1 \equiv 0 (\mathrm{mod}\, 3)$, $3 \cdot (4^n - 1) \vdots 9$ и $a_n \equiv 3 \cdot (4^n - 1) \equiv 0 (\mathrm{mod}\, 9)$, т. е. a_n делится на 9. Делимость на 13 и 17 доказывается совсем просто: $a_n \equiv 0 + 17 \cdot 1^n - 30 \equiv 0 (\mathrm{mod}\, 13)$; $a_n \equiv 13 \cdot 1^n + 0 - 30 \equiv 0 (\mathrm{mod}\, 17)$. Итак, a_n делится на попарно взаимно простые числа 9, 13 и 17, поэтому a_n кратно их произведению — 1989. ►

8) Найти остаток от деления на 3 числа $\prod\limits_{k=1}^{1000} (k^2 + 1)$.

◄ Имеем:

$$\prod_{k=1}^{1000} (k^2 + 1) \equiv ((1+1)(1+1) \cdot 1)^{333} \cdot (1+1) \equiv 4^{333} \cdot 2 \equiv 1^{333} \cdot 2 \equiv 2 (\mathrm{mod}\, 3).$$

Остаток равен 2. ►

9) Доказать, что уравнение $x^2 - 4x + 12y = 19$ не имеет решений в целых числах.

◄ Действительно, поскольку $4x - 12y \vdots 4$, $x^2 = 4x - 12y + 19 \equiv 3 (\mathrm{mod}\, 4)$, что противоречит результату 4). ►

§6. Системы вычетов

Как показано в § 5, отношение сравнимости по модулю m обладает свойствами рефлексивности, симметричности и транзитивности; поэтому оно является отношением *эквивалентности*[1].

Возьмем произвольное целое число a. Обозначим через $\bar{a}$ множество чисел, сравнимых с a по модулю m: $\bar{a} = \{x \in \mathbb{Z} \mid x \equiv a (\mathrm{mod}\, m)\}$. Пусть $b \notin \bar{a}$ и $\bar{b} = \{x \in \mathbb{Z} \mid x \equiv b (\mathrm{mod}\, m)\}$. Пусть теперь $c \notin \bar{a} \cup \bar{b}$ и $\bar{c} = \{x \in \mathbb{Z} \mid x \equiv c (\mathrm{mod}\, m)\}$. И так далее. Процесс будет длиться до тех пор, пока построенные множества не будут покрывать все множество целых чисел. При этом возникает *разбиение*[2] множества $\mathbb{Z}$ на множества $\bar{a}, \bar{b}, \bar{c}, \ldots$, которые называют *классами вычетов по модулю m*; каждое число, входящее в какой-нибудь из классов, называется *вычетом* этого класса.

Число классов вычетов по модулю m равно m. Действительно, остаток от деления целого числа на m принимает одно из значений $0, 1, \ldots, m-2$ или $m-1$ и поэтому каждое из чисел попадает в один из классов $\bar{0}, \bar{1}, \ldots, \overline{m-1}$, количество которых равно m.

Взяв по одному числу из каждого класса вычетов $x_1, x_2, \ldots, x_m$, получим систему представителей классов вычетов, *или полную систему вычетов по модулю m*.

Пример 1. Различные полные системы вычетов по модулю 7:

1) $0, 1, 2, 3, 4, 5, 6$;
2) $-3, -2, -1, 0, 1, 2, 3$;
3) $7, -6, 9, -4, 11, -2, 13$.

Лемма 3. *Числа $x_1, x_2, \ldots, x_m$ образуют полную систему вычетов по модулю m тогда и только тогда, когда они попарно не сравнимы по модулю m.*

◄ Необходимость очевидна. Докажем достаточность. Если два числа не сравнимы по модулю m, то они попадают в разные классы вычетов. Так как всего классов вычетов m и рассматриваемых чисел m, то они составляют полную систему вычетов. ►

Лемма 4. *Пусть $x_1, x_2, \ldots, x_m$ — полная система вычетов по модулю m, целое число a взаимно просто с m, b — произвольное целое число. Тогда числа $ax_1 + b$, $ax_2 + b$, $\ldots$, $ax_m + b$ также образуют полную систему вычетов.*

◄ Согласно лемме 3 достаточно убедиться в том, что $ax_i + b \not\equiv ax_j + b (\mathrm{mod}\, m)$ при $i \neq j$. Предположим (для приведения к противоречию), что $ax_i + b \equiv ax_j + b (\mathrm{mod}\, m)$.

---

[1] Об общем определении отношения и его свойствах речь пойдет ниже — в главе LXVIII; заметим, что теория чисел является источником многих важных примеров для общей алгебры.

[2] Разбиение множества — это представление его в виде объединения попарно не пересекающихся подмножеств.

Тогда $a(x_i - x_j) \vdots m$, и, поскольку $(a, m) = 1$, имеем $(x_i - x_j) \vdots m$, что противоречит лемме 3. ►

Лемма 5. *Пусть* $x \equiv a (\mathrm{mod}\, m)$. *Тогда* $(x, m) = (a, m)$.

◄ Действительно, пусть r — остаток от деления a на m. Тогда по лемме 2 $(a, m) = (r, m)$. Но так как $x \equiv a (\mathrm{mod}\, m)$, при делении на m число x также имеет остаток r, и, следовательно, $(x, m) = (r, m)$, откуда и вытекает требуемое. ►

Итак, числа из одного класса вычетов по модулю m имеют один и тот же наибольший общий делитель с m. Поэтому становится корректным следующее определение.

Вычет по модулю m называют *приведенным*, если он взаимно прост с m. Совокупность приведенных вычетов из разных классов вычетов называют *приведенной системой вычетов.*

Пример 2. При $m = 7$ приведенная система вычетов может выглядеть так: 1, 2, 3, 4, 5, 6; а при $m = 6$ так: 1, 5.

Функцией Эйлера $\varphi(m)$ называют число натуральных чисел, не превосходящих m и взаимно простых с m. Например, $\varphi(1) = 1$; $\varphi(2) = 1$; $\varphi(3) = 2$; $\varphi(4) = 2$; $\varphi(5) = 4$. Легко видеть, что если p — простое число, то $\varphi(p) = p - 1$.

Очевидно, что приведенная система вычетов по модулю m содержит $\varphi(m)$ чисел.

Лемма 6. *Пусть* a *взаимно просто с* m, $k = \varphi(m)$ *и* $x_1, x_2, \ldots, x_k$ *— приведенная система вычетов по модулю* m. *Тогда числа* $ax_1, ax_2, \ldots, ax_k$ *также образуют приведенную систему вычетов по модулю* m.

◄ Так как числа a и x_i взаимно просты с m, таким же свойством обладает и их произведение ax_i. В силу леммы 4 числа $ax_1, ax_2, \ldots, ax_k$ принадлежат k разным классам вычетов, и, следовательно, в силу предыдущего, образуют приведенную систему вычетов. ►

§ 7. Теорема Эйлера

Пусть m — натуральное число, $k = \varphi(m)$, $x_1, x_2, \ldots, x_k$ — приведенная система вычетов по модулю m. Пусть a — какое-нибудь натуральное число, взаимно простое с m. Тогда в силу результатов предыдущего параграфа числа $ax_1, ax_2, \ldots, ax_k$ также образуют приведенную систему вычетов по тому же модулю. Поскольку ax_j — приведенный вычет, для некоторого числа $i_j \in \{1, 2, \ldots, k\}$ справедливо соотношение $ax_j \equiv x_{i_j} (\mathrm{mod}\, m)$. Числа $i_1, i_2, \ldots, i_k$ попарно различны и поэтому образуют перестановку чисел от 1 до k. Перемножив k полученных сравнений, получим

$$a^k \cdot x_1 \cdot x_2 \cdot \ldots \cdot x_k \equiv x_{i_1} \cdot x_{i_2} \cdot \ldots \cdot x_{i_k} (\mathrm{mod}\, m).$$

Пусть $s = x_1 \cdot x_2 \cdot \ldots \cdot x_k$. Тогда произведение $x_{i_1} \cdot x_{i_2} \cdot \ldots \cdot x_{i_k}$ также равно s. Заметим, что поскольку делители s взаимно просты с m, число s также обладает

этим свойством. Итак, $a^k s \equiv s (\mathrm{mod}\, m)$, отсюда $s(a^k - 1) \vdots m$, и, в силу взаимной простоты s и m, имеем $a^k - 1 \vdots m$. Доказано следующее утверждение.

Теорема 6 (Л. Эйлер, 1736 г.). *Если целое число a взаимно просто с натуральным числом m, то число $a^{\varphi(m)} - 1$ делится на m.*

Следствие (малая теорема Ферма). *Пусть p — простое число, a — целое число, не кратное p. Тогда $a^{p-1} - 1$ делится на p.*

Заметим, что в условиях малой теоремы Ферма $a^p - a$ делится на p, но последнее справедливо и при a, кратном p. В связи с этим часто под малой теоремой Ферма понимают следующее легко запоминаемое утверждение:

Если p — простое число, то для любого целого a число $a^p - a$ делится на p.

Малая теорема Ферма дает лишь *необходимое* условие простоты числа. Нечетное число $m \geqslant 3$ называют *условно простым по базе* a $(a = 2, 3, \ldots, m - 1)$, если $a^{m-1} \equiv 1 (\mathrm{mod}\, m)$. Простое число является условно простым по любой базе. Существуют, однако, составные числа m, являющиеся условно простыми по любой базе a, взаимно простой с m. Такие числа называют *числами Кармайкла*. Наименьшее из них — 561. В 1994 г. было доказано, что чисел Кармайкла бесконечно много.

В последние годы задача проверки простоты числа или — более широко — задача разложения числа на простые множители вновь приобрела актуальность в связи с проблемами создания надежных шифров (см. § 10).

§ 8. Линейные диофантовы уравнения

Диофантовым[3] называют уравнение в целых числах вида

$$P(x_1, \ldots, x_n) = 0,$$

где P — многочлен от n переменных с целыми коэффициентами. Предметом изучения в этом параграфе будет служить линейное диофантово уравнение с двумя неизвестными

$$ax + by = c, \tag{1}$$

где a, b и c — целые константы, а x и y — неизвестные, или переменные. Решением (более точно, *частным решением*) уравнения, как известно, называют набор значений переменных, обращающих его в верное равенство. Стоит задача описания всех решений уравнения (1) в целых числах.

Если один из коэффициентов при неизвестных равен нулю, то уравнение фактически содержит лишь одно неизвестное. Поэтому будем считать, что $a \neq 0$ и $b \neq 0$. Более того, при необходимости меняя знак переменной, можно без ограничения общности считать в этом случае, что $a > 0$ и $b > 0$. Пусть d — наибольший общий делитель a и b. Тогда для любых целых x и y левая часть уравнения $ax + by$ делится на d. Если при этом c не делится на d, то уравнение

[3] В честь древнегреческого математика Диофанта, жившего в III веке.

не имеет (целых) решений. Если же c кратно d, т. е. $c = c_1 d$ для некоторого целого c_1, то, положив $a = a_1 d$, $b = b_1 d$ и сократив на d, уравнение (1) сведем к виду

$$a_1 x + b_1 y = c_1,$$

в котором коэффициенты при неизвестных являются взаимно простыми числами.

Теорема 7. *Уравнение* (1) *с взаимно простыми коэффициентами при неизвестных разрешимо в целых числах.*

◄ Рассмотрим сначала уравнение

$$ax + by = 1. \tag{2}$$

Построим цепочку делений с остатком

$$\begin{aligned}
a &= bq_0 + r_1, && 0 < r_1 < b;\\
b &= r_1 q_1 + r_2, && 0 < r_2 < r_1;\\
r_1 &= r_2 q_2 + r_3, && 0 < r_3 < r_2;\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, && 0 < r_n < r_{n-1};\\
r_{n-1} &= r_n q_n.
\end{aligned}$$

Последний ненулевой остаток, как известно, равен наибольшему общему делителю a и b, т. е. $r_n = 1$. Заметим, что каждый остаток r_i может быть представлен целочисленной линейной комбинацией a и b: $r_i = \alpha_i a + \beta_i b$. Действительно,

$$\begin{aligned}
r_1 &= a - bq_0 = \alpha_1 a + \beta_1 b;\\
r_2 &= b - r_1 q_1 = b - (\alpha_1 a + \beta_1 b) q_1 = \alpha_2 a + \beta_2 b;\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
r_{i+1} &= r_{i-1} - r_i q_i = \alpha_{i-1} a + \beta_{i-1} b - (\alpha_i a + \beta_i b) q_1 = \alpha_{i+1} a + \beta_{i+1} b;\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
1 &= r_n = \alpha_n a + \beta_n b.
\end{aligned}$$

Последнее равенство показывает, что пара целых чисел (α_n, β_n) является решением (2). Очевидно, что пара целых чисел $(c\alpha_n, c\beta_n)$ — суть решение (1). Теорема доказана. ►

Пример 1. Найти какие-нибудь целые x и y, для которых

$$1000x + 73y = 1.$$

◄ Применив алгоритм Евклида к паре чисел 1000 и 73, получим цепочку равенств

$$1000 = 73 \cdot 13 + 51; \quad 73 = 51 \cdot 1 + 22; \quad 51 = 22 \cdot 2 + 7; \quad 22 = 7 \cdot 3 + 1,$$

из которых получаем

$$\begin{aligned}
1 &= 22 - 7 \cdot 3 = 22 - 3(51 - 2 \cdot 22) = 7 \cdot 22 - 3 \cdot 51 = 7(73 - 51) - 3 \cdot 51 =\\
&= 7 \cdot 73 - 10 \cdot 51 = 7 \cdot 73 - 10(1000 - 73 \cdot 13) = -10 \cdot 10\,000 + 137 \cdot 73.
\end{aligned}$$

Ответом в данной задаче может служить пара $(-10, 137)$. ►

Итак, мы теперь умеем находить *частное решение* уравнения (1) (в том случае, когда это диофантово уравнение разрешимо). О том, каким является *общее решение* (1) — множество всех (частных) решений, говорит

Теорема 8. *Пусть a и b — взаимно простые натуральные числа, (x_0, y_0) — некоторое решение диофантова уравнения* (1). *Тогда множество всех решений* (1) *описывается формулами*

$$x = x_0 + bt, \quad y = y_0 - at, \tag{3}$$

где $t \in \mathbb{Z}$.

◄ Очевидно, что для любого целого t значения x и y, определяемые формулами (3), дают решение (1). Действительно,

$$a(x_0 + bt) + b(y_0 - at) = ax_0 + by_0 = c,$$

так как (x_0, y_0) удовлетворяет (1) по условию теоремы.

Убедимся теперь в том, что *произвольное* решение (1) имеет вид (3) для некоторого целого t. Вычтя из (1) почленно равенство $ax_0 + by_0 = c$, получим равносильное уравнение $a(x - x_0) + b(y - y_0) = 0$, или

$$a(x - x_0) \vdots b(y_0 - y). \tag{4}$$

Из того, что $a(x - x_0)$ кратно b и a взаимно просто с b, следует $(x - x_0) \vdots b$, т. е. для некоторого целого t имеем $x - x_0 = bt$, или $x = x_0 + bt$. Подставив выражение для x в (4), получим $abt = b(y_0 - y)$ и, поскольку $b \neq 0$, справедливо равенство $y_0 - y = at$, или $y = y_0 - at$. Теорема доказана. ►

Пример 2. Общее решение рассматривавшегося выше уравнения $1000x + 73y = 1$ таково:

$$\{(-10 + 73t, 137 - 1000t) \mid t \in \mathbb{Z}\}.$$

§ 9. Мультипликативные функции

Функция натурального аргумента $\theta(n)$ называется *мультипликативной*, если для любых взаимно простых чисел m и n выполняется равенство

$$\boxed{\theta(m \cdot n) = \theta(m) \cdot \theta(n).}$$

Простейшими примерами мультипликативных функций являются степенная функция $\theta(n) = n^\alpha$ и постоянные функции $\theta(n) = 1$ и $\theta(n) = 0$. Заметим, что $\theta(1) = \theta(1 \cdot 1) = \theta(1) \cdot \theta(1)$, откуда $\theta(1)$ может быть равно 1 или 0. В последнем случае $\forall\, n\ \theta(n) = \theta(n \cdot 1) = \theta(n) \cdot 0 = 0$. Чтобы исключить возможность тождественного равенства нулю, иногда в определение мультипликативной функции включают дополнительное требование: $\theta(1) = 1$.

Пусть $n_1, n_2, \ldots, n_k$ — попарно взаимно простые числа. Индукцией легко доказать, что для любой мультипликативной функции справедливо соотношение

$$\boxed{\theta(n_1 \cdot n_2 \cdot \ldots \cdot n_k) = \theta(n_1) \cdot \theta(n_2) \cdot \ldots \cdot \theta(n_k).}$$

До конца этого параграфа будем считать, что n имеет каноническое разложение

$$n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}.$$

Докажем сначала мультипликативность функции Эйлера (определение см. § 6). Пусть m и n — взаимно простые числа. Чтобы подсчитать количество чисел, не превосходящих mn и взаимно простых с mn, расположим все числа от 1 до mn в виде следующей таблицы (табл. 1).

Таблица 1

1	2	3	...	n
$n+1$	$n+2$	$n+3$	...	$2n$
$2n+1$	$2n+2$	$2n+3$	...	$3n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$(m-1)n+1$	$(m-1)n+2$	$(m-1)n+3$	...	mn

Любое натуральное число взаимно просто с mn тогда и только тогда, когда оно взаимно просто и с m, и с n (в силу взаимной простоты чисел m и n). Числа из каждого фиксированного столбца таблицы попарно сравнимы по модулю n; поэтому можно оставить в таблице только столбцы, первые элементы которых взаимно просты с n, не потеряв при этом ни одного интересующего нас числа. Число таких столбцов есть $\varphi(n)$. Элементы каждого столбца в силу леммы 4 образуют полную систему вычетов по модулю m. Поэтому ровно $\varphi(m)$ элементов каждого столбца взаимно просты с m. Таким образом, всего имеется $\varphi(n)\cdot\varphi(m)$ чисел не больше mn и взаимно простых с mn, т. е. $\varphi(mn) = \varphi(m)\cdot\varphi(n)$, что и требовалось доказать.

Используя свойство мультипликативности, нетрудно вывести формулу для вычисления $\varphi(n)$ [4]. Поскольку $\varphi(n) = \varphi(p_1^{k_1}) \cdot \varphi(p_2^{k_2}) \cdot \dots \cdot \varphi(p_s^{k_s})$, достаточно научиться вычислять функцию Эйлера от степени простого числа. Для этого заметим, что если p — простое число, то среди любых p последовательных натуральных чисел ровно $p-1$ чисел взаимно просты с p, а также с любой степенью p. Поэтому $\varphi(p^k) = \varphi(p\cdot p^{k-1}) = (p-1)\cdot p^{k-1}$. Таким образом,

$$\varphi(n) = \prod_{i=1}^{s} \varphi(p_i^{k_i}) = \prod_{i=1}^{s} (p_i - 1)\cdot p_i^{k_i-1} = \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right)\cdot p_i^{k_i} = n \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right).$$

Пример 1. $\varphi(24) = 24 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 8.$

Рассмотрим еще несколько задач, при решении которых возникают мультипликативные функции.

1) Найти $\tau(n)$ — число различных делителей натурального числа n (включая 1 и n).

[4] Ниже (§ 8 гл. LXVIII) будет показан еще один способ получения указанной формулы.

Общий вид делителя n имеет вид

$$d = p_1^{r_1} p_2^{r_2} \dots p_s^{r_s},$$

где для каждого i показатель степени r_i принимает значения $0, 1, \dots, k_i$. Произвольный делитель числа n можно построить в результате выполнения процедуры из s действий, где i-е действие состоит в выборе r_i — показателя степени простого числа p_i. Поскольку i-е действие может быть выполнено $k_i + 1$ способами, применение правила произведения дает

$$\boxed{\tau(n) = (k_1 + 1)(k_2 + 1) \dots (k_s + 1) = \prod_{i=1}^{s} (k_i + 1).}$$

Пример 2.

1) $\tau(2^3 \cdot 3^4 \cdot 5^6) = 4 \cdot 5 \cdot 7 = 140.$
2) $\tau(2^3 \cdot 3^4 \cdot 4^5) = \tau(2^{13} \cdot 3^4) = 14 \cdot 5 = 70.$

2) Найти $\sigma(n)$ — сумму всевозможных делителей числа n.

Покажем, что

$$\sigma(n) = (1 + p_1 + p_1^2 + \dots + p_1^{k_1})(1 + p_2 + p_2^2 + \dots + p_2^{k_2}) \dots (1 + p_s + p_s^2 + \dots + p_s^{k_s}).$$

Действительно, раскрывая скобки и не меняя при этом порядка множителей, получим

$$\sigma(n) = 1 \cdot 1 \cdot \dots \cdot 1 + 1 \cdot 1 \cdot \dots \cdot p_s + \dots + p_1^{k_1} p_2^{k_2} \cdot \dots \cdot p_s^{k_s}$$

— сумму всех делителей n. С помощью формулы суммы членов геометрической прогрессии получаем компактную формулу

$$\boxed{\sigma(n) = \prod_{i=0}^{s} \frac{p_i^{k_i+1} - 1}{p_i - 1}.}$$

Пример 3.

1) $\sigma(12) = \sigma(2^2 \cdot 3) = \dfrac{2^3 - 1}{2 - 1} \cdot \dfrac{3^2 - 1}{3 - 1} = 7 \cdot 4 = 28.$
2) $\sigma(60) = \sigma(12) \cdot \sigma(5) = 28 \cdot 6 = 168.$

3) Функция Мёбиуса $\mu(n)$ вводится следующими соотношениями:

- $\mu(1) = 1$;
- если n делится на какой-нибудь точный квадрат > 1, т. е. для некоторого i выполняется $k_i > 1$, то $\mu(n) = 0$;
- если же все показатели степени k_i равны 1, т. е. $n = p_1 \cdot p_2 \cdot \dots \cdot p_s$ (где $p_1, p_2, \dots, p_s$ — различные простые числа)[5], то $\mu(n) = (-1)^s$.

Проверка мультипликативности функций $\tau(n)$, $\sigma(n)$, $\mu(n)$ проводится непосредственной подстановкой.

[5] В этом случае говорят, что число n *свободно от квадратов*.

§ 10. Система РША

В этом параграфе будет показано, какое применение нашли некоторые классические результаты теории чисел к решению проблемы создания надежных шифров — проблемы чрезвычайно актуальной в эпоху массового распространения телекоммуникаций.

Системой тайнописи с открытым ключом (*public key cryptosystem*) называют такую систему шифрования и дешифрования информации, которая удовлетворяет следующим двум условиям:

- *получатель информации* публикует алгоритм шифрования для всеобщего сведения;
- алгоритм дешифрования известен только получателю информации (держится им в секрете) и *практически* (с помощью вычислительной техники) не может быть раскрыт.

Шифрующий и дешифрующий алгоритмы называют соответственно *открытым* и *закрытым* ключом.

Идея подобной системы тайнописи была высказана в 1975 г., эффективная реализация идеи была предложена в 1977 г. тремя американскими математиками: Р. Райвестом, А. Шамиром и Л. Адлеманом; первые буквы их имен[6] составили имя придуманной ими системы. Описание РША-системы предварим некоторыми соображениями, связанными с общей идеей тайнописи с открытым ключом.

Всякое сообщение, передаваемое с помощью компьютера по электронным сетям, может быть представлено в виде элемента некоторого числового множества S. Пусть $x \in S$; результат шифровки x (*шифрограмму*) обозначим $y = f(x)$, где f — функция, задаваемая алгоритмом шифровки. Удобно считать, что y тоже принадлежит S; при этом функция f должна осуществлять взаимно однозначное отображение S на себя (разным сообщениям должны соответствовать разные шифрограммы, и наоборот), таким образом, функция f должна осуществлять некоторую перестановку элементов S (т. е. f — *подстановка*, действующая на множестве S). Дешифрующий алгоритм состоит в применении обратной подстановки f^{-1} к шифрограмме $y \in S$: $x = f^{-1}(y)$. Если множество содержит n элементов, то на нем определено $n!$ различных подстановок. *Теоретически* можно найти обратную подстановку f^{-1}, вычислив $f(x)$ для всех $x \in S$. Если, к примеру, S состоит из всех последовательностей 200 десятичных цифр, то $n = 10^{200}$, и реализовать предложенный алгоритм за обозримое время невозможно; знание открытого ключа не дает, таким образом, *практической* возможности найти закрытый ключ.

Покажем, как решается в предложенной системе тайнописи *проблема электронной подписи*. Предположим, что имеется группа бизнесменов, которым требуется сообщать друг другу сведения, составляющие коммерческую тайну. Каждый бизнесмен придумывает свой алгоритм шифрования (*прямой алгоритм*); при этом он знает и *обратный алгоритм*. Участники группы издают специальный справочник, в котором приводят полностью все прямые алгоритмы (обратные алгоритмы держатся в секрете). К справочнику имеет доступ любой желающий. Пользуясь справочником, можно послать сообщение любому члену группы, например, Z,

[6] В оригинале — RSA (Rivest, Shamir, Adleman).

зашифровав сообщение с помощью (прямого) алгоритма f_Z. Понять это сообщение сможет только Z, поскольку только он знает обратный алгоритм f_Z^{-1}. Теперь допустим, что бизнесмен A хочет *подписать* свое сообщение, т. е. добиться того, чтобы у Z не было сомнений в том, кто действительный автор сообщения. Тогда бизнесмен A шифрует свое сообщение x дважды: сначала с помощью своего обратного алгоритма f_A^{-1}, а затем полученная шифрограмма шифруется еще раз с помощью прямого алгоритма f_Z. В результате Z получает шифрограмму $y = f_Z(f_A^{-1}(x))$. Для того чтобы восстановить исходное сообщение, Z применяет свой обратный алгоритм f_Z^{-1}, а затем (всем известный) прямой алгоритм f_A: $f_A(f_Z^{-1}(y)) = x$. Теперь бизнесмен Z знает, что только A мог послать ему этот дважды зашифрованный текст, так как при шифровании был использован секретный алгоритм бизнесмена A.

Описание системы РША

Множество S составляют натуральные числа, меньшие некоторого натурального числа m и взаимно простые с ним; таким образом, S — приведенная система вычетов по модулю m. Функция $f(x)$ вычисляет остаток от деления x^k на m; при этом показатель степени k должен быть взаимно простым с $\varphi(m)$ ($\varphi(m)$ — функция Эйлера). Числа k и m составляют открытый ключ. В качестве закрытого ключа используется такое число k', что $k \cdot k' \equiv 1 (\mathrm{mod}\, \varphi(m))$. Пусть $y \equiv x^k (\mathrm{mod}\, m)$ и $0 \leqslant y < m$. Тогда

$$y^{k'} \equiv x^{k \cdot k'} \equiv x^{1+s \cdot \varphi(m)} \equiv x \cdot (x^{\varphi(m)})^s \equiv x (\mathrm{mod}\, m),$$

так как по теореме Эйлера $x^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$ при взаимно простых x и m.

Зная разложение m на множители, легко вычислить $\varphi(m)$. Покажем, как по $\varphi(m)$ найти k'. Рассмотрим диофантово уравнение

$$kx + \varphi(m)y = 1.$$

Коэффициенты при неизвестных x и y по условию взаимно просты, поэтому уравнение разрешимо, а его общее решение имеет вид

$$x = x_0 + \varphi(m)t, \quad y = y_0 - kt,$$

где t — произвольное целое число, а (x_0, y_0) — некоторое частное решение уравнения. Ясно, что при некотором t число x будет положительно и может быть выбрано в качестве k', так как $kx \equiv 1 (\mathrm{mod}\, \varphi(m))$.

Как правило, в качестве m берут произведение двух (многозначных) простых чисел: $m = pq$, тогда $\varphi(m) = (p-1)(q-1)$.

В оригинальной публикации (1977 г.) о методе РША p и q были соответственно 64- и 65-значными числами. Авторы опубликовали зашифрованный текст из 129 цифр и открытый ключ (128-значное число m и $k = 9007$), предложив 100 долларов тому, кто первый расшифрует текст. Существовавшие в то время алгоритмы разложения числа на простые множители (а также быстродействие вычислительной техники) не позволяли найти разложение 129-значного числа m за разумное время.

Лишь спустя 17 лет с помощью метода *квадратичного решета* указанное 129-значное число было разложено на множители, что потребовало девятимесячной работы примерно 1600 компьютеров, объединенных сетью Интернет.

Ныне для выбора p и q рекомендуют 200-значные числа.

В заключение остановимся на технике вычисления остатка от деления x^k на m. Эта операция не столь трудоемка, как может показаться на первый взгляд. С помощью двоичного представления числа k

$$k = \sum_{i=0}^{s} b_i 2^i$$

получим, что

$$x^k \equiv \prod_{b_i \neq 0} x^{2^i} \pmod{m}.$$

Количество умножений (по модулю m) при вычислении степеней числа x

$$x, x^2, x^4, x^8, \ldots, x^{2^s}$$

равно s (каждое число в этой последовательности, начиная со второго, получается из предыдущего возведением в квадрат). При вычислении ранее приведенного произведения понадобится не более s умножений. Таким образом, общее число умножений не превосходит $2s$, где $s \leqslant \log_2 k$. Например, при вычислении 9007-й степени понадобится 20 умножений (двоичное представление 9007: 10001100101111).

Упражнения

1. Является ли число 57 599 простым?
2. Найти наибольший общий делитель чисел
   1) 321 и 843; 2) 2166 и 6099; 3) 6787 и 7194; 4) 23 521 и 75 217.
3. Пусть r_n — n-значное число $11\ldots1$. Доказать: $(r_n, r_m) = r_{(n,m)}$.
4. Показать, что простое число p является делителем $n!$ с кратностью $\sum\limits_{k \geqslant 1} \dfrac{n}{p^k}$.
5. Записать 20! в виде произведения степеней простых чисел.
6. Найти остаток от деления
   1) 6^{100} на 7; 2) 6^{100} на 35; 3) $10^{10} + 10^{100} + 10^{1000} + \ldots + 10^{10^{10}}$ на 7.
7. Доказать, что
   1) $30^{99} + 61^{100}$ делится на 31;
   2) $43^{101} + 23^{101}$ делится на 66;
   3) $11^{10} - 1$ делится на 100;
   4) $7^{120} - 1$ делится на 143.
8. Пусть k и n — натуральные числа. Доказать, что $k^{n+2} + (k+1)^{2n+1}$ делится на $k^2 + k + 1$.
9. Доказать, что если сумма квадратов двух целых чисел делится на 3, то и каждое из них делится на 3.
10. Доказать, что если сумма квадратов двух целых чисел делится на 7, то и каждое из них делится на 7.
11. Пусть $n \equiv 2 \pmod 3$, $n \equiv 3 \pmod 5$. Найти остаток от деления n на 15.
12. Выяснить, при каких $k \leqslant 11$ сумма квадратов k последовательных натуральных чисел может быть квадратом натурального числа.

13. Найти остаток от деления

1) 2^{100} на 101; 2) 3^{102} на 101; 3) 8^{900} на 29; 4) 7^{120} на 143.

14. Доказать, что для любого натурального n число $n^{73} - n^{37}$ делится на 10.

15. Доказать, что если n не делится на 17, то либо $n^8 - 1$, либо $n^8 + 1$ делится на 17.

16. Решить в целых числах уравнения:

1) $16x + 4y = 1830$; 2) $13x + 7y = 1$; 3) $21x + 19y = 5$; 4) $1994x - 171y = 1$.

17. Даша гадает на ромашке: «Любит — не любит — плюнет — поцелует — к сердцу прижмет — к черту пошлет». Глаша при гадании к этим шести вариантам добавляет еще один: «своей назовет». На ромашках с n и $2n$ лепестками у Даши хорошее предсказание, а у Глаши плохое. Чему равно n, если считать, что на ромашке не может быть более 100 лепестков?

18. На клетчатой бумаге нарисован прямоугольник. Количество его клеток, примыкающих к границе прямоугольника, равно количеству остальных его клеток. Найти размеры прямоугольника.

19. Доказать, что произведение мультипликативных функций мультипликативно.

20. Найти количество чисел, не превосходящих m и взаимно простых с m для $m =$ 25, 60, 250, 1 000 000.

21. Сколько существует правильных несократимых дробей со знаменателем 288?

Ответы

1. $57\,599 = 240^2 - 1 = 239 \cdot 241$. **2.** 1) 3; 2) 57; 3) 11; 4) 1. **5.** $2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$. **6.** 1) 1; 2) 1; 3) 5. В последнем примере имеем: $10^{10} \equiv 3^{10} = 9^5 \equiv 2^5 \equiv 4 (\mathrm{mod}\, 7)$; $10^{100} = (10^{10})^{10} \equiv 4^{10} \equiv (-3)^{10} \equiv 3^{10} \equiv 4 \bmod 7$. Далее по индукции легко доказать, что $\forall k$ $10^{10^k} \equiv 4 (\mathrm{mod}\, 7)$. **11.** 8. **12.** При $k = 2$ и 11. **13.** 1) 1; 2) $3^{102} = 3^{100} \cdot 3^2 \equiv 9 (\mathrm{mod}\, 101)$; 3) $8^{900} = 8^{28 \cdot 32} \cdot 8^4 \equiv 8^4 \equiv 6^2 \equiv 7 (\mathrm{mod}\, 29)$; 4) 1. **16.** 1) Решений нет; 2) $x = -1 + 7t$, $y = 2 - 13t$, $t \in \mathbb{Z}$; 3) $x = -7 + 19t$, $y = 8 - 21t$, $t \in \mathbb{Z}$; 4) $x = 56 + 171t$, $y = 653 + 1994t$, $t \in \mathbb{Z}$. **17.** 17. **18.** 12×5 или 8×6. **20.** 20, 16, 100, 400 000. **21.** 96.

Глава LXVII

НАЧАЛЬНЫЕ ПОНЯТИЯ ОБЩЕЙ АЛГЕБРЫ

С простейшими алгебраическими операциями — арифметическими действиями над числами — мы встречаемся еще в начальной школе, но об алгебре говорим только тогда, когда приступаем к решению задач, содержащих буквенные переменные — известные и неизвестные. Тождественные преобразования буквенных выражений, решение алгебраических уравнений, где под буквами понимаются действительные или комплексные числа, составляют содержание *элементарной алгебры*. Одна из основных проблем здесь — решение уравнения n-ой степени в радикалах

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0,$$

т. е. задача отыскания формул, выражающих корни уравнения через его коэффициенты при помощи простых арифметических операций — сложения, вычитания, умножения и деления — и процедур извлечения корней. Например, для уравнения второй степени $a_2 x^2 + a_1 x + a_0 = 0$ эти формулы имеют вид

$$x_1 = \frac{-a_1 - \sqrt{a_1^2 - 4a_2 a_0}}{2a_2}, \qquad x_2 = \frac{-a_1 + \sqrt{a_1^2 - 4a_2 a_0}}{2a_2}.$$

Похожие формулы есть и для уравнений третьей (формула Кардано) и четвертой (формула Феррари) степени. Однако для уравнений, степень которых выше четвертой, подобные формулы, вообще говоря, получить нельзя. Этот результат, опубликованный Нильсом Хенриком Абелем в 1824 году, не приостановил попыток исследования уравнений высших степеней. К этому времени уже было известно, что всякое уравнение n-ой степени с комплексными коэффициентами имеет ровно n комплексных корней, и усилия математиков были направлены на описание классов уравнений, для которых решение все-таки может быть получено в радикалах, и на установление условий, обеспечивающих подобную разрешимость. Эта задача была блестяще решена молодым французским математиком Эваристом Галуа, чьи результаты стали известны широкой математической общественности в 1830 году (полное изложение результатов Галуа было дано Жозефом Лиувиллем в 1846 году).

Работа Галуа стала основой новой алгебраической идеологии — он перенес центр тяжести исследования (в данном случае задачи решения уравнений) с собственно задачи на методы ее решения. Введенные им при этом понятия *группы*,

поля, *композиционного ряда* и др. надолго определили пути развития алгебры. В частности, понятие группы оказалось столь плодотворным в разных областях математики (в геометрии — группы преобразований, в теории чисел — группы вычетов, в линейной алгебре — группы матриц, в топологии — гомологические группы) и естествознания (группы симметрий в кристаллографии и квантовой механике), что стало одним из центральных объектов приложения сил математиков различных направлений.

Дальнейший прогресс в алгебре связан с распространением понятия *алгебраической операции* с чисел на объекты нечисловой природы — элементы абстрактных групп, матрицы, кватернионы, подстановки и т. п. Все это привело к постепенному переносу интересов алгебраистов с исследования конкретных объектов (уравнений, систем уравнений и т. д.) на абстрактные — группы, кольца, поля, модули — и на изучение произвольных алгебраических операций.

Именно абстрактные алгебраические операции и абстрактные алгебраические системы являются предметом изучения современной алгебры, которая окончательно сформировалась в первой половине XX столетия под влиянием работ Д. Гильберта, Э. Артина, О. Ю. Шмидта, Б. Л. Ван-дер Вардена, А. И. Мальцева, Дж. Биркгофа и др.

§ 1. Отношения

Понятие *отношения* в математике служит для теоретико-множественного описания связей между элементами множеств.

Пусть A — некоторое множество с элементами $\{a, b, \ldots\}$. Рассмотрим декартов квадрат этого множества $A \times A = \{(a, b) \mid a \in A,\ b \in A\}$ — множество упорядоченных пар элементов множества A.

Пусть $\mathcal{R}$ — некоторое подмножество множества $A \times A$. Мы будем говорить, что *элемент $a \in A$ находится в отношении $\mathcal{R}$ с элементом $b \in A$* и записывать это как $a\mathcal{R}b$ или $\mathcal{R}(a, b)$ в том случае, когда $(a, b) \in \mathcal{R}$.

Множество $\mathcal{R} \subset A \times A$ при этом называется *двуместным* (или *бинарным*) *отношением на множестве A*.

Рассмотрим несколько примеров, иллюстрирующих понятие бинарного отношения.

Отношение *«не больше»*. Пусть $A = \mathbb{R}$ — множество действительных чисел. В этом случае декартов квадрат $A \times A = \mathbb{R} \times \mathbb{R}$ можно отождествить с плоскостью $\mathbb{R}^2$. Положим $\mathcal{R} = \{(a, b) \in \mathbb{R}^2 \mid a \leqslant b\}$. В этом случае множество $\mathcal{R}$ задает на множестве действительных чисел отношение порядка — число a находится в отношении «не больше» с элементом b тогда и только тогда, когда $a \leqslant b$.

Отношение *сравнимости по модулю m* изучалось в § 5.

Отношение *«функция»*. Пусть $A = \mathbb{R}$ — множество действительных чисел, а $f : \mathbb{R} \to \mathbb{R}$ — некоторая функция. Положим $\mathcal{R} = \{(a, b) \in \mathbb{R}^2 \mid b = f(a)\}$. Это отношение задает функциональную связь между числами a и b: если $a\mathcal{R}b$, то это означает, что $b = f(a)$. Важнейшими бинарными отношениями являются отношения эквивалентности, порядка, и функциональные отношения[1]. Первые

[1] Примером отношения эквивалентности может служить отношение сравнимости по модулю m; примером отношения порядка — отношение «не больше».

два типа отношений будут определены и рассмотрены ниже, а здесь мы определим только функциональные отношения.

Бинарное отношение $\mathcal{R}$ называется *функциональным*, если из $a\mathcal{R}b$ и $a\mathcal{R}c$ следует $b = c$. Т.е. каждому элементу a, стоящему на первом месте в отношении, отвечает не более одного элемента, который может быть поставлен на второе место. Легко видеть, что всякое функциональное отношение определяет некоторую функцию посредством задания ее графика.

Свойства отношений

Отношение на множестве A называют

- *рефлексивным*, если для любого элемента $a \in A$ выполняется $a\mathcal{R}a$;
- *антирефлексивным*, если для любого элемента $a \in A$ не выполняется $a\mathcal{R}a$;
- *симметричным*, если для любых $a, b \in A$ из $a\mathcal{R}b$ следует $b\mathcal{R}a$;
- *антисимметричным*, если из $a\mathcal{R}b$ и $b\mathcal{R}a$ следует, что $a = b$;
- *транзитивным*, если условия $a\mathcal{R}b$ и $b\mathcal{R}c$ влекут $a\mathcal{R}c$.

Таблица 1

множество	$\mathbb{R}$	$\mathbb{R}$	$\mathbb{R}$	$\mathbb{N}$	$\mathbb{N}$	L	L	P	P
отношение	$=$	$\leqslant$	$<$	$\vdots$	$\equiv (\mathrm{mod}\, m)$	$\parallel$	$\perp$	сын	земляк
рефлексивность	+	+	−	+	+	+	−	−	+
антирефлексивность	−	−	+	−	−	−	+	+	−
симметричность	+	−	−	−	+	+	+	−	+
антисимметричность	+	+	+	+	−	−	−	+	−
транзитивность	+	+	+	+	+	+	−	−	+

Свойства отношений будем иллюстрировать на следующих примерах. На множестве действительных чисел $\mathbb{R}$ рассмотрим отношения $=, \leqslant, <$. На множестве натуральных чисел $\mathbb{N}$ — отношения делимости $\vdots$ и отношение $\equiv (\mathrm{mod}\, m)$ (отношение сравнимости по модулю m). На множестве прямых плоскости L — отношения параллельности $\parallel$ и перпендикулярности $\perp$. На множестве людей P — отношения «сын» и «земляк». В табл. 1 указано, какими свойствами обладают эти отношения.

§ 2. Отношение эквивалентности

Отношение, обладающее свойствами рефлексивности, симметричности и транзитивности, называют *отношением эквивалентности*. Из отношений, рассматривавшихся в предыдущем параграфе, таким свойством обладают отношения равенства чисел, сравнимости по модулю m натуральных чисел, параллельности прямых, а также отношение «земляк» на множестве людей.

Напомним понятие разбиения множества.

Семейство непустых подмножеств непустого множества A называют разбиением множества A, если выполняются следующие свойства:

1) объединение этих подмножеств совпадает с A;
2) подмножества попарно не пересекаются.

Пусть $\mathcal{R} \subset A^2$ — отношение эквивалентности. Множество $\bar{a} = \{x \in A \mid x\mathcal{R}a\}$ называют *классом эквивалентности.*

Теорема 1. *Различные классы эквивалентности образуют разбиение множества A.*

◄ Во-первых, каждый элемент $a \in A$ попадает в некоторый класс эквивалентности (выполнено первое свойство разбиения). Действительно, в силу рефлексивности имеем $a\mathcal{R}a$, откуда $a \in \bar{a}$. Осталось проверить, что различные (т. е. несовпадающие как множества) классы эквивалентности не пересекаются.

Итак, пусть $\bar{a} \neq \bar{b}$. Докажем, что $\bar{a} \cap \bar{b} = \varnothing$.

Предположим (для приведение к противоречию), что найдется такой элемент $y \in A$, который одновременно принадлежит $\bar{a}$ и $\bar{b}$. Поскольку $y \in \bar{a}$, имеем $y\mathcal{R}a$ и, в силу свойства симметричности отношения $\mathcal{R}$, $a\mathcal{R}y$. Из того, что $y \in \bar{b}$, следует $y\mathcal{R}b$. Соотношения $a\mathcal{R}y$ и $y\mathcal{R}b$ влекут (в силу транзитивности $\mathcal{R}$) $a\mathcal{R}b$, откуда вытекает (вследствие симметричности $\mathcal{R}$), что $b\mathcal{R}a$. Теперь уже легко убедиться в том, что $\bar{a} = \bar{b}$. Действительно, если x — произвольный элемент $\bar{a}$, то $x\mathcal{R}a$ и (так как $a\mathcal{R}b$) $x\mathcal{R}b$, т. е. $x \in \bar{b}$. Доказано, что $\bar{a}$ — подмножество $\bar{b}$. Аналогично устанавливается, что $\bar{b} \subset \bar{a}$. Таким образом, $\bar{a} = \bar{b}$. Получили противоречие.

Теорема доказана. ►

Теорему 1 можно обратить. Справедлива

Теорема 2. *Всякое разбиение множества порождает на нем отношение эквивалентности.*

◄ Это отношение задается так:

$$a\mathcal{R}b \Leftrightarrow (a \text{ и } b \text{ принадлежат одному подмножеству разбиения}).$$

Очевидно, что при этом для $\mathcal{R}$ выполняются свойства рефлексивности, симметричности и транзитивности, т. е. это отношение действительно является отношением эквивалентности. ►

§ 3. Отношения порядка

Отношение называют отношением *нестрогого порядка*, если оно рефлексивно, транзитивно и антисимметрично.

Отношениями нестрогого порядка являются отношения $\leqslant, =$ на множестве $\mathbb{R}$, отношение делимости $\vdots$ на множестве $\mathbb{N}$. Приведем еще один пример.

Пусть A — некоторое множество; $\beta(A) = \{X \mid X \subset A\}$ — множество всех его подмножеств[2]. Отношение $\subset$ — отношение нестрогого порядка на $\beta(A)$.

Отношение называют отношением *строгого порядка*, если оно антирефлексивно, транзитивно и антисимметрично.

Примером такого отношения является отношение $<$ на $\mathbb{R}$.

Отношения строгого или нестрогого порядка называют отношениями *порядка*.

Говорят, что элементы a и b сравнимы по отношению $\mathcal{R}$, если имеет место по крайней мере одно из соотношений: $a\mathcal{R}b$ или $b\mathcal{R}a$.

Пример. Рассмотрим отношение $\vdots$ на множестве натуральных чисел. 100 и 25, 2 и 6 сравнимы по этому отношению, а числа 16 и 31 не сравнимы.

Множество с введенным на нем отношением порядка называется *линейно упорядоченным*, если любые два его элемента сравнимы по данному отношению, и *частично упорядоченным* в противном случае.

Например, множество $\mathbb{R}$ линейно упорядочено по отношению $\leqslant$, а множество $\mathbb{N}$ частично упорядочено по отношению $\vdots$.

§ 4. Алгебраические структуры. Группа

Отображение $\alpha : A^n \to A$ называют n-арной *алгебраической операцией* на множестве A. При $n = 1$ используют термин *унарная* операция, а при $n = 2$ — *бинарная* операция.

Примерами унарной и бинарной операций на множестве действительных чисел могут служить соответственно операция смены знака и операция сложения.

Множество A вместе с заданными на нем алгебраическими операциями $\alpha_1, \alpha_2, \ldots, \alpha_n$ называют *алгебраической структурой* $\langle A; \alpha_1, \alpha_2, \ldots, \alpha_n\rangle$.

Пусть G — множество, на котором задана бинарная операция $*$[3], обладающая следующими свойствами (*аксиомы группы*):

(G1) $\forall\, a, b \in G \quad a * b \in G$ (т.е. операция $*$ всюду определена)[4];

(G2) $\forall\, a, b, c \in G \quad (a * b) * c = a * (b * c)$ (*ассоциативность*)[5];

(G3) $\exists\, e \in G \quad \forall\, a \in G \; a * e = e * a = a$ (*существование нейтрального элемента*);

(G4) $\forall\, a \in G \quad \exists\, a' \in G \; a' * a = a * a' = e$ (*существование обратного элемента*).

Тогда алгебраическая структура $\langle G, *\rangle$ называется *группой*.

Если, кроме того, выполняется условие *коммутативности*

(G5) $\forall\, a, b \in G \quad a * b = b * a$,

то группу называют *коммутативной* или *абелевой*.

Особенности терминологии (и обозначений) по отношению к группам, в которых (групповую) операцию называют сложением или умножением, отражены в табл. 2.

---

[2] $\beta(A)$ называют *булеаном* множества A.

[3] Результат действия операции на пару элементов (a, b) удобно записывать в *инфиксной форме*: $a * b$.

[4] Говорят также: множество G *замкнуто* относительно данной операции, т.е. операция $*$ над элементами G не выводит за пределы G.

[5] В силу этого свойства выражения вида $a * b * c$ или $a_1 * a_2 * \ldots * a_n$ понимаются однозначно, т.е. от расстановки скобок результат не зависит.

Таблица 2

операция	сложение	умножение
название группы	аддитивная	мультипликативная
нейтральный элемент (e)	нулевой $(0, O)$	единичный $(1, I, E)$
обратный к a элемент (a')	противоположный $(-a)$	обратный (a^{-1})

Примеры групп

1. $\langle \mathbb{Z}, + \rangle$ — аддитивная группа целых чисел.
2. $\langle \mathbb{R}\backslash\{0\}, \cdot \rangle$ — мультипликативная группа действительных чисел без нуля. Заметим, что алгебраическая структура $\langle \mathbb{Z}\backslash\{0\}, \cdot \rangle$ группой не является (не выполняется свойство **(G4)**.
3. Пусть $Z_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$ — множество классов вычетов по модулю m. Тогда $\langle Z_m, + \rangle$ — аддитивная группа.

   Остановимся на этой группе поподробнее. Во-первых, нужно определить групповую операцию. Положим: $\bar{a} + \bar{b} = \overline{a+b}$. Для проверки корректности этого определения нужно убедиться в том, что класс вычетов, объявляемый суммой классов вычетов $\bar{a}$ и $\bar{b}$, не зависит от того, какие представители слагаемых классов берутся. Пусть $a_1 \in \bar{a}$ и $b_1 \in \bar{b}$. Тогда $a_1 \equiv a (\mathrm{mod}\, m)$ *и* $b_1 \equiv b (\mathrm{mod}\, m)$. *По свойству сравнений* $a_1 + b_1 \equiv a + b (\mathrm{mod}\, m)$, т. е. $\overline{a_1} + \overline{b_1} = \overline{a+b}$, что и требовалось. Ассоциативность сложения очевидна. Нулевым элементом в данной группе будет класс $\bar{0}$. Противоположным элементом к $\bar{a}$ будет класс вычетов $\overline{-a}$.

   $\langle Z_m; + \rangle$ — пример конечной группы; эта группа абелева и содержит m элементов.
4. $\langle Z_p\backslash\{\bar{0}\}, \cdot \rangle$ (p — простое число) — мультипликативная группа классов вычетов по модулю p.

   Так же, как и выше, проверяется корректность определения произведения классов вычетов: $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$. В роли единичного элемента, как легко видеть, выступает $\bar{1}$. Для того чтобы найти класс вычетов $\bar{x}$, обратный к $\bar{a}$ (где a не кратно p), т. е. такой, что $\bar{x} \cdot \bar{a} = \bar{1}$ [6], нужно решить сравнение $ax \equiv 1 (\mathrm{mod}\, p)$, которое сводится к диофантову уравнению $ax - py = 1$. В данном уравнении коэффициенты при неизвестных a и p взаимно просты, так как p — простое число и a не кратно p; по теореме 7 это уравнение разрешимо в целых числах.

Отображение $\varphi : G \to \widehat{G}$ называется *гомоморфизмом* групп $\langle G, * \rangle$ и $\langle \widehat{G}, \widehat{*} \rangle$, если это отображение *сохраняет групповую операцию*, т. е.

$$\forall\, g_1, g_2 \in G \quad \varphi(g_1 * g_2) = \varphi(g_1)\, \widehat{*}\, \varphi(g_2).$$

[6] В силу очевидного свойства коммутативности умножения свойство $\bar{a} \cdot \bar{x} = \bar{1}$ в этом случае также будет выполняться.

Примеры гомоморфизмов

1. $\varphi : Z_9 \to Z_3$, где
$$\varphi(\overline{0}) = \overline{0}, \quad \varphi(\overline{1}) = \varphi(\overline{4}) = \varphi(\overline{7}) = \overline{1}, \quad \varphi(\overline{2}) = \varphi(\overline{5}) = \varphi(\overline{8}) = \overline{2}.$$
2. Функция ln осуществляет гомоморфное отображение мультипликативной группы положительных чисел $\langle \mathbb{R}^+, \cdot \rangle$ на аддитивную группу действительных чисел $\langle \mathbb{R}, + \rangle$. Действительно, $\forall\, x, y > 0$ $\ln(x \cdot y) = \ln x + \ln y$.

Взаимно однозначный гомоморфизм называют *изоморфизмом*. Очевидно, что из только что приведенных примеров лишь второй является также примером изоморфизма групп.

В заключение данного параграфа установим некоторые

Простейшие свойства групп

1. *Группа имеет ровно один нейтральный элемент.*
Действительно, пусть имеется два нейтральных элемента e_1 и e_2. Тогда в силу аксиомы **(G3)** имеем $e_1 = e_1 * e_2 = e_2$, т. е. любые два нейтральных элемента совпадают.
2. *Обратный элемент к элементу группы определяется единственным образом.*
В самом деле, предположим, что a'_1 и a'_2 — элементы, обратные к a. Тогда по аксиомам **(G4)** и **(G3)** одновременно имеем
$$a'_1 * (a * a'_2) = a'_1 * e = a'_1; \quad (a'_1 * a) * a'_2 = e * a'_2 = a'_2,$$
откуда в силу ассоциативности $a'_1 = a'_2$.
3. *Элемент, обратный к произведению элементов группы, есть произведение обратных к ним элементов, взятых в другом порядке:* $(a * b)' = b' * a'$.
Проверяется это свойство непосредственно:
$$(b' * a') * (a * b) = b' * (a' * a) * b = b' * e * b = b' * b = e.$$

§ 5. Кольцо и поле

Пусть на множестве K определены две бинарные операции $+$ и $\cdot$ [7], называемые *сложением* и *умножением*, так, что выполняются свойства (*аксиомы кольца*):

(K1) $\langle K, + \rangle$ — коммутативная группа;

(K2) умножение ассоциативно: $\forall\, a, b, c \in K \quad (ab)c = a(bc)$;

(K3) умножение дистрибутивно относительно сложения:
$$\forall\, a, b, c \in K \quad (a + b)c = ac + bc; \quad c(a + b) = ca + cb.$$

Тогда алгебраическая структура $\langle K, +, \cdot \rangle$ называется *кольцом*. Если, кроме того, умножение коммутативно:

(K4) $\forall\, a, b \in K \quad ab = ba$,

[7] Знак умножения при записи выражений над элементами группы, как правило, опускается.

то кольцо называют *коммутативным*. Если в кольце существует нейтральный элемент по умножению:

(K5) $\exists e \in G \quad \forall a \in G \; ae = ea = a,$

то говорят о *кольце с единицей*.

Пример 1. $\mathbb{Z}[x]$ — множество многочленов с целыми коэффициентами вместе с естественным образом введенными операциями сложения и умножения образует кольцо (коммутативное кольцо с единицей). Также образуют кольца многочлены с рациональными и вещественными коэффициентами $\mathbb{Q}[x]$ и $\mathbb{R}[x]$.

$\langle Z_m, +, \cdot \rangle$ — кольцо классов вычетов по модулю m.

Алгебраическая структура $\langle F, +, \cdot \rangle$ называется *полем*, если выполняются свойства (*аксиомы поля*):

(F1) $\langle F, + \rangle$ — (аддитивная) коммутативная группа;

(F2) $\langle F \backslash \{0\}, \cdot \rangle$ — (мультипликативная) коммутативная группа;

(F3) умножение дистрибутивно относительно сложения:

$$\forall a, b, c \in F \quad (a + b)c = ac + bc.$$

Очевидно, что всякое поле является кольцом. Обратное утверждение, вообще говоря, неверно. Например, $\mathbb{Q}[x]$ — кольцо, но не поле (не выполняется свойство **(F2)**).

Пример 2. Множества рациональных ($\mathbb{Q}$), действительных ($\mathbb{R}$) и комплексных ($\mathbb{C}$) чисел образуют поля. Более экзотическим примером поля является множество

$$M = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

◄ Поскольку это — числовое множество, содержащее 0 и 1, для того, чтобы убедиться в наличии структуры поля, достаточно проверить замкнутость M относительно операций сложения (что очевидно) и умножения. Действительно,

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = c + d\sqrt{2},$$

где

$$c = \frac{a}{a^2 - 2b^2}, \quad d = -\frac{b}{a^2 - 2b^2} \in \mathbb{Q}.$$

Заметим, что

$$a^2 - 2b^2 \neq 0,$$

так как в противном случае $\sqrt{2}$ был бы рациональным числом, что неверно. ►

Существуют и конечные поля. Примеры, рассмотренные в § 4, показывают, что если p — простое число, то множество классов вычетов по простому модулю p с введенными на нем операциями сложения и умножения $(\langle Z_p, +, \cdot \rangle)$ — поле.

Известно, что число элементов любого конечного поля (*порядок поля*) равно p^k для некоторого простого числа p и некоторого натурального числа k. Кроме того, для любого числа вида p^k поле такого порядка существует и определяется однозначно (с точностью до изоморфизма). Обозначение: $GF(p^k)$ (Galois field — поле Галуа). В частности, $GF(p)$ есть поле классов вычетов по модулю p.

§ 6. Группы самосовмещений многоугольников и многогранников

Сведения, излагаемые в этом параграфе, будут использованы при решении задач с помощью теории Пойа.

Пусть F — геометрическая фигура. Под *самосовмещением* фигуры F понимают такое перемещение (движение) F (в пространстве или на плоскости), которое переводит F в F. Тривиальным примером самосовмещения является тождественное преобразование ε, при котором каждая точка переходит сама в себя.

Рассмотрим множество G всех самосовмещений фигуры F. *Произведение* $g_1 \cdot g_2$ двух самосовмещений g_1 и g_2 определим как композицию движений $g_1(g_2)$ — это движение, возникающее в результате последовательного выполнения g_2, а затем g_1. Легко проверить, что $\langle G, \cdot \rangle$ — группа. Чем «более симметричной» будет фигура F, тем «более богатой» будет ее группа самосовмещений. Например, для круга и шара соответствующие группы бесконечны.

Группа вращений правильного n-угольника. Под вращением правильного n-угольника будем понимать поворот в его плоскости, приводящий к его самосовмещению. Очевидно, что если поворот нетривиален (т. е. не является тождественным преобразованием), то его центром является центр правильного n-угольника. Поскольку при вращении всякая вершина должна перейти в вершину, угол поворота (с точностью до угла, кратного 2π) равен $k\frac{2\pi}{n}$, $k = 0, 1, \ldots, n-1$.

Группа симметрий правильного n-угольника. Под симметрией правильного n-угольника будем понимать его самосовмещение в пространстве. К перечисленным выше поворотам в плоскости добавляются «опрокидывания» многоугольника, т. е. повороты на 180° вокруг осей симметрии многоугольника[8]. Их ровно n штук. Если n четно, то осями симметрии являются $n/2$ прямых, соединяющих пары противоположных вершин многоугольника, и $n/2$ прямых, соединяющих середины его противоположных сторон. При нечетном n каждая из осей симметрии проходит через некоторую вершину n-угольника и середину противоположной стороны.

Группы вращений многогранников. Под вращением многогранника будем понимать его самосовмещение.

1. **Куб.** Сначала покажем, что группа вращений куба содержит 24 элемента. Будем считать, что куб расположен таким образом, что о его гранях можно говорить: нижняя, верхняя, передняя и т. д. Самосовмещение куба полностью определяется тем,

   1) какая грань из шести станет нижней и
   2) какая из смежных с ней граней будет передней.

   Согласно правилу произведения имеется всего $6 \cdot 4 = 24$ разных самосовмещения. Перечислим их:

   - тождественное преобразование;
   - повороты на $\pm 90°$, 180° вокруг прямых, соединяющих центры противоположных граней (таких вращений $3 \cdot 3 = 9$);

[8] Эти преобразования равносильны осевым симметриям.

- повороты на 180° вокруг прямых, соединяющих середины противоположных ребер куба (6);
- повороты на $\pm 120^\circ$ вокруг диагоналей куба (8) [9].

Легко проверить (рассмотрев, например, подстановки на множестве вершин, порождаемые вращениями), что все эти самосовмещения различны; так как всего их ровно 24, других самосовмещений нет.

2. **Тетраэдр.** Под тетраэдром будем понимать *правильный тетраэдр*. Будем считать, что тетраэдр расположен в пространстве таким образом, что о его гранях можно говорить: нижняя, передняя, задние левая и правая. Самосовмещение тетраэдра полностью определяется тем,

   1) какая грань из четырех становится нижней и
   2) какая из оставшихся трех граней будет передней.

   Таким образом, всего данная группа содержит $4 \cdot 3 = 12$ элементов:
   - тождественное преобразование;
   - повороты на $\pm 120^\circ$ вокруг высот тетраэдра (всего 8 таких поворотов);
   - повороты на 180° вокруг прямых, соединяющих середины скрещивающихся ребер тетраэдра (таких поворотов 3).

   Все названные самосовмещения различны, общее их число 12; поэтому они исчерпывают рассматриваемую группу.

3. **Правильная n-угольная пирамида.** Очевидно, что группа вращений правильной n-угольной пирамиды, отличной от правильного тетраэдра, изоморфна группе вращений правильного n-угольника, лежащего в ее основании.

4. **Двойная пирамида (диэдр).** Эта геометрическая фигура представляет собой объединение двух одинаковых правильных n-угольных пирамид, чьи основания совмещены, а вершины находятся по разные стороны от основания. Если диэдр не является октаэдром, то его группа вращений изоморфна группе симметрий правильного n-угольника.

   Как известно, *октаэдр* — многогранник, двойственный кубу (центры граней октаэдра являются вершинами некоторого куба; центры граней куба являются вершинами некоторого октаэдра). Неудивительно поэтому, что группы вращений октаэдра и куба изоморфны. То же справедливо и для групп вращений двух оставшихся правильных многогранников [10].

5. **Икосаэдр и додекаэдр.** Рассуждая так же, как и в случае куба или тетраэдра, легко найти число элементов группы самосовмещений додекаэдра, зная, что он имеет 20 вершин и из каждой вершины исходит 3 ребра.

---

[9] Рассмотрим, например, поворот куба $ABCDA_1B_1C_1D_1$ вокруг диагонали AC_1. Высота треугольной пирамиды $ABDA_1$ лежит на диагонали AC_1; основанием этой пирамиды является правильный треугольник BA_1D (каждая его сторона — диагональ грани куба), который самосовмещается при поворотах на углы, кратные 120°.

[10] Всего правильных многогранников — ровно пять: тетраэдр, куб, октаэдр, икосаэдр, додекаэдр.

Упражнения

1. Какими свойствами (рефлексивность, антирефлексивность, симметричность, антисимметричность, транзитивность) обладают следующие бинарные отношения на множестве действительных чисел?
   1) $x\mathcal{R}y \iff x^2 = y^2$;
   2) $x\mathcal{R}y \iff x^2 + y^2 = 1$;
   3) $x\mathcal{R}y \iff xy > 1$;
   4) $x\mathcal{R}y \iff y = |x|$;
   5) $x\mathcal{R}y \iff x^2 + x = y^2 + y$;
   6) $x\mathcal{R}y \iff x^3 + x = y^3 + y$;
   7) $x\mathcal{R}y \iff x - y \in \mathbb{Z}$;
   8) $x\mathcal{R}y \iff x - y \in \mathbb{N}$.
2. Какие из отношений предыдущей задачи являются отношениями эквивалентности? Для каждого из таких отношений выяснить, что представляют собой классы эквивалентности и сколько элементов они содержат.
3. На множестве учеников класса введем отношение «учится лучше». Будем говорить «Ученик A учится лучше ученика B», если по большинству контрольных работ A имел оценки выше, чем B. Обладает ли данное отношение свойством транзитивности?
4. На множестве A введено симметричное и транзитивное отношение $\mathcal{R}$ такое, что
$$\forall a \quad \exists b \quad a\mathcal{R}b.$$
Доказать, что отношение $\mathcal{R}$ рефлексивно.

Соглашение. В задачах данного раздела e обозначает нейтральный элемент группы.

Пусть $A = \{a_1, a_2, \ldots, a_n\}$ — конечное множество, на котором определена бинарная операция $*$. Таблица из n строк и n столбцов, в которой на пересечении i-й строки и j-го столбца стоит элемент множества A, равный $a_i * a_j$, называется *таблицей умножения*, или *квадратом Кэли*.

---

5. На множестве $\{1, 2, 3, 4, 6, 12\}$ определим две бинарные операции:
   1) $a * b = (a, b)$ (наибольший общий делитель);
   2) $a * b = [a, b]$ (наименьшее общее кратное).

   Составить для этих операций квадраты Кэли.
6. Составим матрицу коэффициентов дробно-линейной функции $f_i(x) = \dfrac{a_i x + b_i}{c_i x + d_i}$:
$$A_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}.$$
Какая матрица будет соответствовать сложной функции $f_i(f_j(x))$?
7. На множестве функций
$$\left\{x,\ \frac{1}{x},\ \frac{x-1}{x+1},\ \frac{x+1}{x-1},\ \frac{1-x}{1+x},\ \frac{1+x}{1-x},\ -\frac{1}{x},\ -x\right\}$$
выберем в качестве бинарной операции композицию функций (будем считать, что областью определения всех функций является множество $\mathbb{R} \setminus \{-1, 0, 1\}$). Составить квадрат Кэли для данной операции. Доказать, что рассматриваемая алгебраическая структура является группой.

8. На множестве $(\mathbb{Q} \setminus 0) \times \mathbb{Q}$ введена операция

$$(a, b)(c, d) = (ac, bc + d).$$

Доказать, что данная алгебраическая структура является группой.

9. Доказать, что в квадрате Кэли конечной группы каждый элемент группы встречается в каждой строке (и каждом столбце) ровно один раз.

10. Составить квадрат Кэли для следующих групп:

1) вращений правильного треугольника;
2) вращений квадрата;
3) вращений правильного пятиугольника;
4) симметрий ромба, не являющегося квадратом;
5) симметрий правильного треугольника;
6) симметрий прямоугольника, не являющегося квадратом;
7) симметрий квадрата.

11. Доказать, что группа из задачи 7 изоморфна группе симметрий квадрата.

12. Какие из следующих числовых множеств образуют аддитивные группы?

$$\mathbb{Z},\ 2\mathbb{Z},\ \mathbb{N},\ 2\mathbb{Z}+1,\ \mathbb{Q}^+,\ \mathbb{Q},\ \mathbb{R}\setminus\mathbb{Q},\ \{-1, 0, 1\}.$$

13. Какие из следующих числовых множеств образуют мультипликативные группы?

$$\mathbb{R},\ \mathbb{R}\setminus\{0\},\ \mathbb{R}^+,\ \mathbb{Z},\ 2\mathbb{Z}+1,\ \mathbb{Q},\ \mathbb{Q}\setminus\{0\},\ \{1, -1\},\ \left\{1, 2, \frac{1}{2}\right\},\ \mathbb{R}\setminus\mathbb{Q},\ \{2^n \mid n \in \mathbb{Z}\}.$$

14. Доказать, что если в группе каждый элемент себе обратен ($\forall a \quad a * a = e$), то группа — абелева.

15. Найти с точностью до изоморфизма все группы, состоящие не более чем из 4 элементов.

16. Пусть $\varphi : G \to H$ — сюръективное гомоморфное отображение абелевой группы G на группу H. Доказать, что H — абелева группа.

17. Пусть $\langle G, \cdot\rangle$ — группа, $g \in G$. Доказать, что отображение $\varphi_g : G \to G$, заданное правилом $\varphi_g(x) = g^{-1}xg$, является изоморфизмом.

18. Пусть $\langle G, \cdot\rangle$ — конечная группа. Доказать, что

$$\forall g \in G \quad \exists n \in \mathbb{N} \quad g^n = e.$$

Наименьшее $n > 0$, при котором $g^n = e$, называют ***порядком*** *элемента g.*

19. Порядком конечной группы называется количество ее членов. Доказать, что конечная группа четного порядка обязательно содержит элемент второго порядка.

20. Пусть группа обладает единственным элементом второго порядка. Доказать, что этот элемент перестановочен с каждым элементом группы.

Ответы

1. См. табл. 3. **2.** 1, 5, 6, 7. **3.** Нет. **5.** НОД (табл. 4). НОК (табл. 5). **6.** A_iA_j. **7.** См. табл. 6.

8. Указание. Нейтральный элемент $e = (1, 0)$, обратный к $g = (a, b)$:

$$g^{-1} = \left(\frac{1}{a}, -\frac{b}{a}\right).$$

9. Возьмем строку, соответствующую элементу a. В ней встретится элемент b, если для некоторого элемента x выполняется равенство

$$a * x = b. \tag{1}$$

Таблица 3

№	$\mathcal{R}$	рефл.	антирефл.	симм.	антисимм.	транз.
1	$x^2 = y^2$	+	−	+	−	+
2	$x^2 + y^2 = 1$	−	−	+	−	−
3	$xy > 1$	−	−	+	−	−
4	$y = \|x\|$	−	−	−	+	+
5	$x^2 + x = y^2 + y$	+	−	+	−	+
6	$x^3 + x = y^3 + y$	+	−	+	+	+
7	$x - y \in \mathbb{Z}$	+	−	+	−	+
8	$x - y \in \mathbb{N}$	−	+	−	+	+

Таблица 4

	1	2	3	4	6	12
1	1	1	1	1	1	1
2	1	2	1	2	2	2
3	1	1	3	1	3	3
4	1	2	1	4	2	4
6	1	2	3	2	6	6
12	1	2	3	4	6	12

Таблица 5

	1	2	3	4	6	12
1	2	2	3	4	6	12
2	2	2	6	4	6	12
3	3	6	3	12	6	12
4	4	4	12	4	12	12
6	6	6	6	12	6	12
12	12	12	12	12	12	12

Таблица 6

	x	$\frac{1}{x}$	$\frac{x-1}{x+1}$	$\frac{x+1}{x-1}$	$\frac{1-x}{1+x}$	$\frac{1+x}{1-x}$	$-\frac{1}{x}$	$-x$
x	x	$\frac{1}{x}$	$\frac{x-1}{x+1}$	$\frac{x+1}{x-1}$	$\frac{1-x}{1+x}$	$\frac{1+x}{1-x}$	$-\frac{1}{x}$	$-x$
$\frac{1}{x}$	$\frac{1}{x}$	x	$\frac{x+1}{x-1}$	$\frac{1-x}{1+x}$	$\frac{1+x}{1-x}$	$-\frac{1}{x}$	$-x$	$-\frac{1}{x}$
$\frac{x-1}{x+1}$	$\frac{x-1}{x+1}$	$\frac{1-x}{1+x}$	$-\frac{1}{x}$	$\frac{1}{x}$	$-x$	x	$\frac{1+x}{1-x}$	$\frac{x+1}{x-1}$
$\frac{x+1}{x-1}$	$\frac{x+1}{x-1}$	$\frac{1+x}{1-x}$	$-x$	x	$-\frac{1}{x}$	$\frac{1}{x}$	$\frac{1-x}{1+x}$	$\frac{x-1}{x+1}$
$\frac{1-x}{1+x}$	$\frac{1-x}{1+x}$	$\frac{x-1}{x+1}$	$\frac{1}{x}$	$-\frac{1}{x}$	x	$-x$	$\frac{x+1}{x-1}$	$\frac{1+x}{1-x}$
$\frac{1+x}{1-x}$	$\frac{1+x}{1-x}$	$\frac{x+1}{x-1}$	x	$-x$	$\frac{1}{x}$	$-\frac{1}{x}$	$\frac{x-1}{x+1}$	$\frac{1-x}{1+x}$
$-\frac{1}{x}$	$-\frac{1}{x}$	$-x$	$\frac{1+x}{1-x}$	$\frac{1-x}{1+x}$	$\frac{x+1}{x-1}$	$\frac{x-1}{x+1}$	x	$\frac{1}{x}$
$-x$	$-x$	$-\frac{1}{x}$	$\frac{1-x}{1+x}$	$\frac{1+x}{1-x}$	$\frac{x-1}{x+1}$	$\frac{x+1}{x-1}$	$\frac{1}{x}$	x

Аналогично, в столбце, соответствующем элементу a, встретится элемент b, если для некоторого элемента y выполняется равенство

$$y * a = b. \tag{2}$$

Таким образом, задача сводится к доказательству существования и единственности решения каждого из уравнений (1) и (2). Умножив равенство (1) слева на элемент a' (элемент, обратный к a), получим $x = a' * b$. Значит, если решение уравнения (1) существует, то оно единственно. С другой стороны, непосредственной подстановкой в (1) убеждаемся, что $a' * b$ — решение.

Аналогично, находим решение уравнения (2): $y = b * a'$.

12. $\mathbb{Z}, 2\mathbb{Z}, \mathbb{Q}$. **13.** $\mathbb{R}\backslash\{0\}$, $\mathbb{R}^+$, $\mathbb{Q}\backslash\{0\}$, $\{-1, 1\}$, $\{2^n | n \in \mathbb{Z}\}$.

14. $ab \cdot ab = e \Rightarrow ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.

15. Указание. Использовать результат упражнения 9.

Приведем набросок решения для случая $n = 4$.

Один из элементов группы — нейтральный (e); пусть три других — a, b и c. Рассмотрим два возможных случая.

1. Каждый элемент группы себе обратен ($a^2 = b^2 = c^2 = e$), т. е. каждый элемент диагонали квадрата Кэли — e. Ясно, как выглядят строка и столбец, отвечающие e. Теперь нам предстоит заполнить пустые клетки в таблице

e	a	b	c
a	e		
b		e	
c			e

На пересечении второй строки и третьего столбца может стоять только элемент c, так как во второй строке уже есть элементы a и e, а в третьем столбце — элемент b (напомним, что в каждой строке и каждом столбце квадрата Кэли по одному разу встречается каждый элемент группы). Аналогичные рассуждения позволяют однозначно заполнить оставшиеся клетки таблицы.

Операция, заданная полученной таблицей, удовлетворяет аксиомам **(G1)**, **(G3)** и **(G4)**. Осталось проверить выполнение аксиомы **(G2)**. Это можно сделать непосредственно либо привести пример группы, имеющей данный квадрат Кэли.

2. Не каждый элемент группы себе обратен. Пусть, например, $a^2 = b$. Имеем таблицу

e	a	b	c
a	b		
b			
c			

Хотя в ней пустых клеток больше, чем в предыдущем случае, но и она заполняется однозначно. Здесь удобно начать с пересечения второй строки и четвертого столбца.

16. Указание. Воспользоваться тем, что у каждого элемента группы H есть прообраз в G и тем, что $\forall x, y \in G \quad \varphi(xy) = \varphi(yx)$ в силу коммутативности G.

17. Указание. Заметить, что $g^{-1}eg = e$ и $g^{-1}(xy)g = (g^{-1}xg)(g^{-1}yg)$.

18. Указание. В силу конечности группы в последовательности степеней $e, g^1, g^2, \ldots$ есть одинаковые элементы.

19. Если a' — элемент, обратный к a, то a — элемент, обратный к a'. Стало быть, элементы порядка выше второго (для каждого такого элемента a имеем $a \neq a'$) разбиваются на пары взаимно обратных. Поэтому в группе (с четным числом элементов) содержится и четное число элементов порядка 1 и 2. Но порядок 1 имеет только нейтральный элемент. Значит, порядок 2 имеют нечетное число элементов.

20. Пусть $g \neq e$, $g^2 = e$, $a \in G$ — произвольный элемент группы. Докажите, что aga^{-1} — элемент второго порядка. Из условия задачи теперь следует: $aga^{-1} = g$, откуда $ag = ga$.

Глава LXVIII

КОМБИНАТОРИКА

В разных областях науки и техники приходится решать задачи, содержание которых — комбинирование различных элементов и объектов в группы и определение числа различных способов, которыми это можно сделать. Такие задачи называют *комбинаторными*, а соответствующий раздел математики — *комбинаторикой*.

Комбинаторика — часть математики, изучающая способы решения задач перечисления и пересчета элементов в конечных множествах. Задача *перечисления* состоит в выделении элементов из некоторого заданного конечного множества, обладающих определенными свойствами, а задача *пересчета* — в нахождении числа таких элементов. Например, задача: Описать все возможные расположения 8 одинаковых ладей на шахматной доске, при которых ладьи не бьют друг друга — есть задача перечисления, а задача отыскания количества указанных расстановок есть задача пересчета.

Истоки комбинаторной проблематики кроются в азартных играх. Умение оценивать количество способов, которыми можно получить данную сумму очков при бросании нескольких игральных костей или данную комбинацию цифр в рулетке, определение шансов на получение того или иного расклада в карточных играх и другие, аналогичные проблемы — вот первоисточники современной комбинаторики.

Даже Исаак Ньютон был не чужд подобной проблематике. В 1693 году некто Сэмюэл Пипс, президент Королевского Общества (так именовалась британская Академия наук), поинтересовался у Ньютона, какую из ситуаций следует предпочесть при игре в кости — выпадение по крайней мере одной единицы при бросании 6 костей или появление не менее двух единиц при бросании 12 костей. Ньютон ответил, что «легкие вычисления» показывают преимущества первой ситуации и привел соответствующие расчеты в подтверждение своего мнения[1)].

Впервые строгое научное исследование комбинаторных проблем было предпринято Блезом Паскалем и Пьером Ферма. В дальнейшем Якоб Бернулли, Готфрид Лейбниц, Леонард Эйлер и многие другие выдающиеся математики и естествоиспытатели занимались комбинаторными задачами и разработали основные методы их решения, не потерявшие своего значения и поныне.

По-видимому, одной из первых комбинаторных задач следует считать задачу о так называемых «магических квадратах», упоминание о которой встречается еще

[1)] Следует отметить, что на Пипса аргументы Ньютона не произвели впечатления и он остался при своем убеждении об эквивалентности этих ситуаций.

в китайских наставлениях. Согласно преданию, Фу Си (мифический прародитель китайской цивилизации) получил панцирь черепахи с начертанным на нем магическим квадратом от Великого императора (божества) в знак признания за профессионально выполненные технические работы на реке Ло.

Напомним, что *магическим квадратом* называется такое расположение n^2 натуральных чисел в клетках квадрата $n \times n$, что суммы чисел по строкам, столбцам и диагоналям совпадают. Магический квадрат, полученный Фу Си, является квадратом третьего порядка ($n = 3$) и имеет вид

4	9	2
3	5	7
8	1	6

Для него $S_{\text{стр}} = S_{\text{столб}} = S_{\text{диаг}} = 15$. Нахождение числа всех магических квадратов порядка $n > 4$ представляет собой очень трудную задачу.

Другой классической комбинаторной задачей, стимулировавшей разработку теории и методов комбинаторного анализа, является задача Эйлера о 36 офицерах, в которой требовалось построить 36 офицеров 6 различных воинских званий и 6 различных родов войск для парада в каре размером 6×6 так, чтобы в каждой шеренге и каждой колонне был ровно один офицер данного воинского звания из данного рода войск. Она положила начало теории *латинских квадратов и латинских прямоугольников*, нашедших широкое применение в теории планирования эксперимента и прикладной статистике, и надолго определила тематику исследований в комбинаторике.

Задача эта долго не поддавалась решению (Эйлер высказал гипотезу о невозможности требуемого размещения) и только в 1900 году было установлено, что Эйлер был прав и задача решения не имеет.

Задача о числе разбиений натурального числа n на слагаемые была поставлена Лейбницем в 1669 году и эффективно решена Эйлером, который разработал и с успехом использовал для решения этой и подобных задач метод производящих функций, задаваемых в виде бесконечных произведений.

Прикладное значение комбинаторных методов было осознано сравнительно недавно — в начале XX века, когда бурное развитие теории вероятностей и ее приложений потребовало развитой комбинаторной техники и активизировало работу ученых в этом направлении. В дальнейшем оказалось, что комбинаторные методы незаменимы в теории графов и статистике, теории информации и криптографии, линейном программировании и теории массового обслуживания. Они находят широкое применение при построении блок-схем, алгоритмов и расписаний. Даже в таких совершенно абстрактных областях, как теория чисел, теория групп, теория представлений, теория неассоциативных алгебр и т. д., комбинаторные методы оказываются удивительно эффективными и результативными.

В настоящее время этот раздел математики активно развивается учеными различных направлений. В немалой степени это развитие стимулировано запросами приложений (в первую очередь теорией блок-схем) и широкими возможностями использования современной электронно-вычислительной техники.

В элементарной комбинаторике, связанной с размещением группы однородных объектов по ячейкам, при наличии различных ограничений на способы подобного размещения, большое значение имеют принципы подсчета численностей выборочных совокупностей, называемые *правилом произведения* и *правилом сложения*.

§ 1. Правило произведения

Теорему, которую мы сейчас сформулируем и докажем, часто называют *основным принципом комбинаторики*.

Теорема 1 (правило произведения). *Пусть производится выбор n объектов из множества объектов произвольной природы. Если первый элемент может быть выбран a_1 способами, второй — a_2 способами, независимо от того как выбирался первый, третий — a_3 способами, независимо от того как выбирались первый и второй, и т. д., то общее количество способов, которыми подобный выбор может быть осуществлен, равно произведению $a_1 \cdot a_2 \cdot \ldots \cdot a_n$.*

◄ Доказательство проведем методом математической индукции.

При $n = 1$ утверждение очевидно. Пусть $n = 2$. Закодируем отбор упорядоченной парой чисел (i, j), где i — один из вариантов выбора первого элемента, а j — второго. Все способы выбора пары элементов можно описать прямоугольной таблицей, приведенной ниже.

$$\begin{array}{cccc} (1,1) & (1,2) & (1,3) & \ldots & (\mathrm{I}, a_2) \\ (2,1) & (2,2) & (2,3) & \ldots & (2, a_2) \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots \\ (a_1,1) & (a_1,2) & (a_1,3) & \ldots & (a_1, a_2) \end{array}$$

В таблице a_1 строк и a_2 столбцов, а, значит, $a_1 \cdot a_2$ элементов. Утверждение для случая $n = 2$ доказано.

Предположим теперь, что правило произведения справедливо при $n = k \geqslant 2$. Последовательность из $k+1$ шагов выбора будем кодировать упорядоченным набором чисел $(i_1, i_2, \ldots, i_k, i_{k+1})$, где i_j — некоторый вариант выбора j-го элемента. Таких наборов — столько же, сколько *упорядоченных пар* $((i_1, i_2, \ldots, i_k), i_{k+1})$, в которых первый элемент — упорядоченный набор из k элементов. По предположению число наборов $(i_1, i_2, \ldots, i_k)$ равно $a_1 \cdot a_2 \cdot \ldots \cdot a_k$; второй элемент этой пары — i_{k+1} — по условию может быть отождествлен с любым из способов, которыми может быть отобран $(k+1)$-й объект. Поскольку этот выбор можно осуществить a_{k+1} способами, то всего пар будет

$$(a_1 \cdot a_2 \cdot \ldots \cdot a_k) \cdot a_{k+1} = a_1 \cdot a_2 \cdot \ldots \cdot a_k \cdot a_{k+1},$$

что и требовалось доказать. ►

Применим правило произведения к решению двух важных комбинаторных задач.

1.1. Число перестановок

Пусть имеется n различных элементов. *Перестановкой* n элементов называют их расположение на n различных местах. Подсчитаем число таких перестановок. Каждую перестановку можно получить в результате последовательного выполнения n действий.

Первое действие — выбор места для первого элемента — выполняется n способами.

Второе действие — выбор места для второго элемента — выполняется $n-1$ способами, поскольку одно место уже занято, и число свободных мест на единицу уменьшилось. И так далее. Наконец, размещение последнего, n-го элемента осуществляется однозначно.

По правилу произведения число всех перестановок n элементов равно

$$\boxed{n \cdot (n-1) \cdot \ldots \cdot 1 = n!}.$$

1.2. Число подмножеств конечного множества

Пусть A — множество, содержащее n элементов. Для малых n подсчитаем число всевозможных подмножеств множества A. Для этого составим следующую таблицу (табл. 1).

Таблица 1

n	A	все подмножества A	число подмножеств
1	$\{a\}$	$\varnothing, \{a\}$	2
2	$\{a, b\}$	$\varnothing, \{a\}, \{b\}, \{a, b\}$	4
3	$\{a, b, c\}$	$\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}$	8

Возникает предположение, что число всех подмножеств n-элементного множества равно 2^n. Справедливость его легко доказать с помощью правила произведения. Действительно, произвольное подмножество n-элементного множества можно получить в результате выполнения следующих n действий: 1-е действие «определяет судьбу» 1-го элемента множества — быть ему в формируемом подмножестве или нет, 2-е действие касается 2-го элемента, ..., n-е действие — n-го элемента. Таким образом каждое из n действий может быть выполнено двумя способами. Согласно правилу произведения, число способов выполнить все n действий, а значит, и число всех подмножеств исходного множества равно 2^n.

§ 2. Выборки. Размещения

Пусть задано некоторое конечное множество $A = \{a_1, a_2, \ldots a_n\}$ — *генеральная совокупность.* Из элементов генеральной совокупности образуются *выборки*:

$$a_{i_1}, a_{i_2}, \ldots, a_{i_r}, \quad \text{где} \quad \forall j \quad i_j \in \{1, 2, \ldots, n\}.$$

Выборки классифицируются следующим образом.

В зависимости от того, существен порядок элементов выборки или нет, ее называют *упорядоченной* или *неупорядоченной*.

В зависимости от того, могут или не могут элементы выборки повторяться, ее называют выборкой *с повторениями* или выборкой *без повторений*. Упоминание об отсутствии повторений часто опускают, в то время как допустимость повторений элементов в выборке всегда специально оговаривается.

Число элементов выборки называют ее *объемом*. Выборку объема r называют r-выборкой.

Размещением из n элементов по m называется упорядоченная m-выборка из n-элементной генеральной совокупности.

Пример. Пусть $n = 3$, $m = 2$. Обозначим элементы исходного 3-элементного множества a, b, c. Выпишем всевозможные размещения из 3 по 2 (без повторений):

$$(a, b), (a, c), (b, a), (b, c), (c, a), (c, b).$$

Если говорить о размещениях с повторениями, то к указанному списку добавится еще 3 размещения: $(a, a), (b, b), (c, c)$.

Число размещений из n по m без повторений обозначают A_n^m, а с повторениями $\overline{A_n^m}$. Например, $A_3^2 = 6$, $\overline{A_3^2} = 9$. Несложно получить общие формулы для числа размещений. Если элементы размещения не могут повторяться, то число способов, каким можно выбрать каждый очередной элемент размещения, будет на единицу меньше, чем для предшествующего ему, а так как первый элемент размещения выбирается n способами, то с помощью правила произведения получаем формулу

$$\boxed{A_n^m = n(n-1)(n-2)\dots(n-m+1).}$$

Полученное произведение содержит m множителей, его иногда обозначают так: $(n)_m$. В размещении с повторениями *каждый* очередной элемент может быть выбран n способами, поэтому

$$\boxed{\overline{A_n^m} = n^m.}$$

§ 3. Сочетания

Сочетанием из n по m называют неупорядоченную m-выборку из n-элементной генеральной совокупности.

Пример 1. Пусть $n = 3$, $m = 2$. Обозначим элементы исходного 3-элементного множества a, b, c. Выпишем всевозможные сочетания из 3 по 2 (без повторений): ab, ac, bc. Если говорить о сочетаниях с повторениями, то к указанному списку добавится еще 3 сочетания: aa, bb, cc.

◀ Число сочетаний из n по m (без повторений) обозначают C_n^m или $\binom{n}{m}$, а с повторениями — $\overline{C_n^m}$. Например, $C_3^2 = 3$, $\overline{C_3^2} = 6$.

Выведем формулу для C_n^m. Всякое размещение из n по m можно получить с помощью процедуры из двух действий:

1) выбор элементов, входящих в размещение (другими словами, выбор сочетания из n по m);
2) перестановка выбранных элементов.

По правилу произведения получаем $A_n^m = C_n^m \cdot m!$, откуда

$$C_n^m = \frac{n(n-1)\dots(n-m+1)}{m!}.$$

Умножив числитель и знаменатель полученной дроби на $(n-m)!$, получим

$$\boxed{C_n^m = \frac{n!}{m!(n-m)!}.} \blacktriangleright$$

Число сочетаний с повторениями. «Закодируем» сочетание с повторениями последовательностью из нулей и единиц следующим образом: сначала запишем столько единиц, сколько раз в сочетание входит первый элемент исходного множества, затем — 0, затем столько единиц, сколько раз в сочетание входит второй элемент исходного множества, затем — 0 и т. д. (после единиц, соответствующих последнему элементу, 0 не ставим).

Пример 2. Пусть $n = 3$, $m = 5$. Тогда *aaabc* имеет кодировку 1110101; *abbbb* — 1011110, *ccccc* — 0011111.

Заметим, что в кодирующей последовательности ровно $n+m-1$ элементов: m единиц (столько, сколько элементов в сочетании) и $n-1$ нулей (отделяющих друг от друга n наборов единиц, соответствующих n элементам исходного множества). Очевидно, что любой последовательности такого вида соответствует некоторое сочетание с повторениями из n по m.

Пример 3. При $n = 3$, $m = 5$ последовательности 1110011 отвечает сочетание *aaacc*, а 0111110 — *bbbbb*.

Таким образом, установлено взаимно однозначное соответствие между множеством сочетаний из n по m и множеством последовательностей из m единиц и $n-1$ нуля. Несложно подсчитать число последних: для построения любой последовательности указанного вида нужно определить m позиций для единиц из $n+m-1$ возможных; поэтому число последовательностей равно C_{n+m-1}^m. Доказано, что

$$\boxed{\overline{C_n^m} = C_{n+m-1}^m.}$$

Рассмотрим несколько задач, при решении которых используются сочетания с повторениями.

- Каким числом способов можно разместить n одинаковых шаров по k различным урнам, если в каждую урну разрешается поместить любое количество шариков (допустимо, в том числе, что урна может остаться пустой)?
  Решение. Присвоим урнам номера от 1 до k. Будем считать, что, помещая шар в урну, мы присваиваем ему ее номер. Тогда размещение шаров по урнам сводится к построению последовательности, в которой n элементов и каждый из них принимает одно из k значений. Таким образом, ответ к задаче: $\overline{C_k^n}$.
- Каким числом способов могут распределиться голоса 1 миллиона избирателей среди 42 избирательных блоков?

  Задача сводится к предыдущей. Ответ: $\overline{C_{42}^{10^6}}$.

- Найти число решений уравнения

$$x_1 + x_2 + \ldots + x_k = n$$

в неотрицательных целых числах (n — любое целое неотрицательное; k — целое положительное).

Опять задача сводится к числу распределений одинаковых шаров по различным урнам, если считать, что x_i — количество шаров, помещаемых в i-ю урну, n — общее число шаров, k — общее число урн. Ответ: $\overline{C}_k^n$.

- Найти число решений уравнения

$$x_1 + x_2 + \ldots + x_k = n$$

в *натуральных* числах (n, k — целые положительные, $k \leqslant n$).

Введем новые переменные:

$$x_i = y_i + 1 \quad (i = 1, \ldots, k).$$

Относительно новых переменных y_i получим уравнение уже в *неотрицательных целых* числах

$$y_1 + y_2 + \ldots + y_k = n - k,$$

число решений которого

$$\overline{C}_k^{n-k} = C_{n-1}^{n-k} = C_{n-1}^{k-1}.$$

Читателю предлагается подумать над тем, как ответ может быть получен непосредственно (без сведения к предыдущей задаче).

§ 4. Перестановки с повторениями

Перестановками с повторениями называют упорядоченные выборки, в которых каждый элемент генеральной совокупности встречается фиксированное (свое для каждого элемента) число раз.

Пусть $A = \{a_1, a_2, \ldots, a_k\}$ — генеральная совокупность. Число перестановок с повторениями, в которых элемент a_1 встречается n_1 раз, элемент a_2 — n_2 раз, ..., элемент a_k — n_k раз, обозначают $P(n_1, n_2, \ldots, n_k)$. Выведем формулу для $P(n_1, n_2, \ldots, n_k)$. Обозначим через n общее число элементов в каждой выборке указанного вида: $n = n_1 + n_2 + \ldots + n_k$.

Рассмотрим формирование перестановки с повторениями как процедуру из следующих k шагов.

1-й шаг. Определяем n_1 мест, которые будет занимать элемент a_1.

2-й шаг. Определяем n_2 мест, которые будет занимать элемент a_2.

.....

k-й шаг. Определяем n_k мест, которые будет занимать элемент a_k.

1-й шаг выполняется $C_n^{n_1}$ способами,

2-й шаг — $C_{n-n_1}^{n_2}$ способами,

.....

k-й шаг — $C_{n-n_1-n_2-\ldots-n_{k-1}}^{n_k}$ способами.

Общее число перестановок с повторениями находим по правилу произведения:

$$C_n^{n_1} C_{n-n_1}^{n_2} C_{n-n_1-n_2}^{n_3} \dots C_{n-n_1-n_2-\dots-n_{k-1}}^{n_k} =$$

$$= \frac{n!}{n_1!(n-n_1)!} \cdot \frac{(n-n_1)!}{n_2!(n-n_1-n_2)!} \cdot \frac{(n-n_1-n_2)!}{n_3!(n-n_1-n_2-n_3)!} \dots$$

$$\dots \frac{(n-n_1-\dots-n_{k-1})!}{n_k!(n-n_1-\dots-n_k)!} = \frac{n!}{n_1!n_2!n_3!\dots n_k!(n-n_1-\dots-n_k)!}.$$

Замечая, что $(n-n_1-\dots-n_k)! = 0! = 1$, получаем окончательный результат:

$$\boxed{P(n_1, n_2, \dots, n_k) = \frac{n!}{n_1!n_2!\dots n_k!}, \quad \text{где} \quad n = n_1 + n_2 + \dots + n_k.}$$

Пример. Сколько различных «слов» можно получить, переставляя буквы слова «колокольчик»?

◀ В слове 11 букв, буквы «к» и «о» встречаются по три раза, буква «л» — дважды, остальные — по одному разу.

Ответ: $\dfrac{11!}{3!3!2!1!1!1!} = 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 5 \cdot 2.$ ▶

§ 5. Полиномиальная формула

Теорема 2. *Для любых натуральных чисел n и k и любых чисел $x_1, x_2, \dots, x_k$ справедливо равенство*

$$(x_1 + x_2 + \dots + x_k)^n = \sum_{n_1+\dots+n_k=n} \frac{n!}{n_1!n_2!\dots n_k!} x_1^{n_1} x_2^{n_2} \dots x_k^{n_k}.$$

Пояснение. Суммирование производится по всем решениям уравнения $n_1+n_2+\dots+n_k = n$ в неотрицательных целых числах. Таким образом, в силу результатов § 3 число слагаемых в данной сумме равно $\overline{C}_k^n$.

◀ Запишем n-ю степень суммы как произведение n множителей, после чего раскроем скобки, не приводя подобных и не меняя порядка множителей:

$$(x_1+x_2+\dots+x_k)^n = (x_1+x_2+\dots+x_k)(x_1+x_2+\dots+x_k)\dots(x_1+x_2+\dots+x_k) =$$

$$= x_1x_1\dots x_1 + x_1x_1\dots x_2 + \dots + x_kx_k\dots x_k.$$

Если каждое слагаемое рассматривать как n-буквенное «слово», то в полученной сумме присутствуют *все* «слова» из n букв, в которых каждая буква принимает одно из k значений: $x_1, x_2, \dots, x_k$, причем каждое такое слово встречается ровно один раз. После приведения подобных коэффициент при $x_1^{n_1} x_2^{n_2} \dots x_k^{n_k}$ будет равен числу n-буквенных слов, в которых буква x_1 встречается n_1 раз, x_2 — n_2 раз, $\dots$, x_k — n_k раз, т. е. числу перестановок с повторениями

$$P(n_1, n_2, \dots, n_k) = \frac{n!}{n_1!n_2!\dots n_k!} x_1^{n_1} x_2^{n_2} \dots x_k^{n_k}.$$

Теорема доказана. ▶

Замечание 1. Частным случаем полиномиальной формулы является формула бинома Ньютона

$$\boxed{(x+y)^n = \sum_{i=0}^{n} C_n^i x^{n-i} y^i.}$$

Действительно, если в полиномиальной формуле положить $k = 2$, $x_1 = x$, $x_2 = y$, $n_2 = i$, то $n_1 = n - i$ и

$$(x+y)^n = \sum_{n_1+n_2=n} \frac{n!}{n_1! n_2!} x^{n_1} y^{n_2} = \sum_{i=0}^{n} C_n^i x^{n-i} y^i.$$

Замечание 2. Другим широко известным частным случаем рассматриваемой формулы является формула квадрата суммы k слагаемых

$$(x_1 + x_2 + \ldots + x_k)^2 = \sum_i x_i^2 + 2 \sum_{i<j} x_i x_j.$$

Пример 1. Получить формулу куба суммы трех слагаемых.

◄ Уравнение $n_1 + n_2 + n_3 = 3$ имеет $\overline{C}_3^3 = C_5^3 = 10$ решений в неотрицательных целых числах:

$$(3, 0, 0),\ (2, 1, 0),\ (1, 1, 1),$$

а также тройки чисел, получающиеся из указанных перестановками элементов. Таким образом, в формуле три различных полиномиальных коэффициента:

$$P(3, 0, 0) = 1,$$
$$P(2, 1, 0) = 3,$$
$$P(1, 1, 1) = 6.$$

Искомая формула:

$$(x+y+z)^3 = x^3 + y^3 + z^3 + 3(x^2y + x^2z + y^2x + y^2z + z^2x + z^2y) + 6xyz. \ ►$$

Пример 2. В разложении многочлена $(2 - x + x^2)^5$ найти коэффициент при x^5.

◄ Применяя полиномиальную формулу, получаем:

$$(2 - x + x^2)^5 = \sum_{n_1+n_2+n_3=5} \frac{5!}{n_1! n_1! n_3!} 2^{n_1} (-x)^{n_2} (x^2)^{n_3} =$$
$$= \sum_{n_1+n_2+n_3=5} \frac{5!}{n_1! n_1! n_3!} 2^{n_1} (-1)^{n_2} x^{n_2+2n_3}. \qquad (1)$$

Для того чтобы определить, какие слагаемые в полученной сумме содержат x^5, нужно решить в неотрицательных целых числах систему двух линейных уравнений с тремя неизвестными

$$\begin{cases} n_1 + n_2 + n_3 = 5, \\ n_2 + 2n_3 = 5. \end{cases}$$

Из второго уравнения следует нечетность n_2; в силу неотрицательности переменных n_2 принимает значения: 1, 3 или 5. Все решения системы удобно записать в виде табл. 2,

Таблица 2

n_1	n_2	n_3	$\frac{5!(-1)^{n_2}2^{n_3}}{n_1!n_2!n_3!}$
2	1	2	−120
1	3	1	−40
0	5	0	−1

к которой припишем столбец значений коэффициентов при x^5 в отвечающих каждому решению слагаемых в (1).

Таким образом, коэффициент при x^5 равен $-120-40-1=-161$. ▶

§ 6. Комбинаторные тождества

В этом параграфе будет доказан ряд соотношений для биномиальных коэффициентов. Все они интересны сами по себе и многие будут использоваться нами в дальнейшем. Однако не менее интересны *способы* их доказательства (или получения). Мы будем, как правило, предлагать доказательства, исходящие из *комбинаторной природы* соотношений. Общая схема рассуждений здесь такова. Пусть доказывается тождество $f(n, m, \ldots) = g(n, m, \ldots)$. По виду левой и правой частей реконструируется задача на *подсчет числа комбинаций* определенного вида ($n, m, \ldots$ выступают в роли параметров), решая которую одним способом, получаем в качестве ответа $f(n, m, \ldots)$, а другим способом — $g(n, m, \ldots)$.

В нижеприводимых соотношениях значения параметров предполагаются такими, чтобы все биномиальные коэффициенты имели смысл (например, если в формуле присутствует C_n^k, то предполагается, что $0 \leqslant k \leqslant n$).

Имеют место следующие тождества:

1) $C_n^k = C_n^{n-k}$;

2) $C_{n-1}^{k-1} + C_{n-1}^k = C_n^k$;

3) $\sum\limits_{k=0}^{n} C_n^k = 2^n$;

4) $\sum\limits_{k=0}^{n} (-1)^k C_n^k = 0 \quad (n \geqslant 1)$;

5) $\sum\limits_{k=1}^{n} (-1)^{k-1} C_n^k = 1$;

6) $C_{m+n}^k = \sum\limits_{s=0}^{k} C_m^s C_n^{k-s} \quad (m, n \geqslant k)$;

7) $C_{2n}^n = \sum\limits_{k=0}^{n} (C_n^k)^2$;

8) $kC_n^k = nC_{n-1}^{k-1}$;

9) $C_n^k C_k^m = C_n^m C_{n-m}^{k-m}$;

10) $\sum\limits_{p=0}^{k} C_{m+p}^m = C_{m+k+1}^{m+1}$;

11) $\sum\limits_{p=0}^{k} C_{n+p}^m = C_{n+k+1}^{m+1} - C_n^{m+1}$;

12) $\sum\limits_{k=0}^{m} C_n^k C_{n-k}^{m-k} = C_n^m \cdot 2^m$;

13) $\sum\limits_{n=k}^{m} \frac{1}{n} C_n^k = \frac{1}{k} C_m^k$;

14) $\sum\limits_{k=1}^{n} \frac{(-1)^{k-1}}{k} C_n^k = \sum\limits_{k=1}^{n} \frac{1}{k}$.

◀ 1) Каждому k-элементному подмножеству n-элементного множества поставим в соответствие его дополнение до всего множества. Нетрудно видеть, что при этом задается взаимно однозначное соответствие между k-элементными и $(n-k)$-элементными подмножествами n-элементного множества. Если между двумя конечными множествами существует взаимно однозначное соответствие, то эти множества содержат одинаковое количество элементов. Таким образом, число сочетаний из n по k совпадает с числом сочетаний из n по $n-k$.

2) Пусть в парламенте n депутатов, включая спикера. Подсчитаем число способов составить парламентскую делегацию из k человек. С одной стороны, это число сочетаний C_n^k.

Произведем подсчет по-другому. Для того чтобы сформировать делегацию, включающую спикера, нужно из $n-1$ рядовых депутатов выбрать $k-1$; это можно сделать C_{n-1}^{k-1} способами. Если же спикер в делегацию не входит, то ее членов можно выбрать C_{n-1}^k способами (из $n-1$ рядовых депутатов выбирается k человек). Таким образом, всего имеется $C_{n-1}^{k-1}+C_{n-1}^k$ способов составить делегацию.

3) 2^n — число всех подмножеств n-элементного множества. Так как C_n^k — число всех его k-элементных подмножеств, то просуммировав C_n^k по k от 0 до n, вновь получим общее число всех подмножеств.

Другой способ доказательства состоит в применении формулы бинома Ньютона

$$(1+x)^n=\sum_{k=0}^{n}C_n^kx^k.$$

Положив в ней $x=1$, получим требуемое.

4) Тождество доказывается подстановкой в приведенной выше формуле $x=-1$.

Приведем также *комбинаторное доказательство*.

Найдем количество подмножеств n-элементного множества, имеющих четное число элементов. Оно совпадает с количеством способов составить парламентскую делегацию из четного числа человек, если в парламенте всего n депутатов.

Произвольная делегация такого вида может быть получена в результате выполнения следующей процедуры. Сначала относительно каждого из депутатов, не считая спикера, будем принимать решение, войдет данный депутат в делегацию или нет. Согласно правилу произведения, эти решения могут быть вынесены 2^{n-1} способами. Спикер включается в делегацию только в том случае, когда в ней нечетное число «рядовых» депутатов. Таким образом, общее число делегаций с четным числом членов равно 2^{n-1}.

Поскольку общее число подмножеств есть 2^n, подмножеств с нечетным числом элементов также 2^{n-1}, то есть столько же, сколько и с четным числом элементов. Значит,

$$C_n^1+C_n^3+C_n^5+\ldots=C_n^0+C_n^2+C_n^4+\ldots,$$

поскольку части записанного равенства выражают собой число подмножеств n-элементного множества соответственно с нечетным и четным числом элементов. Полученное равенство равносильно доказываемому.

5) Данное соотношение является другой формой записи предыдущего тождества.

6) Решим такую задачу: *Имеется m мужчин и n женщин. Из них нужно сформировать делегацию из k человек. Каким числом способов это можно сделать?* Ответ очевиден: C_{m+n}^k. Будем классифицировать делегации по числу мужчин. Если в делегацию входят s мужчин и $k-s$ женщин, то мужчин можно выбрать C_m^s способами, а женщин — C_n^{k-s} способами; значит, число делегаций с s мужчинами равно $C_m^s C_n^{k-s}$. Суммируя $C_m^s C_n^{k-s}$ по s от 0 до k, получим общее число делегаций.

7) Для доказательства достаточно в предыдущем соотношении положить $k = m = n$ и применить 1).

8) Доказательство тождества может быть получено из решения следующей задачи: *Каким числом способов можно из n кандидатов выбрать k депутатов и среди последних спикера?* Депутаты выбираются C_n^k способами, после чего спикер выбирается k способами; таким образом, общее число способов равно $C_n^k \cdot k$. То же число можно подсчитать по-другому. Будем сначала (всенародным голосованием) избирать спикера (из n кандидатов), а затем из оставшихся $n-1$ кандидата — еще $k-1$ депутата. Указанная процедура может быть выполнена $n \cdot C_{n-1}^{k-1}$ способами. Доказано, что $kC_n^k = nC_{n-1}^{k-1}$. Отсюда вытекает полезное рекуррентное соотношение $C_n^k = \frac{n}{k} C_{n-1}^{k-1}$, применяя которое несколько (точнее: k) раз, можно вновь вывести формулу для числа сочетаний:

$$C_n^k = \frac{n}{k} C_{n-1}^{k-1} = \frac{n}{k} \cdot \frac{n-1}{k-1} \cdot C_{n-2}^{k-2} = \ldots =$$
$$= \frac{n}{k} \cdot \frac{n-1}{k-1} \cdot \ldots \cdot \frac{n-k+1}{1} C_{n-k}^0 = \frac{n(n-1)\ldots(n-k+1)}{k!}.$$

9) Это тождество — обобщение предыдущего (если в 9) положить $m = 1$, то получим 8)) и может быть доказано с помощью решения задачи, также являющейся обобщением ранее рассмотренной: *Каким числом способов можно выбрать из n кандидатов k депутатов и среди последних m членов президиума?*

10) **1-й способ.** Докажем тождество математической индукцией по k. *База индукции.* При $k = 0$ имеем верное равенство:

$$C_m^m = C_{m+1}^{m+1} = 1.$$

Индукционный шаг. Пусть доказываемое утверждение верно при $k = n$:

$$\sum_{p=0}^{n} C_{m+p}^m = C_{m+n+1}^{m+1}.$$

Прибавив к обеим частям равенства C_{m+n+1}^m, получим

$$\sum_{p=0}^{n+1} C_{m+p}^m = C_{m+n+1}^{m+1} + C_{m+n+1}^m = [\text{в силу 2})] = C_{m+n+2}^{m+1}.$$

Таким образом, соотношение 10) справедливо и при $k = n+1$.

2-й способ. Общее число $(m+1)$-элементных подмножеств множества $\{1, 2, 3, \ldots, m+k+1\}$ равно C_{m+k+1}^{m+1} (правой части доказываемого тождества). Будем

классифицировать указанные подмножества по их наибольшему элементу, который, очевидно, принимает значения $m+1, m+2, \ldots, m+k+1$. Найдем число подмножеств с наибольшим элементом $m+p+1$. Поскольку наибольший элемент уже выбран, оставшиеся m элементов выбираются из множества $\{1, 2, \ldots, m+p\}$ — значит, число таких подмножеств равно C_{m+p}^{m}. Суммируя C_{m+p}^{m} по p от 0 до k, вновь получим общее число $(m+1)$-элементных подмножеств (левую часть доказываемого тождества).

11) Тождество доказывается на основе предыдущего:

$$\sum_{p=0}^{k} C_{n+p}^{m} = \sum_{i=m}^{n+k} C_i^m - \sum_{i=m}^{n-1} C_i^m = [p = i - m] =$$

$$= \sum_{p=0}^{n+k-m} C_{m+p}^{m} - \sum_{p=0}^{n-1-m} C_{m+p}^{m} = C_{n+k+1}^{m+1} - C_n^{m+1}.$$

12) Решим задачу: *Каким числом способов можно из n кандидатов выбрать m депутатов и среди депутатов некоторых (может быть, всех, а может быть, никого) наградить?*

С одной стороны, депутаты выбираются C_n^m способами, а награжденные выделяются 2^m способами (столько подмножеств имеет множество из m элементов), и, значит, ответ к задаче: $C_n^m \cdot 2^m$.

С другой стороны, если число награждаемых депутатов равно k $(0 \leqslant k \leqslant m)$, то их можно выбрать C_n^k способами, после чего остальные $m-k$ депутатов выбираются C_{n-k}^{m-k} способами. Суммируя $C_n^k C_{n-k}^{m-k}$ по k от 0 до m, вновь получим ответ к рассматриваемой задаче. Тождество доказано.

13) Используя соотношение 8), преобразуем общий член суммы:

$$\frac{1}{n} C_n^k = \frac{1}{k} C_{n-1}^{k-1}.$$

Имеем:

$$\sum_{n=k}^{m} \frac{1}{n} C_n^k = \sum_{n=k}^{m} \frac{1}{k} C_{n-1}^{k-1} = \frac{1}{k} \sum_{n=k}^{m} C_{n-1}^{k-1} = [\text{в силу 10})] = \frac{1}{k} C_m^k.$$

14) **1-й способ.**

$$\sum_{k=1}^{n} (-1)^{k-1} \frac{1}{k} C_n^k = \sum_{k=1}^{n} C_n^k \int_0^1 (-x)^{k-1}\, dx = \int_0^1 \left(\sum_{k=1}^{n} C_n^k (-x)^{k-1} \right) dx =$$

$$= -\int_0^1 \left(\frac{1}{x} \sum_{k=1}^{n} C_n^k (-x)^k \right) dx = -\int_0^1 \frac{1}{x} ((1-x)^n - 1)\, dx = \begin{bmatrix} t = 1-x; \\ dt = -dx \end{bmatrix}$$

$$= \int_1^0 \frac{t^n - 1}{1-t}\, dt = \int_0^1 \frac{t^n - 1}{t-1}\, dt = \int_0^1 (1 + t + t^2 + \ldots + t^{n-1})\, dt =$$

$$= 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} = \sum_{k=1}^{n} \frac{1}{n}.$$

2-й способ. Воспользовавшись 13) тождеством, заменим $\frac{1}{k}C_n^k$ на $\sum\limits_{j=k}^{n} \frac{1}{j}C_j^k$ и в полученной двойной сумме поменяем порядок суммирования:

$$\sum_{k=1}^{n}(-1)^{k-1}\frac{1}{k}C_n^k = \sum_{k=1}^{n}(-1)^{k-1}\sum_{j=k}^{n}\frac{1}{j}C_j^k =$$

$$= \sum_{j=1}^{n}\frac{1}{j}\sum_{k=1}^{j}(-1)^{k-1}C_j^k = [\text{в силу 5)}] = \sum_{j=1}^{n}\frac{1}{j}. \blacktriangleright$$

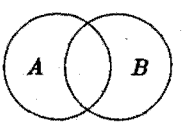
§ 7. Формула включения-исключения

Мощностью конечного множества называется число его элементов. Мощность множества A будем обозначать $|A|$. В этом параграфе мы выведем формулу для мощности объединения конечного числа конечных множеств. В случае двух и трех множеств имеем соответственно:

$$|A \cup B| = |A| + |B| - |A \cap B|;$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Действительно, в сумме $|A| + |B|$ каждый элемент, принадлежащий одновременно и A, и B, учитывается дважды; поэтому после вычитания из $|A| + |B|$ мощности пересечения этих множеств получим в точности число элементов $A \cup B$. Аналогичными рассуждениями обосновывается вторая формула (рис. 1).



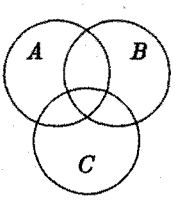


Рис. 1. Геометрическая иллюстрация формул включения-исключения

В общем случае имеет место следующая

Теорема 3 (формула включения-исключения). *Пусть $A_1, A_2, \ldots, A_n$ — конечные множества. Тогда*

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{i=1}^{n}|A_i| - \sum_{1 \leqslant i < j \leqslant n}|A_i \cap A_j| +$$

$$+ \sum_{1 \leqslant i < j < k \leqslant n}|A_i \cap A_j \cap A_k| - \ldots + (-1)^{n-1}|A_1 \cap A_2 \cap \ldots \cap A_n|. \qquad (1)$$

◄ Возьмем произвольный элемент из объединения данных n множеств и подсчитаем его «вклад» в правую часть доказываемой формулы. Пусть элемент входит ровно в m множеств A_i $(m \leqslant n)$. Тогда в сумме $\sum |A_i|$ он учитывается m раз, в сумме $\sum |A_i \cap A_j|$ — C_m^2 раз (в стольких попарных пересечениях m множеств он содержится), в сумме $\sum |A_i \cap A_j \cap A_k|$ — C_m^3 раз и т.д. Общий вклад элемента выражается формулой $m - C_m^2 + C_m^3 - \ldots + (-1)^{m-1} C_m^m$ и равен 1 в силу тождества 5) предыдущего параграфа. Таким образом, правая часть (1) равна общему числу элементов из объединения n множеств, что и требовалось доказать. ►

Замечание. При решении многих задач применяется следующий вариант формулы включения-исключения. Пусть для любого i множество A_i является подмножеством некоторого множества A. Обозначим через $\overline{A}_i$ дополнение к A_i до множества A: $\overline{A}_i = A \setminus A_i$. Как известно, дополнение к объединению множеств есть пересечение их дополнений [2]; поэтому

$$|\overline{A}_1 \cap \ldots \cap \overline{A}_n| = |A \setminus (A_1 \cup \ldots \cup A_n)| = |A| - |A_1 \cup \ldots \cup A_n|.$$

Воспользовавшись формулой (1), окончательно получим

$$\boxed{|\overline{A}_1 \cap \ldots \cap \overline{A}_n| = |A| - \sum_{i=1}^{n} |A_i| + \sum_{1 \leqslant i < j \leqslant n} |A_i \cap A_j| - \ldots + (-1)^n |A_1 \cap A_2 \cap \ldots \cap A_n|.}$$

§ 8. Функция Эйлера

Применяя формулу включения-исключения, выведем формулу для функции Эйлера $\varphi(m)$. Напомним, что $\varphi(m)$ — количество натуральных чисел, не превосходящих m и взаимно простых с m. Пусть натуральное число m имеет следующее каноническое разложение на простые множители: $m = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$. Введем в рассмотрение следующие множества: $A = \{1, 2, \ldots, m\}$, $A_i = \{j \mid j \in A, j \vdots p_i\}$, $\overline{A}_i = A \setminus A_i$ $(i = 1, \ldots, n)$. Число взаимно просто с m тогда и только тогда, когда оно не делится ни на один простой делитель m. Поэтому множество чисел, не превосходящих m и взаимно простых с m, совпадает с множеством $\overline{A}_1 \cap \overline{A}_2 \cap \ldots \cap \overline{A}_n$. Таким образом, $\varphi(m)$ есть мощность указанного множества.

Отметим, что $A_i = \{p_i, 2p_i, \ldots, m\}$ и $|A_i| = \frac{m}{p_i}$. Несложно найти и мощность пересечения двух множеств: $|A_i \cap A_j| = \frac{m}{p_i p_j}$ (множество $A_i \cap A_j$ состоит из чисел, кратных произведению $p_i p_j$), и вообще мощность пересечения любого числа из множеств A_i:

$$\boxed{|A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_s}| = \frac{m}{p_{i_1} p_{i_2} \cdots p_{i_s}}}$$

(рассуждения аналогичны). Теперь все готово для того, чтобы применить формулу включения исключения. Имеем:

$$\varphi(m) = |\overline{A}_1 \cap \ldots \cap \overline{A}_n| = |A| - \sum_{i=1}^{n} |A_i| + \sum_{1 \leqslant i < j \leqslant n} |A_i \cap A_j| - \ldots +$$

[2] Закон де Моргана.

$$+(-1)^s \sum_{1\leqslant i_1<\ldots<i_s\leqslant n} |A_{i_1}\cap\ldots\cap A_{i_s}| + \ldots + (-1)^n |A_1\cap A_2\cap\ldots\cap A_n| =$$

$$= m - \sum \frac{m}{p_i} + \sum \frac{m}{p_i p_j} - \ldots + (-1)^s \sum \frac{m}{p_{i_1}\cdots p_{i_s}} + \ldots + (-1)^n \frac{m}{p_1\cdots p_n} =$$

$$= m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_n}\right).$$

(При раскрытии скобок в последнем произведении получается предыдущая сумма.) Итак, доказано, что

$$\boxed{\varphi(m) = m\prod_{i=1}^{n}\left(1-\frac{1}{p_i}\right).}$$

§ 9. Задача о беспорядках и встречах

В популярной литературе по теории вероятностей часто встречается

Задача о рассеянной секретарше. *Секретарше нужно отправить n различных писем по n различным адресам. Она подписывает конверты и случайным образом вкладывает письма в конверты. Какова вероятность того, что ни одно письмо не дойдет до своего адресата?*

Оказывается, искомая вероятность не так мала, как может показаться на первый взгляд, и, что замечательно, имеет пределом (при $n\to\infty$) $\frac{1}{e} = 0{,}367879\ldots$. Данная задача является (литературным) вариантом широко известной комбинаторной *задачи о беспорядках*, решением которой мы сейчас и займемся.

Перестановка $(a_1, a_2, \ldots a_n)$ чисел $1, 2, \ldots, n$ называется *беспорядком*, если для любого i $a_i \neq i$. Через D_n обозначим число всех беспорядков из n элементов. Заметим, что в задаче о секретарше искомая вероятность P_n равна отношению D_n к общему числу всех перестановок n элементов: $P_n = \frac{D_n}{n!}$.

Пусть $A = \{(a_1, a_2, \ldots, a_n)\}$ — множество всех перестановок чисел $1, 2, \ldots, n$; $A_i = \{(a_1, a_2, \ldots, a_n) \mid a_i = i\}$ — множество тех перестановок, у которых на i-м месте стоит число i, $\overline{A}_i = A \setminus A_i$ $(i = 1, \ldots, n)$. Тогда множество беспорядков совпадает с пересечением множеств $\overline{A}_1\cap\overline{A}_2\cap\ldots\cap\overline{A}_n$, а D_n равно его мощности. Для того чтобы применить формулу включения-исключения, нужно найти мощности соответствующих множеств.

Имеем: $|A| = n!$, $\forall\, i\ |A_i| = (n-1)!$ (так как во всех перестановках, входящих в A_i, положение одного числа фиксировано, то число таких перестановок совпадает с числом перестановок $n-1$ элементов), если $i \neq j$, то $|A_i\cap A_j| = (n-2)!$ (здесь фиксированы положения двух элементов); вообще: мощность пересечения k множеств равна $(n-k)!$ (k чисел «знают» свои места, переставляются оставшиеся $n-k$).

Заметим, наконец, что n множеств A_i образуют C_n^2 попарных пересечений, ..., C_n^k пересечений по k множеств $(k \leqslant n)$. Таким образом,

$$D_n = |\overline{A}_1\cap\ldots\cap\overline{A}_n| = |A| - \sum_{i=1}^{n}|A_i| + \sum_{1\leqslant i<j\leqslant n}|A_i\cap A_j| - \ldots +$$

$$+(-1)^k \sum_{1\leqslant i_1<\ldots<i_k\leqslant n} |A_{i_1}\cap\ldots\cap A_{i_k}|+\ldots+(-1)^n|A_1\cap A_2\cap\ldots\cap A_n| =$$

$$= n! - C_n^1(n-1)! + C_n^2(n-2)! - \ldots + (-1)^k C_n^k(n-k)! + \ldots + (-1)^n C_n^n(n-n)! =$$

$$= \sum_{k=0}^{n}(-1)^k C_n^k(n-k)! = \sum_{k=0}^{n}(-1)^k \frac{n!}{k!(n-k)!}(n-k)! =$$

$$= \sum_{k=0}^{n}(-1)^k \frac{n!}{k!} = n!\left(1-\frac{1}{1!}+\frac{1}{2!}-\frac{1}{3!}+\ldots+(-1)^n\frac{1}{n!}\right). \qquad (1)$$

Возвратимся (в последний раз) к задаче о секретарше. Из полученной формулы для числа беспорядков следует:

$$\lim_{n\to\infty} P_n = \lim_{n\to\infty}\frac{D_n}{n!} = \lim_{n\to\infty}\left(1-\frac{1}{1!}+\frac{1}{2!}-\frac{1}{3!}+\ldots+(-1)^n\frac{1}{n!}\right) = e^{-1}.$$

Рекуррентные формулы для числа беспорядков. На основе формулы (1) получим интересные соотношения для D_n.

$$D_{n+1} = (n+1)!\left(1-\frac{1}{1!}+\frac{1}{2!}-\ldots+(-1)^n\frac{1}{n!}+(-1)^{n+1}\frac{1}{(n+1)!}\right) =$$

$$= (-1)^{n+1} + (n+1)n!\left(1-\frac{1}{1!}+\frac{1}{2!}-\ldots+(-1)^n\frac{1}{n!}\right) =$$

$$= (-1)^{n+1} + (n+1)D_n. \qquad (2)$$

Полученное рекуррентное соотношение

$$\boxed{D_{n+1} = (-1)^{n+1} + (n+1)D_n}$$

очень похоже на соотношение, позволяющее рекуррентно вычислять факториалы: $(n+1)! = (n+1)\cdot n!$ (все отличие — слагаемое $(-1)^{n+1}$). В связи с этим обстоятельством число беспорядков D_n иногда называют *субфакториалом* (или *псевдофакториалом*). Зная, что $D_1 = 0$, с помощью (2) найдем несколько значений D_n:

$$D_2 = 1; \quad D_3 = 3\cdot 1 - 1 = 2; \quad D_4 = 4\cdot 2 + 1 = 9; \quad D_5 = 5\cdot 9 - 1 = 44.$$

Еще одно соотношение получается так:

$$D_{n+2} = (n+2)D_{n+1} + (-1)^{n+2} = (n+1)D_{n+1} + (-1)^{n+2} + D_{n+1} =$$

$$= (n+1)D_{n+1} + (-1)^{n+2} + (n+1)D_n + (-1)^{n+1} = (n+1)(D_{n+1} + D_n).$$

Заметим, что рекуррентной зависимости

$$\boxed{a_{n+2} = (n+1)(a_{n+1} + a_n)}$$

наряду с последовательностью псевдофакториалов D_n удовлетворяет и последовательность (обычных) факториалов $n!$ (убедитесь в этом самостоятельно).

Обобщением задачи о беспорядках является *задача о встречах*. Говорят, что перестановка $(a_1, a_2, \ldots, a_n)$ чисел $1, 2, \ldots, n$ *имеет* k *встреч*, если ровно k чисел

«остаются на своих местах» (когда порядковый номер элемента в перестановке совпадает с его величиной: $a_i = i$). Число перестановок n элементов с k встречами обозначим $D_{n,k}$. Отметим несколько частных случаев: $D_{n,0} = D_n$; $D_{n,n} = 1$; $D_{n,n-1} = 0$. Последнее равенство вытекает из того, что если *все* элементы перестановки, *кроме одного*, занимают «свои» места, то и этому элементу не остается ничего другого, как занять место, чей номер совпадает с ним, и, таким образом, *ровно* $n-1$ встреч не может быть!

Каждую перестановку n элементов с k встречами можно сгенерировать, выполняя следующую процедуру:

1-й шаг. Выбрать k элементов, остающихся на своих местах.

2-й шаг. Оставшиеся $n-k$ элементов переставить так, чтобы ни один из них не занял «своего» места.

Первый шаг выполняется C_n^k способами, второй — D_{n-k} способами. С помощью правила произведения получаем формулу для числа встреч

$$\boxed{D_{n,k} = C_n^k D_{n-k}.}$$

§ 10. Число сюръекций

Пусть X и Y — некоторые множества. Отображение $f : X \to Y$ называется *сюръекцией*, если всякий элемент множества Y является образом некоторого элемента множества X:

$$\forall y \in Y \quad \exists x \in X \quad f(x) = y.$$

Определим *образ множества* при заданном отображении как множество образов всех его элементов: $f(X) = \{f(x) \mid x \in X\}$. Отображение $f : X \to Y$ является сюръекцией тогда и только тогда, когда $f(X) = Y$.

Пусть X и Y — конечные множества:

$$X = \{x_1, x_2, \ldots, x_n\}, \quad Y = \{y_1, y_2, \ldots, y_m\},$$

причем $n \geqslant m$. Найдем число всех сюръекций $f : X \to Y$.

Введем в рассмотрение следующие множества:

$$A = \{f : X \to Y\}$$

— множество всех отображений из X в Y;

$$F = \{f : X \to Y \mid f(X) = Y\}$$

— множество всех сюръекций;

$$A_i = \{f : X \to Y \mid y_i \notin f(X)\}, \quad \overline{A}_i = A \setminus A_i = \{f : X \to Y \mid y_i \in f(X)\} \quad (i = 1, \ldots, m).$$

Легко видеть, что $F = \overline{A}_1 \cap \overline{A}_2 \cap \ldots \cap \overline{A}_m$. Вновь находит применение формула включения-исключения!

Каждое отображение $f : X \to Y$ можно задать размещением (с повторениями) объема n: $(f(x_1), f(x_2), \ldots, f(x_n))$. Для отображений $f \in A$ элементы указанного размещения выбираются из m-элементного множества Y; для $f \in A_i$ — из $(m-1)$-элементного множества $Y \setminus \{y_i\}$; для $f \in A_i \cap A_j$ $(i \neq j)$ — из $(m-2)$-элементного

множества $Y \setminus \{y_i, y_j\}$ и т. д. Формула для числа размещений с повторениями уже известна читателю; применив ее, получим

$$|A| = m^n; \quad |A_i| = (m-1)^n; \quad |A_i \cap A_j| = (m-2)^n; \quad \ldots .$$

Таким образом,

$$|F| = |\overline{A}_1 \cap \ldots \cap \overline{A}_m| = |A| - \sum_{i=1}^{m} |A_i| + \sum_{1 \leqslant i < j \leqslant m} |A_i \cap A_j| - \ldots +$$

$$+(-1)^k \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant m} |A_{i_1} \cap \ldots \cap A_{i_k}| + \ldots + (-1)^m |A_1 \cap A_2 \cap \ldots \cap A_m| =$$

$$= m^n - m \cdot (m-1)^n + C_m^2 (m-2)^n - \ldots + (-1)^{m-1} \cdot C_m^{m-1} \cdot 1^n.$$

Итак, число сюръекций n-элементного множества в m-элементное множество равно

$$\boxed{|F| = \sum_{k=0}^{m-1} (-1)^k C_m^k (m-k)^n.}$$

Пример. n различных шаров нужно разместить по m различным ящикам так, чтобы ни один ящик не остался пустым. Каким числом способов это можно сделать?

◀ Распределение шаров по ящикам можно рассматривать как *отображение множества шаров в множество ящиков*; отсутствие пустых ящиков соответствует тому, что указанное отображение является сюръекцией. Число сюръекций подсчитано выше. ▶

§ 11. Обобщение формулы включения-исключения

Пусть A — некоторое множество, $A_1, A_2, \ldots, A_n$ — его подмножества. Определим функцию $w(n)$ следующими соотношениями:

$$w(0) = |A|, \quad w(1) = \sum_{i=1}^{n} |A_i|, \quad w(k) = \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} |A_{i_1} \cap \ldots \cap A_{i_k}| \qquad (k \leqslant n).$$

Пусть $N(r)$ — число элементов множества A, которые принадлежат ровно r различным множествам A_i (если $r = 0$, то — ни одному). С помощью введенных функций формула включения-исключения принимает следующий вид:

$$N(0) = w(0) - w(1) + w(2) - \ldots + (-1)^n w(n).$$

В этом параграфе мы докажем, что имеет место и более общее соотношение:

$$\boxed{N(r) = w(r) - C_{r+1}^1 w(r+1) + C_{r+2}^2 w(r+2) + \ldots + (-1)^{n-r} C_n^{n-r} w(n).} \quad (1)$$

Возьмем произвольный элемент множества A и подсчитаем его «вклад» в правую часть доказываемого равенства. Возможны следующие 3 случая:

1) Элемент входит менее чем в r различных множеств A_i, тогда он не принадлежит никакому пересечению r и более упомянутых множеств, и вклад его в правую часть (1) равен нулю.

2) Элемент принадлежит *ровно* r множествам A_i, тогда он принадлежит ровно одному пересечению r множеств и не принадлежит никакому пересечению большего числа множеств; таким образом, вклад элемента равен 1.

3) Элемент принадлежит k множествам A_i, причем $k > r$. Тогда он входит в C_k^r пересечений r множеств A_i, в C_k^{r+1} пересечений $r+1$ множеств A_i, в C_k^j пересечений j множеств A_i $(j \leqslant k)$. Вклад указанного элемента в правую часть (1) равен

$$\sum_{j=r}^{k}(-1)^{j-r}C_j^{j-r}C_k^j = [\text{в силу комбинаторного тождества 1)}] =$$

$$= \sum_{j=r}^{k}(-1)^{j-r}C_j^rC_k^j = [\text{в силу 9)}] = \sum_{j=r}^{k}(-1)^{j-r}C_k^rC_{k-r}^{j-r} =$$

$$= [i = j-r] = C_k^r\sum_{i=0}^{k-r}(-1)^iC_{k-r}^i = [\text{в силу 4)}] = 0.$$

Таким образом, формула из правой части (1) дает число элементов A, входящих ровно в r подмножеств A_i. Это и требовалось доказать.

Пример. Из 100 студентов 60 читают журнал A, 50 читают журнал B, 50 — C, 30 — A и B, 20 — B и C, 40 — A и C, 10 — A, B и C. Сколько студентов не читает ни один из трех журналов? Сколько студентов читает ровно два журнала?

◄ В данной задаче в роли исходного множества A выступает множество из 100 студентов, подмножества A_1, A_2, A_3 составляют студенты, читающие соответствующие журналы. Имеем: $w(0) = 100$; $w(1) = 60+50+50 = 160$; $w(2) = 30+20+40 = 90$; $w(3) = 10$. Тогда $N(0) = w(0)-w(1)+w(2)-w(3) = 20$; $N(2) = w(2)-C_3^1w(3) = 90-3\cdot 10 = 60$. ►

Ответ. 20 человек не читают журналов, 60 человек читают по два журнала.

§ 12. Числа Стирлинга II рода

Числом Стирлинга II рода $S(n, k)$ называют число неупорядоченных разбиений[3] n-элементного множества на k непустых множеств. Элементы разбиения будем называть *блоками*.

Пример. Вычислим $S(6, 2)$. Число неупорядоченных разбиений 6-элементного множества на два блока, один из которых содержит 1 элемент, равно $C_6^1 = 6$. Если в одном из двух блоков 2 элемента, то число соответствующих разбиений равно $C_6^2 = 15$. Наконец, если оба блока, на которые разбивается исходное множество, — 3-элементные, то число таких разбиений — $C_6^3/2 = 10$. Таким образом, $S(6, 2) = 6+15+10 = 31$.

Очевидно выполнение следующих «граничных условий»: при любом натуральном n $S(n, 1) = 1$, $S(n, n) = 1$, при $k > n$ $S(n, k) = 0$.

[3] О понятии разбиения см. § 2 гл. LXVII.

По определению полагают

$$\boxed{S(0,0)=1, \quad \text{при любом натуральном } n \quad S(n,0)=0, \quad S(0,n)=0.} \tag{1}$$

С помощью результатов § 10 мы сейчас выведем формулу для чисел Стирлинга II рода. Каждую сюръекцию n-элементного множества A в k-элементное ($n > k$) можно рассматривать как *упорядоченное* разбиение A на k непустых частей (каждая часть состоит из элементов, имеющих один и тот же образ при заданном сюръективном отображении). Пусть $S_{n,k}$ — число таких сюръекций:

$$S_{n,k}=\sum_{j=0}^{k-1}(-1)^j C_k^j (k-j)^n = [i=k-j] = (-1)^k \sum_{i=1}^{k} C_k^i (-1)^i i^n.$$

Всякое *упорядоченное* разбиение на k блоков можно получить в результате выполнения следующей процедуры:

1) сделать *неупорядоченное* разбиение;
2) упорядочить его (т. е. перенумеровать полученные k множеств числами $1, 2, \ldots, k$).

Первый шаг процедуры может быть выполнен $S(n,k)$ способами, второй — $k!$ способами. С помощью правила произведения получаем соотношение

$$S_{n,k} = S(n,k) \cdot k!,$$

или

$$\boxed{S(n,k)=\frac{(-1)^k}{k!}\sum_{i=1}^{k} C_k^i (-1)^i i^n \quad (k \in \mathbb{N}).}$$

Для вычисления чисел Стирлинга удобно применять следующую рекуррентную формулу:

$$\boxed{S(n,k)=S(n-1,k-1)+kS(n-1,k).} \tag{2}$$

Докажем ее. Пусть A — множество из n элементов; x — некоторый фиксированный элемент A. Число разбиений A на k блоков, среди которых содержится блок $\{x\}$, равно $S(n-1,k-1)$ (множество $A \setminus \{x\}$, мощность которого $n-1$, разбивается на $k-1$ блоков). Всякое разбиение, не содержащее блока $\{x\}$, можно получить,

1) разбив множество $A \setminus \{x\}$ на k блоков;
2) добавив элемент x к одному из полученных блоков.

Первое действие выполняется $S(n-1,k)$ способами, второе — k способами. Таким образом, число разбиений второго вида равно $kS(n-1,k)$, а общее число разбиений равно $S(n-1,k-1)+kS(n-1,k)$, что и требовалось доказать.

Применяя соотношения (1) и (2), составим таблицу значений $S(n,k)$ для $0 \leqslant n, k \leqslant 8$ (табл. 3).

Анализируя таблицу, можно заметить еще одно любопытное соотношение:

$$\boxed{S(n,n-1)=C_n^2.}$$

Таблица 3

Числа Стирлинга II рода $S(n, k)$

k / n	0	1	2	3	4	5	6	7	8
0	1	0	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0	0
2	0	1	1	0	0	0	0	0	0
3	0	1	3	1	0	0	0	0	0
4	0	1	7	6	1	0	0	0	0
5	0	1	15	25	10	1	0	0	0
6	0	1	31	90	65	15	1	0	0
7	0	1	63	301	350	140	21	1	0
8	0	1	127	966	1701	1050	266	28	1

Действительно, если n элементов разбиваются на $n-1$ блоков, то все блоки, кроме одного, будут одноэлементными, и разбиение определяется тем, какие два элемента составят этот блок.

Для дальнейшего нам понадобится следующая рекуррентная зависимость для чисел Стирлинга II рода:

$$\boxed{S(n, k) = \sum_{b=1}^{n-(k-1)} S(n-b, k-1) C_{n-1}^{b-1}.}$$

Для доказательства рассмотрим блок B, содержащий некоторый фиксированный элемент x. Мощность b блока B может быть равна $1, 2, \ldots, n-(k-1)$, так как в остальных блоках не менее $k-1$ элементов. Подсчитаем число разбиений с фиксированным значением b. В этом случае блок B можно сформировать C_{n-1}^{b-1} способами (к элементу x нужно добавить еще $b-1$ элементов). Не вошедшие в данный блок $n-b$ элементов $S(n-b, k-1)$ способами могут быть разбиты на $k-1$ блоков. Значит, число разбиений, в которых $|B| = b$, равно $S(n-b, k-1)C_{n-1}^{b-1}$. Суммируя это выражение по возможным значениям b, получаем искомую формулу, которой удобно придать следующий вид:

$$S(n, k) = \sum_{b=1}^{n-(k-1)} S(n-b, k-1) C_{n-1}^{b-1} = \left[\begin{array}{c} n-b=i; \\ C_{n-1}^{b-1} = C_{n-1}^{n-b} = C_{n-1}^{i} \end{array}\right] =$$

$$= \sum_{i=k-1}^{n-1} S(i, k-1) C_{n-1}^{i}. \tag{3}$$

Числом Белла B_n называют число *всех* неупорядоченных разбиений n-элементного множества. Его можно найти, просуммировав по k количества разбиений на k блоков:

$$\boxed{B_n = \sum_{k=0}^{n} S(n, k).} \tag{4}$$

Удобно считать, что $B_0 = 1$ (это согласуется с формулой (4); если $n > 0$, то $S(n, 0) = 0$ и в (4) нижнюю границу индекса суммирования можно заменить на 1). Выведем с помощью формул (3) и (4) рекуррентную формулу для чисел Белла; при $n > 0$ имеем

$$B_n = \sum_{k=1}^{n} S(n,k) = \sum_{k=1}^{n} \sum_{i=k-1}^{n-1} S(i,k-1)C_{n-1}^{i} = \sum_{i=0}^{n-1} C_{n-1}^{i} \sum_{k=1}^{i+1} S(i,k-1) = \sum_{i=0}^{n-1} C_{n-1}^{i} B_i.$$

В заключение данного параграфа установим очень важное свойство чисел Стирлинга II рода, которое иногда берут в качестве их определения. Оказывается, числа Стирлинга II рода являются коэффициентами разложения многочлена x^n $(n = 0, 1, 2, \ldots)$ по следующему базису в пространстве многочленов степени не выше n:

$$(x)_0 = 1, \quad (x)_1 = x, \quad (x)_2 = x(x-1),$$
$$(x)_3 = x(x-1)(x-2), \quad \ldots, \quad (x)_n = x(x-1)\ldots(x-n+1).$$

Теорема 4. *Для любого целого неотрицательного n справедливо тождество*

$$x^n = \sum_{k=0}^{n} S(n,k)(x)_k. \tag{5}$$

◀ Для $n = 0$ утверждение теоремы проверяется непосредственно; поэтому будем считать, что $n \in \mathbb{N}$.

Докажем сначала, что соотношение (5) справедливо, если x — натуральное число.

Пусть F — множество всех функций $f : A \to B$, где $|A| = n$, $|B| = x$.

С одной стороны, их число есть $\overline{A_x^n} = x^n$.

С другой стороны, будем классифицировать функции по мощности множества $f(A)$. Если $|f(A)| = k$, то, во-первых, множество $C = f(A)$ может быть выбрано C_x^k способами, а, во-вторых, при фиксированном C число функций $f : A \to C$ равно числу сюръекций $S_{n,k}$ (если $f(A) = C$, то функция $f : A \to C$ — сюръекция). Таким образом,

$$\left|\{f : A \to B, |f(A)| = k\}\right| = C_x^k \cdot S_{n,k} = C_x^k \cdot S(n,k) \cdot k! =$$
$$= \frac{x(x-1)\ldots(x-k+1)}{k!} \cdot S(n,k) \cdot k! = (x)_k \cdot S(n,k).$$

Просуммировав полученное выражение по k от 1 до x, вновь найдем мощность множества F:

$$|F| = \sum_{k=1}^{x} S(n,k)(x)_k.$$

Покажем, что верхнюю границу суммирования можно поменять с x на n, не изменив при этом суммы. Действительно, если $x < n$, то слагаемые в сумме, отвечающие значениям $k > x$, равны нулю, так как $(x)_k = 0$ (проверьте!); если же $x > n$, то при $k > n$ $S(n,k) = 0$ и соответствующие слагаемые в сумме также равны

нулю. Нижнюю границу суммирования можно заменить на 0, так как возникающее при этом дополнительное слагаемое $S(n, 0)$ равно нулю (поскольку $n \in \mathbb{N}$).

Итак, вычислив $|F|$ двумя способами, приходим к равенству

$$x^n = \sum_{k=0}^{n} S(n, k)(x)_k,$$

справедливому для *всех натуральных* x. Как известно из алгебры, если два многочлена n-й степени имеют одинаковые значения более, чем в n точках, то они тождественно равны[4]. Теорема доказана. ►

§ 13. Числа Стирлинга I рода

Как было показано в конце предыдущего параграфа, числа Стирлинга II рода $S(n, k)$ появляются при переходе от базиса $\{1, x, x^2, \ldots, x^n\}$ к базису $\{1, (x)_1, (x)_2, \ldots, (x)_n\}$ в пространстве многочленов степени не выше n. *Числа Стирлинга I рода* $s(n, k)$ позволяют совершить обратный переход; они определяются как коэффициенты при последовательных степенях x многочлена $(x)_n$ $(n \geqslant 0)$:

$$\boxed{(x)_n = \sum_{k=0}^{n} s(n, k)x^k.} \tag{1}$$

Очевидно, что

$$\boxed{s(n, n) = 1 \quad (n \geqslant 0).} \tag{2}$$

Полагают также, что

$$\boxed{s(n, k) = 0, \quad \text{если} \quad k > n.} \tag{3}$$

Докажем, что имеет место следующее рекуррентное соотношение:

$$\boxed{s(n, k) = s(n-1, k-1) - (n-1)s(n-1, k) \quad (0 < k < n).} \tag{4}$$

Действительно, разложив по степеням x многочлены $(x)_n$ и $(x)_{n-1}$ в тождестве

$$(x)_n = (x)_{n-1} \cdot (x - n + 1),$$

имеем:

$$\sum_{k=0}^{n} s(n, k)x^k = (x - n + 1) \sum_{k=0}^{n-1} s(n-1, k)x^k =$$

$$= \sum_{k=0}^{n-1} s(n-1, k)x^{k+1} - (n-1) \sum_{k=0}^{n-1} s(n-1, k)x^k =$$

[4] Разность указанных многочленов является многочленом степени не выше n, у которого более n корней. По известному следствию из *основной теоремы алгебры* такой многочлен тождественно равен нулю.

$$= s(n-1, n-1)x^n - (n-1)s(n-1, 0) + \sum_{k=1}^{n-1} \big(s(n-1, k-1) - (n-1)s(n-1, k)\big)x^k.$$

Приравнивая коэффициенты в левой и правой частях тождества при одинаковых степенях x, получаем требуемое.

С помощью соотношений (2), (3) и (4), составим таблицу значений $s(n, k)$ для $0 \leqslant n,\ k \leqslant 8$ (табл. 4).

Таблица 4

Числа Стирлинга I рода $s(n, k)$

k / n	0	1	2	3	4	5	6	7	8
0	1	0	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0	0
2	0	−1	1	0	0	0	0	0	0
3	0	2	−3	1	0	0	0	0	0
4	0	−6	11	−6	1	0	0	0	0
5	0	24	−50	35	−10	1	0	0	0
6	0	−120	274	−225	85	−15	1	0	0
7	0	720	−1764	1624	−735	175	−21	1	0
8	0	−5040	13 068	−13 132	6769	−1960	322	−28	1

Глядя на таблицу, нельзя не заметить «шахматный» порядок расстановки знаков коэффициентов. Эту закономерность нетрудно доказать. С одной стороны, многочлен

$$(-x)_n = (-x)(-x-1)\dots(-x-n+1) = (-1)^n x(x+1)\dots(x+n-1)$$

при разложении по степеням x имеет коэффициенты одного знака ($(-1)^n$). С другой стороны, его можно представить в виде

$$(-x)_n = \sum_{k=0}^{n} s(n, k)(-x)^k = (-1)^n \sum_{k=0}^{n} s(n, k)(-1)^{k-n}x^k,$$

откуда следует, что $(-1)^{k-n}s(n, k) > 0$ при $1 \leqslant k \leqslant n$, то есть если $k - n$ — четное число, то $s(n, k) > 0$, если $k - n$ — нечетное число, то $s(n, k) < 0$.

В заключение данного параграфа отметим

Связь между числами Стирлинга I и II рода

Представив для произвольного неотрицательного n многочлен x^n в виде

$$x^n = \sum_{k=0}^{n} S(n, k)(x)_k = \sum_{k=0}^{n} S(n, k) \sum_{j=0}^{k} s(k, j)x^j,$$

изменим в полученной двойной сумме порядок суммирования:

$$x^n = \sum_{j=0}^{n} x^j \sum_{k=j}^{n} S(n, k)s(k, j).$$

Поскольку при $k < j$ имеем $s(k, j) = 0$, можно поменять нижний предел суммирования во внутренней сумме, не изменив при этом ее значения:

$$x^n = \sum_{j=0}^{n} x^j \sum_{k=0}^{n} S(n, k)s(k, j).$$

Из полученного тождества следует:

$$\boxed{\sum_{k=0}^{n} S(n, k)s(k, j) = \begin{cases} 1, & \text{если } j = n; \\ 0, & \text{если } j \neq n. \end{cases}}$$

Данное соотношение имеет простую матричную интерпретацию: произведение матриц (одинаковой размерности), составленных соответственно из чисел Стирлинга II и I рода, есть единичная матрица [5].

§ 14. Производящие функции

Производящей функцией для последовательности $a_0, a_1, \ldots, a_n, \ldots$ называется формальный степенной ряд

$$A(x) = \sum_{k=0}^{\infty} a_k x^k. \tag{1}$$

Термин «формальный» означает, что мы не находим область сходимости ряда $A(x)$, нигде не будем вычислять значений $A(x)$ для конкретных значений переменной x, будем лишь выполнять некоторые операции над такими рядами и определять коэффициенты при степенях x; таким образом, $A(x)$ интересует нас не как числовая функция от переменной x, а как «носитель» последовательности (a_k).

Суммой произвольных рядов

$$A(x) = \sum_{k=0}^{\infty} a_k x^k, \quad B(x) = \sum_{k=0}^{\infty} b_k x^k$$

называется ряд

$$A(x) + B(x) = \sum_{k=0}^{\infty} (a_k + b_k) x^k. \tag{2}$$

Произведением ряда $A(x)$ на число λ называется ряд

$$\lambda A(x) = \sum_{k=0}^{\infty} \lambda a_k x^k. \tag{3}$$

[5] Этот факт можно было предвидеть сразу, исходя из общих алгебраических соотношений: матрицы $S(i,j)$ и $s(i,j)$ $(0 \leqslant i, j \leqslant n)$ являются матрицами перехода от одного базиса к другому и обратно.

Произведением рядов $A(x)$ и $B(x)$ называется ряд

$$A(x)\cdot B(x)=\sum_{k=0}^{\infty}c_kx^k,\quad \text{где}\quad c_k=\sum_{i=0}^{k}a_ib_{k-i}. \tag{4}$$

Если в последовательности (a_k) лишь конечное число членов отлично от нуля, то ряд $A(x)$ можно рассматривать как многочлен. Если и в последовательности (b_k) все члены, начиная с некоторого, равны нулю, то ряд $B(x)$ — также многочлен, и формула (4) переходит в обычную формулу умножения многочленов.

Из курса математического анализа известно, что если степенной ряд сходится в некоторой окрестности нуля, то в этой окрестности его сумма является функцией, по отношению к которой сам ряд является рядом Маклорена:

$$a_k=\frac{A^{(k)}(0)}{k!}\quad \text{для любого}\quad k=0,1,2,\ldots .$$

Заметим, что если $A(x)$ и $B(x)$ — аналитические функции в окрестности нуля, то соотношения (2), (3), (4) будут справедливы для них и как для числовых функций. Сохраняющее операции сложения и умножения взаимно однозначное соответствие между функциями, аналитическими в окрестности нуля, и их рядами Маклорена, позволяет отождествить формальный ряд (1) с определяемой им аналитической функцией. В табл. 5 представлены производящие функции для некоторых простых последовательностей.

Покажем, например, как может быть получена производящая функция для последовательности неотрицательных целых чисел:

$$\sum_{k=0}^{\infty}kx^k=x\sum_{k=1}^{\infty}kx^{k-1}=x\sum_{k=1}^{\infty}(x^k)'=x\left(\sum_{k=1}^{\infty}x^k\right)'=x\left(\frac{x}{1-x}\right)'=\frac{x}{(1-x)^2}.$$

Таблица 5

последовательность (a_k)	производящая функция $A(x)$
$1, 1, \ldots, 1, \ldots$	$\dfrac{1}{1-x}$
$1, \dfrac{1}{1!}, \dfrac{1}{2!}, \ldots, \dfrac{1}{k!}, \ldots$	e^x
$1, 2, 2^2, \ldots, 2^k, \ldots$	$\dfrac{1}{1-2x}$
$0, 1, 2, \ldots, k, \ldots$	$\dfrac{x}{(1-x)^2}$
$C_n^0, C_n^1, \ldots, C_n^k, \ldots, C_n^n, 0, \ldots$	$(1+x)^n$
$1, \alpha, \dfrac{\alpha(\alpha-1)}{2!}, \ldots, \dfrac{(\alpha)_k}{k!}, \ldots$	$(1+x)^\alpha$
$S(n,0), S(n,1), \ldots, S(n,k), \ldots$	$(x)_n$

Применим аппарат производящих функций к решению следующей весьма общей по постановке задачи.

Найти a_k — число всех неупорядоченных k-элементных выборок с повторениями, удовлетворяющих заданным ограничениям на число вхождений в них каждого элемента генеральной совокупности $\{x_1, x_2, \ldots, x_n\}$: элемент x_i может присутствовать в выборке y_i раз, где y_i — элемент некоторого числового множества $X_i \subset \mathbb{N}_0$ $(i = 1, \ldots, n)$.

Проиллюстрируем постановку задачи на нескольких «игрушечных» примерах.

1) *Сколько разных наборов из k шаров можно получить, имея 1 синий шар, 2 одинаковых белых шара и 4 одинаковых красных шара?*
   Здесь генеральная совокупность состоит из синего, белого и красного шара. Возможное число вхождений каждого шара в набор определяется множествами $X_1 = \{0, 1\}$, $X_2 = \{0, 1, 2\}$, $X_3 = \{0, 1, 2, 3, 4\}$.
2) *В условии предыдущей задачи вводится дополнительное ограничение: число красных шаров в наборе должно быть нечетно.*
   Изменение коснется множества, определяющего допустимое число вхождений красного шара: $X_3 = \{1, 3\}$.

Пусть $A(x)$ — производящая функция для последовательности (a_k). Тогда справедливо следующее соотношение:

$$A(x) = \prod_{i=1}^{n} \sum_{y_i \in X_i} x^{y_i}. \tag{5}$$

Действительно, если «раскрыть скобки» в правой части (5), то получим:

$$\prod_{i=1}^{n} \sum_{y_i \in X_i} x^{y_i} = \sum_{y_1, \ldots y_n} x^{y_1} \ldots x^{y_n} = \sum_{k=0}^{\infty} a_k x^k,$$

где $a_k = \sum\limits_{y_1 + \ldots + y_n = k} 1$. В выражении для a_k суммирование производится по всем наборам $(y_1, \ldots, y_n)$ таким, что $\forall i \; y_i \in X_i$ и $y_1 + \ldots + y_n = k$, в результате чего получится искомое число k-выборок.

Возвращаясь к примеру 1), запишем для него производящую функцию:

$$A(x) = (1 + x)(1 + x + x^2)(1 + x + x^2 + x^3 + x^4) =$$
$$= 1 + 3x + 5x^2 + 6x^3 + 6x^4 + 5x^5 + 3x^6 + x^7.$$

Коэффициент при x^k есть число k-элементных наборов. Таким образом, можно составить 3 одноэлементных набора, 5 — двухэлементных, 6 — трехэлементных и т. д.

Во втором примере

$$A(x) = (1 + x)(1 + x + x^2)(x + x^3) = x + 2x^2 + 3x^3 + 3x^4 + 2x^5 + x^6.$$

Теперь одноэлементный набор может быть только один, существует 2 набора из двух элементов и т. д.

В заключение рассмотрим применение аппарата производящих функций к выводу формул для числа сочетаний (без повторений и с повторениями). В обоих случаях будем считать, что генеральная совокупность состоит из n элементов.

Сочетания. Каждый элемент в выборке встречается *не более одного раза*, т.е. $\forall i$ $X_i = \{0, 1\}$; k-выборка при этом является *сочетанием (без повторений) из n по k*. Производящая функция имеет вид:

$$A(x) = (1 + x)^n = \sum_{k=0}^{n} C_n^k x^k.$$

Сочетания с повторениями. Каждый элемент в выборке может появиться *любое число раз*: $\forall i$ $X_i = \mathbb{N}_0$, k-выборка при этом суть *сочетание с повторениями из n по k*. Производящая функция имеет вид:

$$A(x) = (1 + x + x^2 + \ldots)^n = \left(\frac{1}{1-x}\right)^n = (1-x)^{-n} =$$

$$= [\text{ биномиальный ряд }] = \sum_{k=0}^{\infty} \frac{-n(-n-1)\ldots(-n-k+1)}{k!}(-x)^k =$$

$$= \sum_{k=0}^{\infty} \frac{n(n+1)\ldots(n+k-1)}{k!}(-1)^k(-x)^k = \sum_{k=0}^{\infty} C_{n+k-1}^k x^k.$$

Таким образом, вновь получена формула для числа сочетаний с повторениями: $\overline{C_n^k} = C_{n+k-1}^k$.

В следующих параграфах данной главы аппарат производящих функций будет применен к решению ряда комбинаторных задач.

§ 15. Число счастливых билетов

Трамвайные билеты имеют шестизначные номера. Билет называют *счастливым*, если сумма его первых трех цифр равна сумме трех последних. Мы докажем, что число счастливых билетов H может быть выражено формулой

$$\boxed{H = \frac{1}{\pi}\int_0^{\pi}\left(\frac{\sin 10x}{\sin x}\right)^6 dx.}$$

Отметим сначала, что число счастливых билетов совпадает с числом билетов, у которых сумма цифр равна 27. Для доказательства этого факта покажем, что существует взаимно однозначное соответствие между множеством «счастливых» 6-значных номеров и множеством 6-значных номеров с суммой цифр 27. Это соответствие задается так. В произвольном «счастливом» номере заменим 3 последние цифры на цифры, дополняющие их до 9 (например, 147 624 → 147 375). Если сумма трех первых (и трех последних) цифр равна k, то после указанного преобразования сумма трех последних цифр станет равной $27 - k$, а общая сумма шести цифр будет равна 27.

Всякий 6-значный номер с суммой цифр k можно рассматривать как k-выборку, составленную из элементов генеральной совокупности $\{1, 10, 10^2, 10^3, 10^4, 10^5\}$, причем каждый элемент может встречаться не более 9 раз. Пусть a_k — число

таких k-выборок. Производящая функция для последовательности (a_k) такова:

$$A(x) = (1 + x + x^2 + \ldots + x^9)^6 = \left(\frac{x^{10} - 1}{x - 1}\right)^6.$$

Задача, которую мы решаем, сводится к вычислению a_{27}. *Дальнейшие выкладки будут понятны лишь читателям, знакомым с теорией функций комплексного переменного.* Для функции $\frac{A(x)}{x^{28}}$ искомое число будет *вычетом*, и вычислить его можно с помощью интеграла по единичной окружности с центром в начале координат комплексной плоскости:

$$a_{27} = \frac{1}{2\pi i} \oint\limits_{|x|=1} \left(\frac{x^{10} - 1}{x - 1}\right)^6 \frac{dx}{x^{28}} = [x = e^{i\varphi}] =$$

$$= \frac{1}{2\pi i} \int\limits_0^{2\pi} \left(\frac{e^{10i\varphi} - 1}{e^{i\varphi} - 1}\right)^6 \frac{ie^{i\varphi}}{e^{28i\varphi}}\, d\varphi = \frac{1}{2\pi} \int\limits_0^{2\pi} \left(\frac{e^{5i\varphi} - e^{-5i\varphi}}{e^{i\varphi/2} - e^{-i\varphi/2}}\right)^6 d\varphi =$$

$$= \frac{1}{2\pi} \int\limits_0^{2\pi} \left(\frac{\sin 5\varphi}{\sin(\varphi/2)}\right)^6 d\varphi = \left[y = \frac{\varphi}{2}\right] = \frac{1}{\pi} \int\limits_0^{\pi} \left(\frac{\sin 10y}{\sin y}\right)^6 dy.$$

Заметим, что точно так же можно получить число «счастливых» $2n$-значных номеров в k-ичной системе счисления:

$$\frac{1}{\pi} \int\limits_0^{\pi} \left(\frac{\sin kx}{\sin x}\right)^{2n} dx.$$

Таким образом, общее решение классической *дискретной* задачи записывается с помощью *интеграла* от тригонометрической функции!

Чему все-таки равно число (традиционных) счастливых билетов? Ответ: **55252** (примерно каждый восемнадцатый билет — счастливый). Наиболее быстрый практический способ получения этого результата состоит в последовательном вычислении коэффициентов при степенях x не выше 27-й в разложениях многочленов $P_i(x) = (1 + x + x^2 + \ldots + x^9)^i$ для $i = 1, 2, \ldots, 5$ и последующем определении коэффициента при x^{27} в многочлене $P_6(x)$. Выкладки могут быть облегчены следующим соотношением: пусть $P_i(x) = \sum\limits_{k=0}^{9i} a_{i,k}x^k$, тогда $a_{i,k} = a_{i,9i-k}$ (докажите его!). Несложно получить рекуррентную формулу для вычисления коэффициентов $P_i(x)$ через коэффициенты предшествующего многочлена $P_{i-1}(x)$. Попробуйте это сделать и, применяя найденную формулу, не более чем через 5 минут Вы сможете убедиться в правильности приведенного ответа!

§ 16. Число бинарных деревьев с n вершинами

Бинарное дерево T определяется *рекурсивно* следующим образом: $T = \varnothing$ (*пустое дерево*) или $T = \langle L, c, R\rangle$ — упорядоченная тройка, где c — *корень* дерева (элемент некоторого множества), L и R — бинарные деревья; L и R называют

соответственно левым и правым поддеревом дерева T. *Вершинами* дерева называют его корень, корни его поддеревьев, корни поддеревьев его поддеревьев и т. д. Если в L и R содержится соответственно l и r вершин, то количество вершин в T равно $l + r + 1$. В пустом дереве нет вершин.

Так же рекурсивно определяется понятие изоморфизма бинарных деревьев. Два дерева называются *изоморфными*, если либо они оба пустые, либо являются изоморфными их левые поддеревья и правые поддеревья соответственно. Деревья удобно изображать так, как показано на рис. 2.

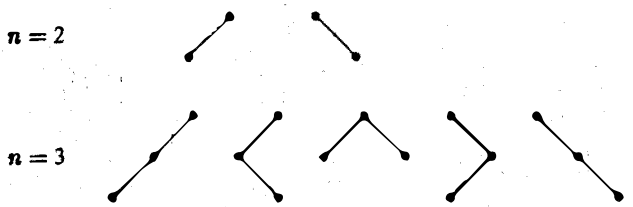


Рис. 2. Деревья с двумя и тремя вершинами

Число *существенно различных* (т. е. попарно неизоморфных) бинарных деревьев с n вершинами обозначим a_n. Непосредственный подсчет показывает, что $a_0 = 1$, $a_1 = 1$, $a_2 = 2$, $a_3 = 5$. Выведем рекуррентную формулу для a_n. Если в дереве, его левом и правом поддеревьях соответственно n, l и r вершин, то l принимает значения $0, 1, \ldots, n-1$; а r равно $n - l - 1$. При фиксированном l существует a_l различных (с точностью до изоморфизма) левых поддеревьев, a_{n-l-1} — правых поддеревьев, всего, в силу правила произведения, — $a_l a_{n-l-1}$ деревьев. Суммируя по всем возможным значениям l, получим искомую формулу:

$$\boxed{a_n = \sum_{l=0}^{n-1} a_l a_{n-l-1}.} \tag{1}$$

Пусть

$$A(x) = \sum_{k=0}^{\infty} a_k x^k$$

— производящая функция для последовательности (a_k). Используя (1), найдем $A(x)$. Для этого заметим, что

$$A^2(x) = (a_0 + a_1 x + a_2 x^2 + \ldots)(a_0 + a_1 x + a_2 x^2 + \ldots) =$$
$$= a_0^2 + (a_0 a_1 + a_1 a_0)x + (a_0 a_2 + a_1^2 + a_2 a_0)x^2 + (a_0 a_3 + a_1 a_2 + a_2 a_1 + a_3 a_0)x^3 + \ldots =$$
$$= a_1 + a_2 x + a_3 x^2 + a_4 x^3 + \ldots,$$

откуда получаем уравнение для $A(x)$: $xA^2(x) = A(x) - 1$. При $x \neq 0$

$$A(x) = \frac{1 \pm \sqrt{1 - 4x}}{2x}. \tag{2}$$

Применим биномиальное разложение:

$$(1-4x)^{1/2} = 1 - 2x + \frac{\frac{1}{2}\left(-\frac{1}{2}\right)}{2!}4^2x^2 - \frac{\frac{1}{2}\left(-\frac{1}{2}\right)\left(-\frac{3}{2}\right)}{3!}4^3x^3 + \\ + \frac{\frac{1}{2}\left(-\frac{1}{2}\right)\left(-\frac{3}{2}\right)\left(-\frac{5}{2}\right)}{4!}4^4x^4 - \ldots = 1 - \sum_{n=1}^{\infty}\frac{2^n(2n-3)!!}{n!}x^n.$$

Поскольку все члены последовательности (a_n) положительны, в формуле (2) нужно выбрать знак минус:

$$A(x) = \frac{1}{2}\sum_{n=1}^{\infty}\frac{2^n(2n-3)!!}{n!}x^{n-1} = [n = k+1] = \sum_{k=0}^{\infty}\frac{2^k(2k-1)!!}{(k+1)!}x^k.$$

Преобразуем коэффициент при x^k, умножив числитель и знаменатель дроби на $(2k)!! = 2\cdot 4\cdot\ldots\cdot 2k = 2^k\cdot k!$:

$$\frac{2^k(2k-1)!!}{(k+1)!} = \frac{2^k(2k-1)!!(2k)!!}{(k+1)!k!2^k} = \frac{(2k)!}{(k+1)!k!} = \frac{1}{k+1}C_{2k}^k.$$

Таким образом, число бинарных деревьев с k вершинами равно

$$\boxed{a_k = \frac{1}{k+1}C_{2k}^k.}$$

Числа a_k называют *числами Каталана*; они появляются при решении очень многих комбинаторных задач. Перечислим некоторые из них:

- Каким числом способов можно разделить выпуклый многоугольник на треугольники с помощью непересекающихся диагоналей?
- На окружности расставлено четное число точек. Сколькими способами их можно попарно соединить непересекающимися хордами?
- Задана некоторая бинарная операция $*$. Каким числом способов можно *правильно* расставить скобки в выражении $a_1 * a_2 * \ldots * a_n$? Термин *правильно* означает: внутри каждой пары скобок (открывающей и закрывающей) находится ровно два операнда, где *операнд* — это буква или выражение, заключенное в скобки.

§ 17. Решение линейных рекуррентных уравнений

Пусть последовательность $x_0, x_1, x_2, \ldots$ удовлетворяет следующему соотношению

$$\forall n \in \mathbb{N}_0 \quad x_{n+k} + a_1x_{n+k-1} + \ldots + a_kx_n = 0, \quad a_k \neq 0, \tag{1}$$

где $a_1, \ldots, a_k$ — некоторые числа.

При заданных значениях $x_0, x_1, \ldots, x_{k-1}$ формула (1) полностью определяет последовательность; каждый ее элемент, начиная с k-го, является линейной комбинацией предыдущих k элементов с коэффициентами a_i; поэтому формулу (1)

называют *линейным рекуррентным соотношением k-го порядка.* Если положить $a_0 = 1$, то (1) можно переписать в виде

$$\sum_{j=0}^{k} a_j x_{n+k-j} = 0,$$

или

$$\forall m \geqslant k \quad \sum_{j=0}^{k} a_j x_{m-j} = 0. \tag{2}$$

Поставим задачу — *перейти от рекуррентного задания последовательности к формуле, выражающей зависимость общего члена последовательности x_n от его номера n.*

Для решения этой задачи введем в рассмотрение:

— производящую функцию последовательности (x_n): $F(t) = \sum\limits_{n=0}^{\infty} x_n t^n$;

— *характеристический многочлен* $f(\lambda) = \lambda^k + a_1\lambda^{k-1} + \ldots + a_k$;

— многочлен $g(t) = 1 + a_1 t + \ldots + a_k t^k$.

Отметим следующую связь между многочленами: при $t \neq 0$ $g(t) = t^k f\left(\frac{1}{t}\right)$. Докажем, что $F(t)$ является дробно-рациональной функцией. Действительно,

$$F(t)g(t) = \sum_{i=0}^{\infty} x_i t^i \sum_{j=0}^{k} a_j t^j = \sum_{m=0}^{k-1} t^m \sum_{j=0}^{m} a_j x_{m-j} + \sum_{m=k}^{\infty} t^m \sum_{j=0}^{k} a_j x_{m-j} =$$

$$= [\text{в силу (2)}] = \sum_{m=0}^{k-1} t^m \sum_{j=0}^{m} a_j x_{m-j} = \sum_{m=0}^{k-1} c_m t^m,$$

где коэффициенты c_m определяются по коэффициентам a_i и первым k членам последовательности (x_n). Итак, $F(t)g(t) = Q(t)$, где $Q(t)$ — многочлен степени не выше $k-1$; поэтому $F(t) = \frac{Q(t)}{g(t)}$ — правильная рациональная дробь.

Дальнейший ход наших выкладок будет следующим: мы представим $F(t)$ в виде суммы *простейших дробей*, запишем разложения простейших дробей по степеням переменной t, после чего по виду полученного ряда для $F(t)$ будет ясен характер зависимости x_n от n.

Пусть характеристический многочлен $f(\lambda)$ имеет s различных (комплексных) корней: λ_1 кратности r_1, ..., λ_s кратности r_s:

$$f(\lambda) = \prod_{i=1}^{s} (\lambda - \lambda_i)^{r_i}, \quad \sum_{i=1}^{s} r_i = k.$$

Тогда

$$g(t) = t^k \cdot \prod_{i=1}^{s} \left(\frac{1}{t} - \lambda_i\right)^{r_i} = \prod_{i=1}^{s} (1 - \lambda_i t)^{r_i}.$$

Как известно из алгебры, разложение правильной рациональной дроби со знаменателем $g(t)$ на простейшие дроби имеет вид

$$F(t) = \frac{Q(t)}{g(t)} = \sum_{i=1}^{s} \sum_{j=1}^{r_i} \frac{A_{ij}}{(1-\lambda_i t)^j},$$

где A_{ij} — некоторые константы. Применив биномиальное разложение, получим

$$(1-\lambda t)^{-j} = 1 + \sum_{n=1}^{\infty} \frac{(-j)(-j-1)\dots(-j-n+1)}{n!}(-\lambda t)^n =$$

$$= 1 + \sum_{n=1}^{\infty} C_{j+n-1}^{n} \lambda^n t^n = 1 + \sum_{n=1}^{\infty} C_{j+n-1}^{j-1} \lambda^n t^n.$$

Таким образом,

$$F(t) = \sum_{i=1}^{s} \sum_{j=1}^{r_i} A_{ij} \left(1 + \sum_{n=1}^{\infty} C_{j+n-1}^{j-1} \lambda_i^n t^n\right) = x_0 + \sum_{n=1}^{\infty} \left(\sum_{i=1}^{s} \lambda_i^n \sum_{j=1}^{r_i} A_{ij} C_{j+n-1}^{j-1}\right) t^n,$$

или, поскольку C_{j+n-1}^{j-1} — многочлен от n степени $j-1$ (при фиксированном j),

$$F(t) = x_0 + \sum_{n=1}^{\infty} \left(\sum_{i=1}^{s} \lambda_i^n \cdot P_i(n)\right) t^n,$$

где $P_i(n)$ — некоторый многочлен степени не выше $r_i - 1$ $(i = 1, \dots, s)$.

Мы доказали, что общий член последовательности, удовлетворяющей линейному рекуррентному соотношению k-го порядка, имеет вид

$$\boxed{x_n = \sum_{i=1}^{s} \lambda_i^n P_i(n),}$$

где для $i = 1, \dots, n$ число λ_i — корень кратности r_i характеристического многочлена рекуррентного соотношения, $P_i(n)$ — многочлен степени, не превосходящей $r_i - 1$. Конкретный вид указанных многочленов определяется первыми k членами последовательности: $x_0, x_1, \dots, x_{k-1}$. В частности, если все корни характеристического многочлена — *простые* (т. е. кратности 1), то последовательность (x_n) представима в виде суммы геометрических прогрессий:

$$\boxed{\forall\, n \in \mathbb{N}_0 \quad x_n = \sum_{i=1}^{k} c_i \lambda_i^n,}$$

где c_i — некоторые константы.

Рассмотрим несколько примеров.

Пример 1. Последовательность *чисел Фибоначчи* задается соотношениями

$$x_0 = 0, \quad x_1 = 1, \quad \forall n \in \mathbb{N}_0 \quad x_{n+2} = x_{n+1} + x_n.$$

◀ Составим *характеристическое уравнение:*

$$\lambda^2 - \lambda - 1 = 0.$$

Его корни $\lambda_{1,2} = \frac{1 \pm \sqrt{5}}{2}$; формула общего члена:

$$x_n = c_1\left(\frac{1+\sqrt{5}}{2}\right)^n + c_2\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Коэффициенты c_1 и c_2 определим из «начальных условий»:

$$x_0 = c_1 + c_2 = 0,\ x_1 = c_1\frac{1+\sqrt{5}}{2} + c_2\frac{1-\sqrt{5}}{2} = 1.$$

Решив систему двух уравнений с двумя неизвестными, получим окончательный результат:

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

Пример 2. Найдем все последовательности, удовлетворяющие условию

$$\forall n \in \mathbb{N}_0 \quad x_{n+2} = 2x_{n+1} - x_n. \tag{3}$$

◀ Характеристическое уравнение $\lambda^2 - 2\lambda + 1 = 0$ имеет двукратный корень: $\lambda_{1,2} = 1$, поэтому общий член последовательности имеет вид:

$$x_n = (an + b) \cdot 1^n = an + b,$$

где константы a и b определяются первыми двумя членами последовательности. Таким образом, (x_n) — арифметическая прогрессия. Этот результат можно было предвидеть, заметив, что соотношение (3) является характеристическим для арифметической прогрессии: каждый член последовательности, начиная со второго, есть среднее арифметическое его соседних членов. ▶

Пример 3. Найдем последовательность (x_n), задаваемую соотношениями

$$x_0 = 1, \quad x_1 = 3, \quad x_2 = 6, \quad \forall n \in \mathbb{N}_0 \quad x_{n+3} = 4x_{n+2} - 5x_{n+1} + 2x_n.$$

◀ Разложим характеристический многочлен на множители:

$$\lambda^3 - 4\lambda^2 + 5\lambda - 2 = (\lambda - 1)^2(\lambda - 2).$$

Вид n-го члена последовательности: $x_n = (an + b) + c \cdot 2^n$. Константы a, b, c найдем из системы уравнений

$$x_0 = b + c = 1; \quad x_1 = a + b + 2c = 3; \quad x_2 = 2a + b + 4c = 6. \ ▶$$

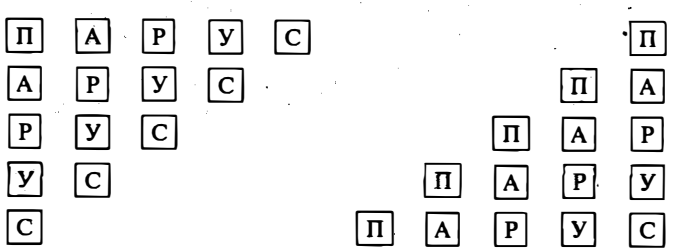
Ответ: $x_n = n + 2^n$.

Упражнения

Правило произведения

1. Из города А в город Б ведут 5 дорог, а из города Б в город В — 7 дорог. Сколько есть различных маршрутов из города А в В через Б?
2. В меню столовой 3 первых, 5 вторых и 3 третьих блюда. Сколькими способами можно выбрать обед из трех блюд (первое, второе и третье)?
3. Сколько есть двузначных чисел, не содержащих цифр 0, 2, 5?
4. Сколько есть двузначных чисел, не содержащих цифр 1, 3, 6?

5. Номер автомашины состоит из трех букв латинского алфавита (содержащего 26 букв) и трех цифр. Сколько можно составить различных номеров автомашин?
6. У рояля 88 клавиш. Сколькими способами можно извлечь последовательно 6 звуков?
7. Сколько натуральных делителей имеет число $2^3 \cdot 3^4 \cdot 5^6$?
8. Сколько натуральных делителей имеет число $2^3 \cdot 3^4 \cdot 4^5$?
9. Сколько есть пятизначных чисел,
   1) оканчивающихся двумя семерками?
   2) начинающихся с двух одинаковых цифр?
   3) в каждом из которых нет одинаковых цифр?
   4) в каждом из которых соседние цифры различны?
   5) делящихся на 4 и не содержащих цифр 0, 4, 6, 8?
   6) в записи которых есть одинаковые цифры?
   7) в записи которых есть хотя бы одна четная цифра?
10. Сколько есть перестановок цифр 0, 1, 2, ..., 9, в которых
    1) цифра 3 занимает третье место, а цифра 5 — пятое?
    2) цифра 1 следует непосредственно за цифрой 0?
    3) цифра 0 занимает одно из первых трех мест, а цифра 1 — одно из последних четырех мест?
    4) цифра 0 занимает одно из первых пяти мест, а цифра 1 — одно из первых трех мест?
    5) между цифрами 0 и 1 стоят ровно три цифры?
    6) цифра 0 расположена левее цифры 1?
    7) цифра 1 расположена между цифрами 0 и 2?
    8) хотя бы одна из первых трех цифр делится на 3?
11. Сколькими способами можно рассадить за десятью партами 10 мальчиков и 10 девочек так, чтобы за каждой партой сидели а) мальчик слева, а девочка справа? б) мальчик и девочка?
12. Сколькими способами можно прочитать слово ПАРУС, двигаясь вправо или вниз по каждой из следующих таблиц?



13. Сколькими способами можно расставить на шахматной доске 8 одинаковых ладей так, чтобы никакие две из них не били друг друга?
14. Сколькими способами можно расставить на шахматной доске 8 одинаковых ладей так, чтобы они били все поля?

Сочетания

15. Вычислить: C_7^2, C_{20}^0, C_{40}^1, C_{35}^{35}, C_8^4, C_{15}^{13}.
16. Найти число подмножеств X множества $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, обладающих следующими свойствами:

1) $|X| = 3$;
2) $|X| = 5$, $1 \in X$;
3) $|X| = 6$, $2 \notin X$;
4) $|X| = 7$, $\{0, 1\} \subset X$, $2 \notin X$;
5) множество X состоит из трех четных и двух нечетных чисел;
6) $|X| \leqslant 5$.

17. На окружности последовательно отмечены точки $A_1, \ldots, A_{12}$. Сколько существует

1) хорд с концами в отмеченных точках;
2) треугольников с вершинами в отмеченных точках;
3) выпуклых четырехугольников с вершинами в отмеченных точках;
4) треугольников с вершинами в отмеченных точках, не имеющих общих точек с прямой A_2A_8;
5) треугольников с вершинами в отмеченных точках, имеющих общие точки с прямой A_1A_5?

18. На окружности отмечено n точек. Точки соединяются всевозможными хордами; известно, что никакие три из них не пересекаются в одной точке внутри круга. Найти:

1) число точек пересечения хорд внутри круга;
2) количество частей, на которые хорды делят круг.

19. На прямой l отмечено 8 точек, а на параллельной ей прямой m ($l \neq m$) — 11 точек. Сколько существует

1) треугольников с вершинами в отмеченных точках;
2) выпуклых четырехугольников с вершинами в отмеченных точках?

20. *Две команды играют в волейбол до 4 побед.* Сколько существует разных вариантов изменения счета в игре по партиям?

21. Сколькими способами можно разложить 4 белых и 3 черных шара по 6 различным ящикам?

22. Решить предыдущую задачу при дополнительном условии: ни один ящик не должен быть пустым.

23. Сколькими способами можно разложить 20 одинаковых шаров по 5 различным ящикам так, чтобы

1) в каждом ящике оказалось не менее двух шаров;
2) в каждом ящике оказалось не более 5 шаров;
3) оказалось не более двух пустых ящиков?

24. Найти коэффициент при x^{100} в разложении многочлена

$$(1 + x + x^2 + \ldots + x^{100})^3.$$

25. Дан квадрат. Каждая его сторона разбита на n равных частей. Через точки деления проведены прямые, параллельные сторонам. Сколько существует

1) прямоугольников;
2) квадратов, ограниченных проведенными линиями?

26. В правлении банка 7 человек. Каково должно быть минимальное число замков от сейфа и как следует распределить ключи между членами правления (каждый член правления может получить ключи от нескольких замков), чтобы любое большинство сейф могло открыть, а любое меньшинство — не могло?

27. Каким числом способов можно прочитать слово «абракадабра», двигаясь вправо или вниз по таблице (с. 76)?

А	Б	Р	А	К	А
Б	Р	А	К	А	Д
Р	А	К	А	Д	А
А	К	А	Д	А	Б
К	А	Д	А	Б	Р
А	Д	А	Б	Р	А

28. На клетчатой бумаге нарисован прямоугольник $ABCD$, стороны которого лежат на линиях сетки, причем длина отрезка AD в k раз больше длины отрезка AB (k — натуральное число). Рассматриваются всевозможные пути, проходящие по линиям сетки и кратчайшим образом ведущие из A в C. Доказать, что среди этих путей в k раз больше тех, у которых первое звено лежит на AD, чем тех, у которых первое звено лежит на AB.

29. Изучите поведение последовательности (a_k), где $a_k = C_n^k$ (при фиксированном n), с точки зрения возрастания-убывания.

30. Имеется карточная колода из 52 карт. Каким числом способов можно раздать по 13 карт четырем игрокам?

Полиномиальная формула

31. Найти коэффициент при x^k в разложении многочленов:

1) $(x+2)^{10}$, $k=3$; 2) $(1-2x)^7$, $k=4$; 3) $\left(\sqrt{x}-\dfrac{2}{x}\right)^8$, $k=-5$;

4) $\left(3\sqrt[3]{x^2}-x\sqrt{x}\right)^9$, $k=11$; 5) $(x^2-x+2)^8$, $k=7$; 6) $\left(\sqrt{x}+\sqrt[3]{x}+\sqrt[4]{x}\right)^6$, $k=2$.

Комбинаторные тождества

32. С помощью формулы бинома Ньютона

$$(1+x)^n = \sum_{k=0}^{n} C_n^k x^k$$

доказать следующие тождества:

1) $\sum\limits_{k=0}^{n} 9^k C_n^k = 10^n$; 2) $\sum\limits_{k=0}^{n} (-1)^{n-k} 2^k C_n^k = 1$; 3) $\sum\limits_{k=0}^{n} k C_n^k = n2^{n-1}$;

4) $\sum\limits_{k=0}^{n} (-1)^{k-1} k C_n^k = 0$; 5) $\sum\limits_{k=0}^{n} \dfrac{C_n^k}{k+1} = \dfrac{2^{n+1}-1}{n+1}$; 6) $\sum\limits_{k=0}^{n} \dfrac{(-1)^k C_n^k}{k+1} = \dfrac{1}{n+1}$;

7) $\sum\limits_{k=0}^{2n} (-1)^k (C_{2n}^k)^2 = (-1)^n C_{2n}^n$; 8) $\sum\limits_{k=0}^{2n-1} (-1)^k (C_{2n-1}^k)^2 = 0$.

33. С помощью комбинаторных рассуждений доказать:

1) $\sum\limits_{k=0}^{n} k C_n^k = n2^{n-1}$; 2) $\sum\limits_{k=m}^{n-r+m} C_k^m C_{n-k}^{r-m} = C_{n+1}^{r+1}$.

Формула включения-исключения

34. На кафедре лингвистики работают 13 человек, причем каждый из них знает хотя бы один иностранный язык. Десять человек знают английский язык, семеро — немецкий, шестеро — французский. Пятеро знают английский и немецкий, четверо — английский и французский, трое — немецкий и французский. Сколько человек знают 1) все три языка; 2) ровно два языка; 3) только английский язык?

35. 1) Показать, что количество натуральных чисел, делящихся на n и не превосходящих положительного числа x, равно $[x/n]$.

2) Сколько есть чисел, не превосходящих 10 000 и не делящихся ни на 3, ни на 5, ни на 7?

3) Сколько есть четырехзначных чисел, не делящихся ни на 3, ни на 5, ни на 7?

4) Сколько есть чисел, не превосходящих 10 000 и не делящихся ни на одно из чисел 6, 10 и 15?

5) Показать, что если $n = 30m$, то количество натуральных чисел, не превосходящих n и не делящихся ни на одно из чисел 6, 10 и 15, равно $22m$.

36. Пусть $n > 5$. Показать, что простых чисел в множестве

$$\{n+1, n+2, \ldots, n+30\}$$

не больше восьми.

37. На каждой стороне треугольника ABC отмечено по n точек, разбивающих ее на $n+1$ равных частей. Рассмотрим всевозможные треугольники с вершинами в отмеченных точках (по одной на каждой стороне). Сколько среди этих треугольников таких, у которых ни одна из сторон не параллельна стороне треугольника ABC?

38. Сколько существует 6-значных номеров (первые цифры могут быть и нулями) с суммой цифр 27?

39. В кошельке лежит по 20 монет достоинством в 1, 2 и 5 рублей. Сколькими способами можно из этих 60 монет выбрать k монет ($k \leqslant 60$)?

Задача о беспорядках и встречах

40. С помощью рекуррентных соотношений найти число беспорядков D_n для $n = 1, \ldots, 8$.

41. Доказать, что $D_n = \left[\dfrac{n!}{e} + \dfrac{1}{2}\right]$.

42. Сколькими способами можно расставить на шахматной доске 8 одинаковых ладей так, чтобы никакие две из них не били друг друга и чтобы ни одна ладья не стояла на главной диагонали?

43. Сколькими способами можно раскрасить клетки шахматной доски 8×8 в 8 цветов так, чтобы клетки, имеющие общую сторону, были бы окрашены в разные цвета и чтобы в каждом горизонтальном ряду встречались все 8 цветов?

44. Две колоды карт, содержащие по 52 карты, тщательно тасуются, после чего сравниваются карта за картой. Какова вероятность того, что не будет ни одной пары совпадающих карт?

45. Для числа перестановок n элементов с k встречами $D_{n,k}$ доказать тождества:

1) $\displaystyle\sum_{k=0}^{n} D_{n,k} = n!$; 2) $D_{n,k} = \dfrac{n}{k} D_{n-1,k-1}$ $(k = 1, \ldots, n)$; 3) $\displaystyle\sum_{k=1}^{n} k D_{n,k} = n!$;

4) $\displaystyle\sum_{k=0}^{n} C_n^k D_k = n!$; 5) $\displaystyle\sum_{k=m}^{n} C_k^m D_{n,k} = \frac{n!}{m!}$; 6) $\displaystyle\sum_{k=0}^{n} (k-1)^2 D_{n,k} = n!$ $(n \geqslant 2)$.

46. Случайным образом выбирается перестановка чисел $1, 2 \ldots, n$. Пусть ξ — количество элементов, остающихся на своих местах. Найти математическое ожидание и дисперсию случайной величины ξ.

47. Секретарше нужно отправить n различных писем по n различным адресам. Она подписывает конверты и случайным образом вкладывает письма в конверты. Сколько в среднем писем дойдет до своего адресата?

Производящие функции

Найти производящие функции следующих последовательностей:

48. $a_n = \begin{cases} 1, & n = 0, 1, \ldots, N, \\ 0, & n > N. \end{cases}$

49. $a_n = \begin{cases} n+1, & n = 0, 1, \ldots, N, \\ 0, & n > N. \end{cases}$

50. $a_n = \begin{cases} (n+1)(n+2), & n = 0, 1, \ldots, N-1, \\ 0, & n \geqslant N. \end{cases}$

51. $a_n = \alpha^n$, $n = 0, 1, 2, \ldots$.

52. $a_n = n^2$, $n = 0, 1, 2, \ldots$.

Пусть (a_n), (b_n) — последовательности, $A(x)$ и $B(x)$ — соответствующие производящие функции. Выразить $A(x)$ через $B(x)$ при следующих соотношениях между последовательностями:

53. $a_0 = 0$, $a_n = b_{n-1}$, $n = 1, 2, \ldots$.

54. $a_n = b_{n+1}$.

55. $a_n = b_{n+k}$, $k \in \mathbb{N}$.

56. $a_n = \alpha^n b_n$.

57. $a_0 = 0$, $a_n = b_n - b_{n-1}$, $n = 1, 2, \ldots$.

58. $a_n = b_{n+1} - b_n$.

59. $a_n = \sum\limits_{i=0}^{n} b_i$.

60. $a_n = \sum\limits_{k=n+1}^{\infty} b_k$.

61. $a_n = nb_n$.

62. $a_n = \sum\limits_{k=0}^{n} b_k c_{n-k}$, $C(x) = \sum\limits_{n=0}^{\infty} c_n x^n$.

63. Пусть $a_n = \sum\limits_{k=n}^{\infty} C_k^n b_k$. Доказать, что $b_n = \sum\limits_{k=n}^{\infty} (-1)^{n-k} C_k^n a_k$.

Рекуррентные соотношения

64. Последовательность (a_n) удовлетворяет соотношению

$$a_{n+2} = \alpha a_{n+1} + \beta a_n;$$

уравнение $x^2 - \alpha x - \beta = 0$ имеет два различных ненулевых корня x_1 и x_2. Доказать, что имеет место тождество

$$a_n = c_1 x_1^n + c_2 x_2^n$$

для некоторых c_1 и c_2, однозначно определяемых a_1 и a_2.

65. Найти формулу общего члена последовательности:

1) $a_{n+2} = 4a_{n+1} - 3a_n$; $a_1 = 10$, $a_2 = 16$;

2) $a_{n+2} = 2\cos\alpha a_{n+1} - a_n$; $a_1 = \cos\alpha$, $a_2 = \cos 2\alpha$.

66. Найти количество n-значных чисел, состоящих из цифр 1, 2, 3, в которых первая и последняя, а также любые две соседние цифры различны.

67. Сколько существует раскрасок вершин n-угольника, если соседние вершины должны быть разного цвета, а всего имеется k цветов?

68. Пусть n-й член последовательности задается формулой

$$a_n = c_1x_1^n + c_2x_2^n, \quad \text{где} \quad x_1 \neq x_2.$$

Доказать, что для последовательности имеет место рекуррентное соотношение

$$a_{n+2} = \alpha a_{n+1} + \beta a_n, \quad \text{где} \quad \alpha = x_1 + x_2, \quad \beta = -x_1x_2.$$

69. Найти $ax^4 + by^4$, если

1) $\begin{cases} a + b = 1, \\ ax + by = 1, \\ ax^2 + by^2 = 2, \\ ax^3 + by^3 = 3; \end{cases}$ 2) $\begin{cases} a + b = 1, \\ ax + by = 2, \\ ax^2 + by^2 = 5, \\ ax^3 + by^3 = 14; \end{cases}$ 3) $\begin{cases} a + b = 23, \\ ax + by = 79, \\ ax^2 + by^2 = 217, \\ ax^3 + by^3 = 691. \end{cases}$

70. Найти число двоичных последовательностей длины 11, не содержащих единиц ни в каких трех соседних позициях.

71. Найти общие решения рекуррентных соотношений:

1) $a_{n+2} + 2a_{n+1} + a_n = 0$;

2) $a_{n+3} + 10a_{n+2} + 32a_{n+1} + 32a_n = 0$;

3) $a_{n+3} + 3a_{n+2} + 3a_{n+1} + a_n = 0$.

72. Найти a_n по рекуррентным соотношениям и начальным условиям:

1) $a_{n+3} - 3a_{n+2} + a_{n+1} - 3a_n = 0$, $a_1 = 3$, $a_2 = 7$, $a_3 = 27$;

2) $a_{n+3} - 3a_{n+1} + 2a_n = 0$, $a_1 = a$, $a_2 = b$, $a_3 = c$.

Ответы

7. 140. **8.** 70. **11.** а) $10!^2$; б) $10!^2 \cdot 2^{10}$. **13.** 8!. **14.** $2 \cdot 8^8 - 8!$. **16.** б) $(2^{10} + C_{10}^5)/2$.

18. 1) C_n^4. Каждая точка пересечения хорд однозначно задается (неупорядоченной) четверкой точек — концов этих хорд.

2) $1 + C_n^2 + C_n^4$. Будем последовательно проводить хорды. Пусть k_i — число точек пересечения i-й хорды с ранее проведенными. Этими точками i-я хорда делится на $k_i + 1$ отрезков, каждый из которых, в свою очередь, делит одну «старую» часть разбиения круга на две «новые». Изначально имелась одна часть. После проведения всех N хорд количество частей равно

$$1 + \sum_{i=1}^{N}(k_i + 1) = 1 + N + \sum_{i=1}^{N} k_i.$$

Осталось заметить, что $N = C_n^2$, а общее количество точек пересечения хорд

$$\sum_{i=1}^{N} k_i = C_n^4$$

(согласно первому пункту данной задачи).

Интересен ответ к задаче при $n = 1, 2, \ldots, 6$. Он таков: 1, 2, 4, 8, 16, 31. Физик из известного анекдота на основании первых пяти результатов заявил бы, что общий ответ — 2^{n-1}, а число 31 возникло в результате погрешности эксперимента.

20. $2C_7^4 = 70$. **23.** 1) $\overline{C_5^{10}}$; 2) $\overline{C_5^5} = 126$; 3) $\overline{C_5^{20}} - C_5^3\overline{C_2^{18}} - 5 = 10\,431$.

25. 1) $(C_{n+1}^2)^2$; 2) $n(n+1)(2n+1)/6$. **27.** C_{10}^5. **29.** Составьте отношение a_{k+1}/a_k. **30.** $52!/(13!)^4$. **33.** Подсчитайте двумя способами сумму мощностей всех подмножеств n-элементного множества. **37.** $(n-1)^3$ при нечетном n; $(n-1)^3 + 1$ при четном n.

38. $\overline{C_6^{27}} - 6\cdot\overline{C_6^{17}} + C_6^2\cdot\overline{C_6^7}$. **Решение.** Пусть U — множество последовательностей $(a_1, a_2, \ldots, a_6)$, составленных из шести неотрицательных целых чисел с суммой 27; а для каждого i множество $A_i \subset U$ состоит из таких последовательностей, в которых $a_i \geqslant 10$. Для решения задачи нужно вычислить $\left|\bigcap\limits_{i=1}^{6} \overline{A_i}\right|$. Заметим, что $|U| = \overline{C_6^{27}}$, $|A_i| = \overline{C_6^{17}}$, $|A_i \cap A_j| = \overline{C_6^7}$ $(i \neq j)$, а пересечение трех и большего числа множеств A_i пусто.

41. Используйте оценку остаточного члена ряда из признака Лейбница. **42.** 14 833.

45. 6) $(k-1)^2 = 2!C_k^2 - 1!C_k^1 + 1$. **46.** $M\xi = D\xi = 1$. **63.** $A(x) = B(x+1)$. **66.** $2\cdot(-1)^n + 2^n$.

70. 927. **Указание.** Обозначим через a_n число двоичных последовательностей длины n, удовлетворяющих условию задачи. Найдите начальные условия и рекуррентное соотношение для последовательности (a_n).

Глава LXIX

ТЕОРИЯ ПОЙА

При решении ряда перечислительных задач комбинаторные объекты могут естественным образом отождествляться.

Приведем конкретный пример. Некогда пассажиры общественного транспорта, заходя в автобус, троллейбус или трамвай, не покупали билет у кондуктора, а пробивали заранее купленный абонемент компостером, установленным в салоне транспортного средства. Контролеры проверяли, соответствует ли расположение дырочек на пробитом абонементе данному компостеру. Ясно, что с точки зрения как контролера, так и пассажира, компостеры, дающие картинки, которые переходят одна в другую (например, в результате выполнения осевой симметрии), различить нельзя.

Впечатляющим примером перечисления объектов с точностью до симметрий была работа Артура Кэли, опубликовавшего в 1875 г. в Докладах немецкого химического общества статью, посвященную перечислению изомеров углеводородов.

Обобщение идей Кэли привело к *теории Пойа*, названной так в честь американского математика венгерского происхождения Джорджа Пойа[1]. Эта теория создавалась в 30-х годах XX столетия, но развивается и применяется и поныне, особенно в части перечисления графов различных видов.

В теории Пойа подсчет числа элементов некоторого множества осуществляется с точностью до отношения эквивалентности, заданного на данном множестве при помощи указания некоторой группы подстановок, действующих на этом множестве. В результате применения теории Пойа для числа классов эквивалентности различных видов строится *производящая функция*. Заметим, что производящие функции к решению различных комбинаторных и вероятностных задач применяли еще Г. Лейбниц, Я. Бернулли, А. Муавр, Л. Эйлер и П. Лаплас.

Теория Пойа является хорошим примером демонстрации возможностей алгебраического аппарата при решении комбинаторных задач.

---

[1] На русском языке изданы такие широко известные в кругу любителей математики книги Д. Пойа, как «Математика и правдоподобные рассуждения», «Как решать задачу». Он также один из авторов знаменитого двухтомника «Задачи и теоремы из анализа», где, правда, фигурирует как Георг Полиа (это немецкий вариант звучания его имени и фамилии).

§ 1. Цикловой индекс группы подстановок

Пусть S — n-элементное множество. *Подстановкой* на множестве S называется взаимно однозначное отображение S на себя.

Образ элемента $s \in S$ при действии на него подстановкой $\pi : S \to S$ будем обозначать πs. *Тождественная* подстановка ε переводит каждый элемент S в себя:

$$\forall s \in S \quad \varepsilon s = s.$$

Произведением $\pi_1\pi_2$ подстановок π_1 и π_2 на множестве S назовем их композицию — подстановку, определяемую последовательным выполнением данных подстановок:

$$\forall s \in S \quad (\pi_1\pi_2)s = \pi_1(\pi_2 s).$$

Операция умножения подстановок обладает свойством ассоциативности:

$$\forall \pi_1, \pi_2, \pi_3 \quad (\pi_1\pi_2)\pi_3 = \pi_1(\pi_2\pi_3).$$

Действительно,

$$(\pi_1\pi_2)(\pi_3 s) = \pi_1(\pi_2(\pi_3 s)); \quad \pi_1(\pi_2\pi_3) = \pi_1(\pi_2(\pi_3 s)),$$

и, значит,

$$\forall s \quad ((\pi_1\pi_2)\pi_3)s = (\pi_1(\pi_2\pi_3))s.$$

Естественным образом теперь определяется (натуральная) степень подстановки. После установления ассоциативности операции умножения подстановок, степень (π^n) определяется стандартно, как n-кратное произведение $\pi \cdot \pi \cdot \ldots \cdot \pi = \pi^n$.

Если некоторое множество подстановок на S

- замкнуто относительно операции умножения;
- содержит тождественную подстановку;
- вместе с каждой подстановкой содержит ей обратную,

то оно образует группу, в которой умножение подстановок является (групповой) бинарной операцией, а в роли нейтрального элемента выступает тождественная подстановка ε. Самой «бедной» (по числу ее элементов) является группа, содержащая лишь ε. Самая «богатая» группа содержит все подстановки на множестве S, их число совпадает с числом перестановок n элементов и равно $n!$. Такую группу называют *симметрической* и обозначают S_n.

Зафиксируем некоторый элемент $s \in S$ и рассмотрим последовательность

$$s, \pi s, \pi^2 s, \pi^3 s, \ldots .$$

Данная последовательность не может содержать бесконечное число различных элементов ввиду конечности множества S. *Первый* элемент, который повторно встретится в последовательности, есть s (если бы это было не так, и подобным свойством обладал элемент $r = \pi^j s = \pi^m s$, то элемент r при подстановке π был бы образом двух *различных* элементов: $\pi^{j-1}s$ и $\pi^{m-1}s$, что противоречит взаимной однозначности отображения π). Наименьшее (натуральное) число k такое, что $\pi^k s = s$, называют *порядком* элемента s. Последовательность $s, \pi s, \pi^2 s, \ldots, \pi^{k-1}s$ называют *орбитой* (или *циклом*) элемента s.

Элементы орбиты циклически переставляются подстановкой π (рис. 1). Возьмем какой-нибудь элемент, не входящий в орбиту s (если, конечно, такой элемент

существует, что будет в случае, когда орбита s не исчерпывает всего множества S); он порождает свою орбиту, не имеющую общих элементов с орбитой s. Если при этом остались элементы множества S, не вошедшие в построенные орбиты, то можно указать еще одну орбиту и т. д. В результате множество S разбивается на непересекающиеся орбиты (каждая подстановка задает, вообще говоря, свое разбиение S).

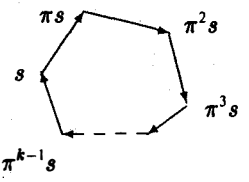


Рис. 1

Длиной орбиты называют число ее элементов. Если подстановка разбивает множество S на k_1 орбит длины 1, k_2 орбит длины $2, \ldots, k_n$ орбит длины n, то говорят, что подстановка имеет *тип* $(k_1, k_2, \ldots, k_n)$. Сумма длин всех орбит равна числу элементов множества S:

$$\sum_{i=1}^{n} i k_i = n.$$

Цикловым индексом подстановки называют одночлен

$$x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n},$$

где $(k_1, k_2, \ldots, k_n)$ — тип подстановки.

Цикловым индексом группы подстановок G называют среднее арифметическое цикловых индексов ее элементов:

$$\boxed{P_G(x_1, x_2, \ldots x_n) = \frac{1}{|G|} \sum_{g \in G} x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}.}$$

Рассмотрим несколько примеров.

Пример 1. Тождественная подстановка ε порождает n орбит длины 1, поэтому цикловой индекс группы, состоящей только из тождественной подстановки, равен:

$$\boxed{P_{\{\varepsilon\}}(x_1, \ldots, x_n) = x_1^n.}$$

Пример 2. Для вычисления циклового индекса симметрической группы S_n найдем число подстановок, имеющих тип $(k_1, k_2, \ldots, k_n)$.

◄ Рассмотрим запись разбиения n-элементного множества на орбиты: сначала k_1 пар скобок для записи одноэлементных орбит, затем k_2 пар скобок для записи 2-элементных орбит и т. д. На имеющихся внутри всех скобок n позициях n элементов можно расставить $n!$ способами; при этом получающимся записям будут соответствовать подстановки указанного типа. Однако одной и той же подстановке будет соответствовать, вообще говоря, несколько записей. Подсчитаем, сколько.

Каждая орбита длины i в пределах данных скобок может быть записана i способами (на первое место можно поставить любой элемент орбиты, заполнение остальных мест после этого определяется однозначно). Например, 3-элементную орбиту $a \to b \to c \to a$ можно записать тремя способами:

$$(a, b, c), \ (b, c, a), \ (c, a, b).$$

Скобки, соответствующие орбитам длины i, можно переставить $k_i!$ способами.

Значит, семейство орбит длины i может быть представлено $i^{k_i} \cdot k_i!$ способами. Поэтому общее число способов записи подстановки типа $(k_1, \ldots, k_n)$ равно

$$\prod_{i=1}^{n} i^{k_i} k_i!,$$

а количество подстановок указанного типа —

$$\frac{n!}{\prod_{i=1}^{n} i^{k_i} k_i!}.$$

Учитывая, что $|S_n| = n!$, получим выражение для циклового индекса симметрической группы

$$\boxed{P_{S_n}(x_1, x_2, \ldots, x_n) = \sum \frac{x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}}{1^{k_1} k_1! 2^{k_2} k_2! \ldots n^{k_n} k_n!},}$$

где суммирование ведется по всем решениям уравнения

$$k_1 + 2k_2 + \ldots + nk_n = n$$

в неотрицательных целых числах. ►

Пример 3. Каждое самосовмещение многоугольника или многогранника задает некоторую подстановку на множестве его вершин (а также ребер или граней). Нетрудно видеть, что если некоторые самосовмещения образуют группу, то тем же свойством обладают и соответствующие им подстановки на множестве вершин (ребер или граней).

Найдем цикловой индекс группы подстановок вершин тетраэдра, порожденных его вращениями.

◄ Вращение тетраэдра вокруг его высоты на 120° в любом направлении задает подстановку на множестве вершин, имеющую тип $(1, 0, 1, 0)$ (вершина, через которую проходит высота, при вращении остается на месте, образуя орбиту из одного элемента, три другие вершины циклически переставляются, образуя орбиту длины 3). Всего имеем 8 таких вращений тетраэдра и соответственно 8 подстановок, имеющих цикловой индекс $x_1^1 x_3^1$.

Вращение тетраэдра на 180° вокруг прямой, соединяющей середины противоположных ребер, порождает подстановку типа $(0, 2, 0, 0)$ (концы каждого из указанных ребер меняются при повороте местами, образуя 2-элементную орбиту). Поэтому в группе подстановок имеется три подстановки с цикловым индексом x_2^2.

Учтя, наконец, тождественную подстановку, имеющую цикловой индекс x_1^4, запишем цикловой индекс рассматриваемой группы:

$$P_G(x_1, x_2, x_3, x_4) = \frac{1}{12}(8x_1x_3 + 3x_2^2 + x_1^4). \quad ►$$

§ 2. Лемма Бернсайда

Пусть S — конечное множество, $\langle G, \cdot \rangle$ — конечная группа, каждому элементу g которой поставлена в соответствие некоторая подстановка π_g, действующая на множестве S. Пусть данное соответствие является гомоморфизмом:

$$\forall\, g_1, g_2 \in G \quad \pi_{g_1 g_2} = \pi_{g_1} \cdot \pi_{g_2}.$$

Отметим, что при этом нейтральному элементу группы $e \in G$ будет соответствовать тождественная подстановка ε, а элементу, обратному к произвольному элементу g, — подстановка, обратная к π_g.

Действительно, с одной стороны, $\forall\, g \in G \;\; \pi_{eg} = \pi_g$. С другой стороны, в силу гомоморфизма, $\pi_{eg} = \pi_e \cdot \pi_g$. Значит,

$$\forall\, g \in G \;\; \pi_e \cdot \pi_g = \pi_g,$$

что говорит о том, что π_e — тождественная подстановка: $\pi_e = \varepsilon$. Второе утверждение доказывается с помощью следующей цепочки выкладок:

$$\varepsilon = \pi_e = \pi_{g \cdot g^{-1}} = \pi_g \cdot \pi_{g^{-1}},$$

откуда получаем $\pi_{g^{-1}} = (\pi_g)^{-1}$.

Назовем элементы s_1 и s_2 множества S *эквивалентными* $(s_1 \sim s_2)$, если найдется такой элемент $g \in G$, что отвечающая ему подстановка π_g переводит s_1 в s_2: $\pi_g s_1 = s_2$. Докажем, что введенное отношение на множестве S, оправдывая свое название, действительно является *отношением эквивалентности.*

Рефлексивность. $\forall\, s \in S \;\; s \sim s$. Действительно, так как $\pi_e = \varepsilon$, то для любого $s \in S \;\; \pi_e s = s$.

Симметричность. Если $s_1 \sim s_2$, то $s_2 \sim s_1$. Для доказательства этого утверждения заметим, что если для некоторого $g \in G \;\; \pi_g s_1 = s_2$, то $s_1 = (\pi_g)^{-1} s_2 = \pi_{g^{-1}} s_2$, и, значит, $s_2 \sim s_1$.

Транзитивность. Если $s_1 \sim s_2$ и $s_2 \sim s_3$, то $s_1 \sim s_3$. В самом деле, если $\pi_{g_1} s_1 = s_2$ и $\pi_{g_2} s_2 = s_3$, то $\pi_{g_2 g_1} s_1 = \pi_{g_2} \pi_{g_1} s_1 = \pi_{g_2} s_2 = s_3$, т. е. $s_1 \sim s_3$. С помощью введенного отношения множество S разбивается на классы эквивалентности, будем называть их *транзитивными множествами.*

Пример 1. Пусть S — множество всех раскрасок вершин тетраэдра в k цветов:

$$S = \{(a_1, a_2, a_3, a_4) \mid a_i \in C\}, \quad |C| = k$$

(a_i — цвет i-й вершины, C — множество цветов); G — группа вращений тетраэдра. При вращении тетраэдра его вершины меняются местами, в результате чего одна раскраска переходит в другую, т. е. каждому вращению тетраэдра соответствует некоторая подстановка на множестве раскрасок. Транзитивное множество в данном случае составляют такие раскраски, которые могут быть получены одна из другой в результате некоторого вращения тетраэдра. Раскраски, входящие в разные транзитивные множества, — *существенно различны,* поскольку не переходят друг в друга одним лишь вращением тетраэдра.

Число транзитивных множеств, на которые разбивается множество S отношением, определяемым группой G, обозначим $T_G(S)$.

Элемент $s \in S$ называется *инвариантным относительно подстановки* π_g, если подстановка π_g «оставляет s на месте» (т. е. переводит s в s): $\pi_g s = s$. Пусть $I(g)$ — число элементов множества S, инвариантных относительно подстановки π_g:

$$I(g) = \big|\{s \in S \mid \pi_g s = s\}\big|.$$

Теорема 1 (лемма Бернсайда; 1911 г.).

$$T_G(S) = \frac{1}{|G|} \sum_{g \in G} I(g).$$

◀ *Стабилизатором* элемента s назовем множество всех элементов $g \in G$ таких, что s является инвариантным относительно соответствующих им подстановок:

$$G_s = \{g \in G \mid \pi_g s = s\}.$$

Докажем, что для любого элемента s алгебраическая структура $\langle G_s, \cdot \rangle$ является группой. Проверим выполнение всех аксиом группы.

1) *Замкнутость.* Пусть $g_1, g_2 \in G_s$. Тогда

$$\pi_{g_1} s = s, \quad \pi_{g_2} s = s \quad \text{и} \quad \pi_{g_1 g_2} s = \pi_{g_1} \pi_{g_2} s = \pi_{g_1} s = s,$$

т. е. $g_1 g_2 \in G_s$.

2) *Ассоциативность* имеет место «по наследству», поскольку это свойство выполняется для элементов G, чьим подмножеством является G_s.

3) *Существование нейтрального элемента.* Как было отмечено, для нейтрального элемента e группы G подстановка π_e является тождественной: $\pi_e = \varepsilon$, т. е. $\forall s \in S \ \ \pi_e s = \varepsilon s = s$; значит, $e \in G_s$ для любого s.

4) *Существование обратного элемента.* Пусть $g \in G_s$. Докажем, что $g^{-1} \in G_s$. Действительно, так как $s = \pi_g s$, $\pi_{g^{-1}} s = \pi_{g^{-1}} \pi_g s = \pi_{g^{-1} g} s = \pi_e s = \varepsilon s = s$.

Подсчитаем двумя способами

$$p = \left|\{(g, s) \mid g \in G, \ s \in S, \ \pi_g s = s\}\right|$$

— число пар (g, s) таких, что элемент $s \in S$ инвариантен относительно подстановки π_g. С одной стороны,

$$p = \sum_{g \in G} \left|\{s \in S \mid \pi_g s = s\}\right| = \sum_{g \in G} I(g).$$

С другой стороны,

$$p = \sum_{s \in S} \left|\{g \in G \mid \pi_g s = s\}\right| = \sum_{s \in S} |G_s|.$$

Для доказательства теоремы теперь достаточно найти сумму мощностей стабилизаторов всех элементов множества S.

Пусть

$$O(s) = \{s' \in S \mid s' \sim s\}$$

— транзитивное множество, содержащее элемент s. Ключевым моментом при доказательстве леммы Бернсайда является следующее соотношение между мощностями стабилизатора элемента и транзитивного множества:

$$\forall s \in S \quad |G_s| \cdot |O(s)| = |G|.$$

Докажем его. Пусть s' — произвольный элемент из $O(s)$, тогда s' эквивалентен s, т. е. для некоторого элемента $h \in G \ \ \pi_h s' = s$. Так как, в свою очередь, $s \sim s'$, существуют элементы $g \in G$, для которых $\pi_g s = s'$. Подсчитаем, сколько их.

Поскольку $s = \pi_h s' = \pi_h \pi_g s = \pi_{hg} s$, $hg \in G_s$. Покажем, что справедливо и обратное. Если $hg \in G_s$, то $\pi_h(\pi_g s) = s$. Отсюда, в силу того, что $\pi_h s' = s$ и π_h — подстановка (взаимно однозначное отображение S на себя), следует: $\pi_g s = s'$, что и требовалось.

Итак, $\pi_g s = s'$ тогда и только тогда, когда $hg \in G_s$. Пусть стабилизатор G_s содержит m элементов: $G_s = \{g_1, g_2, \ldots, g_m\}$. Соотношение $hg = g_i$ равносильно $g = h^{-1}g_i$ и задает взаимно однозначное соответствие между множеством $\{g \in G \mid \pi_g s = s'\}$ и стабилизатором G_s. Таким образом, искомое число равно m — мощности стабилизатора.

Мы выяснили, что ровно $m = |G_s|$ элементам группы G отвечают подстановки, переводящие s в s' — фиксированный элемент транзитивного множества $O(s)$. Так как *каждому* элементу G соответствует подстановка, переводящая s в некоторый элемент $O(s)$, отсюда следует:

$$|G| = |O(s)| \cdot |G_s|.$$

Таким образом,

$$|G_s| = \frac{|G|}{|O(s)|}.$$

Значит, мощности стабилизаторов элементов, составляющих транзитивное множество, равны между собой. Легко найти их сумму:

$$\sum_{s' \in O(s)} |G_{s'}| = \sum_{s' \in O(s)} \frac{|G|}{|O(s)|} = |G|.$$

Общая сумма мощностей стабилизаторов всех элементов S равна произведению $|G|$ на число транзитивных множеств $T_G(S)$.

Заключительный аккорд:

$$p = \sum_{g \in G} I(g) = \sum_{s \in S} |G_s| = T_G(S) \cdot |G|,$$

откуда и вытекает утверждение теоремы. ▶

Пример 2. Подсчитаем число существенно различных раскрасок вершин тетраэдра в k цветов. Группа вращений тетраэдра G состоит из 12 элементов (см. § 6 гл. LXVII). $I(g)$ в данной задаче означает число раскрасок, которые не меняются при вращении g.

Для нейтрального элемента группы имеем:

$$I(e) = |S| = k^4.$$

При повороте тетраэдра на 120° вокруг его высоты раскраска не изменится в том и только в том случае, когда все вершины основания покрашены в один цвет (вершина, через которую проходит высота, может быть любого цвета). Каждая такая раскраска (при фиксированной высоте) задается «цветом основания» и цветом вершины; поэтому количество таких раскрасок равно k^2. При повороте тетраэдра на 180° вокруг прямой, проходящей через середины скрещивающихся ребер, раскраска не изменится тогда и только тогда, когда концы каждого из этих ребер покрашены в один цвет. И в этом случае

$$I(g) = k^2.$$

Таким образом, применив лемму Бернсайда, получим

Ответ: число существенно различных раскрасок вершин тетраэдра в k цветов равно $\frac{1}{12}(k^4 + 11k^2)$.

Полезным упражнением на развитие комбинаторного мышления будет решение данной задачи «в лоб» (непосредственным подсчетом).

§ 3. Функции и классы эквивалентности

Пусть $R^D = \{f : D \to R\}$ — множество всевозможных функций с областью определения D и принимающих значения из множества R, где R и D — некоторые конечные множества. Каждую такую функцию можно отождествить с размещением с повторениями из $|R|$ элементов по $|D|$; поэтому $|R^D| = |R|^{|D|}$ (этим фактом и объясняется введенное обозначение).

Пусть G — группа подстановок, действующих на множестве D. Назовем функции f_1 и f_2 из R^D *эквивалентными* ($f_1 \sim f_2$), если для некоторой подстановки $g \in G$ $f_1(g) = f_2$, т. е.

$$\forall\, d \in D \quad f_1(g(d)) = f_2(d).$$

Докажем, что введенное отношение на множестве R^D, оправдывая свое название, действительно является *отношением эквивалентности.*

Рефлексивность. $\forall\, f \in R^D$ $f \sim f$. Действительно, так как G — группа, то тождественная подстановка $\varepsilon \in G$; $f = f(\varepsilon)$.

Симметричность. Если $f_1 \sim f_2$, то $f_2 \sim f_1$. Для доказательства этого утверждения заметим, что если подстановка g принадлежит G, то и обратная ей подстановка g^{-1} является элементом G; дальнейшее рассуждение очевидно.

Транзитивность. Если $f_1 \sim f_2$ и $f_2 \sim f_3$, то $f_1 \sim f_3$. В самом деле, если $f_1(g_1) = f_2$ и $f_2(g_2) = f_3$, то $f_1(g_1 g_2) = f_3$, т. е. $f_1 \sim f_3$.

Каждому элементу r множества R придадим некоторый *вес* $w(r)$. Вес — это элемент некоторого коммутативного кольца; например, число или переменная. *Весом функции* $f \in R^D$ назовем произведение весов образов всех элементов множества D при отображении f:

$$W(f) = \prod_{d \in D} w(f(d)).$$

Пример. Пусть $D = \{1, 2, 3, 4\}$ — множество вершин тетраэдра; $R = \{$синий, красный, зеленый, белый$\} = \{$с, к, з, б$\}$ — множество цветов. Тогда R^D — множество всевозможных раскрасок вершин тетраэдра в указанные цвета. С помощью G — группы подстановок вершин, возникающих в результате вращений тетраэдра, множество R^D разбивается на классы эквивалентности. Класс эквивалентности составляют раскраски, переходящие друг в друга в результате вращений тетраэдра, такие раскраски будем называть также *геометрически неразличимыми.* Например, с точностью до геометрической неразличимости существует ровно одна раскраска, при которой три вершины — белые, а одна — красная. Каждому элементу множества R придадим вес: $w(\text{с}) = x$, $w(\text{к}) = y$, $w(\text{з}) = z$, $w(\text{б}) = t$. Вес упомянутой выше раскраски равен $t^3 y$.

Теорема 2. *Эквивалентные функции имеют одинаковый вес:*

$$\textit{если} \quad f_1 \sim f_2, \quad \textit{то} \quad W(f_1) = W(f_2).$$

◀ Если $f_1 \sim f_2$, то для некоторой подстановки $g \in G$ имеем $f_1(g) = f_2$. Вес функции f_1 равен

$$W(f_1) = \prod_{d \in D} w(f_1(d)) = \prod_{d \in D} w\big(f_1(g(d))\big).$$

Последнее равенство имеет место в силу того, что g — подстановка: если d пробегает по всему множеству D, то и $c = g(d)$ обладает тем же свойством. Продолжим выкладки:

$$W(f_1) = \prod_{d \in D} w\big(f_1(g(d))\big) = \prod_{d \in D} w(f_2(d)) = W(f_2),$$

что и требовалось доказать. ▶

Теперь становится корректным следующее определение. *Весом класса эквивалентности* называется вес любой функции из этого класса: если F — класс эквивалентности и $f \in F$, то $W(F) = W(f)$.

Заметим, что и у неэквивалентных функций могут совпадать веса. В качестве примера укажем для выше рассматривавшейся задачи две неэквивалентные раскраски одинакового веса (рис. 2): $f(1) = $ с, $f(2) = $ к, $f(3) = $ з, $f(4) = $ б; $h(1) = $ с, $h(2) = $ к, $h(3) = $ б, $h(4) = $ з.

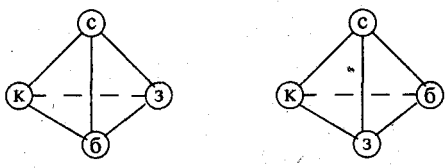


Рис. 2

Инвентарем множества называется сумма весов его элементов:

$$\operatorname{inv} R = \sum_{r \in R} w(r).$$

Поскольку определены веса функций, а также классов эквивалентности функций, то можно говорить об инвентарях соответствующих множеств. Докажем, что

$$\boxed{\operatorname{inv} R^D = (\operatorname{inv} R)^{|D|}.} \tag{1}$$

Пусть $w_1, w_2, \ldots, w_{|R|}$ — веса элементов множества R. Если раскрыть скобки в произведении

$$(\operatorname{inv} R)^{|D|} = (w_1 + w_2 + \ldots + w_{|R|}) \ldots (w_1 + w_2 + \ldots + w_{|R|}),$$

не приводя подобные и не меняя порядок множителей, то получим сумму вида:

$$(\operatorname{inv} R)^{|D|} = w_1 w_1 \ldots w_1 + w_1 w_1 \ldots w_2 + \ldots + w_{|R|} w_{|R|} \ldots w_{|R|}. \tag{2}$$

Выбор члена из каждой скобки при образовании одного члена разложения (2) можно рассматривать как функцию $f : D \to R$, тогда сам член (2) будет ее весом; в сумме (2) каждое слагаемое есть вес некоторой функции из R^D; при этом для каждой такой функции в сумме найдется ровно одно соответствующее ей слагаемое. Таким образом, полученная сумма есть инвентарь множества R^D.

Для дальнейшего нам будет полезно следующее обобщение только что доказанного утверждения. Пусть $D_1, D_2, \ldots, D_k$ — разбиение множества D на k подмножеств; S — множество функций, постоянных на каждом подмножестве. Тогда

$$\boxed{\operatorname{inv} S = \prod_{i=1}^{k} \sum_{r \in R} w(r)^{|D_i|}.} \tag{3}$$

Заметим, что если $|D_i| = 1$ для всех i, то (3) переходит в (1). Раскрыв скобки в правой части (3), получим сумму всевозможных произведений вида

$$w_{i_1}^{|D_1|} \cdot w_{i_2}^{|D_2|} \cdot \ldots \cdot w_{i_k}^{|D_k|}, \tag{4}$$

где $(i_1, i_2, \ldots, i_k)$ — размещение с повторениями из множества $\{1, 2, \ldots, |R|\}$. Пусть функция $f \in S$ на элементах множества D_i принимает значение $r_i^{(f)}$ и $w\left(r_i^{(f)}\right) = w_i^{(f)}$ $(i = 1, 2, \ldots, k)$. Тогда

$$W(f) = \left(w_1^{(f)}\right)^{|D_1|} \cdot \left(w_2^{(f)}\right)^{|D_2|} \cdot \ldots \cdot \left(w_k^{(f)}\right)^{|D_k|}, \tag{5}$$

где $\left(w_1^{(f)}, w_2^{(f)}, \ldots, w_k^{(f)}\right)$ — размещение с повторениями из множества $\{w_1, w_2, \ldots, w_{|R|}\}$. Таким образом, сумма всевозможных произведений (4) совпадает с суммой весов всех функций из S, что и требовалось доказать.

§ 4. Теорема Пойа

Пусть D и R — конечные множества, G — группа подстановок элементов D, с помощью которой множество функций $R^D = \{f : R \to D\}$ разбивается на классы эквивалентности ($f_1 \sim f_2$, если $\exists\, g \in G$ $f_1(g) = f_2$). Пусть элементам $r \in R$ приписаны веса $w(r)$ (элементы некоторого коммутативного кольца). В предыдущем параграфе указано, как задается вес функции $W(f)$ и вес класса эквивалентности $W(F)$.

Теорема 3 (Д. Пойа, 1937 г.). *Сумма весов классов эквивалентности равна*

$$\sum_{F} W(F) = P_G\left(\sum_{r \in R} w(r), \sum_{r \in R} w^2(r), \sum_{r \in R} w^3(r), \ldots\right),$$

где P_G — цикловой индекс группы подстановок G.

Прежде, чем доказывать саму теорему, укажем на ее простое

Следствие. *Число классов эквивалентности равно $P_G(|R|, |R|, |R|, \ldots)$.*

Действительно, если положить вес каждого элемента R равным 1, то и вес каждой функции, и, значит, каждого класса эквивалентности будет равен 1; поэтому сумма весов всех классов эквивалентности будет равна их числу.

◄ Доказательство теоремы Пойа. Пусть S_w — множество функций, имеющих вес w:

$$S_w = \{f \in R^D \mid W(f) = w\}.$$

Обозначим через $I_w(g)$ число функций веса w, инвариантных относительно подстановки $g \in G$, т. е. таких, что $W(f) = w$ и $fg = f$. Тогда

$$\boxed{\sum_{f,\, fg=f} W(f) = \sum_w w I_w(g).} \tag{1}$$

Докажем, что число классов эквивалентности для множества S_w равно

$$\boxed{N_w = \frac{1}{|G|} \sum_{g \in G} I_w(g).} \tag{2}$$

Доказательство основывается на лемме Бернсайда. Если $f \in S_w$, то для произвольной подстановки $g \in G$ функция fg^{-1} также имеет вес w (ввиду эквивалентности $fg^{-1} \sim f$; как было доказано в предыдущем параграфе, эквивалентные функции имеют одинаковый вес). Следовательно, подстановка g, действующая на множестве D, задает подстановку функций из множества S_w; обозначим ее π_g:

$$\pi_g f = fg^{-1}.$$

Нетрудно убедиться в том, что соответствие $g \to \pi_g$ является гомоморфизмом. Действительно, для любой функции f

$$\pi_{g_1 g_2} f = f(g_1 g_2)^{-1} = f g_2^{-1} g_1^{-1} = (f g_2^{-1}) g_1^{-1} = \pi_{g_1}(f g_2^{-1}) = \pi_{g_1} \pi_{g_2} f,$$

то есть $\pi_{g_1 g_2} = \pi_{g_1} \pi_{g_2}$. Осталось заметить, что отношения эквивалентности, порожденные на множестве S_w подстановками g (действующими на множестве D) и подстановками π_g (действующими на самом множестве S_w), совпадают; а инвариантность функции f относительно g означает ее инвариантность относительно π_g ($fg = f \iff f = fg^{-1} \iff f = \pi_g f$). Теперь непосредственное применение леммы Бернсайда дает (2).

Зная число классов эквивалентности N_w для любого (фиксированного) веса w, запишем соотношение для суммы весов *всех* классов эквивалентности:

$$\sum_F W(F) = \sum_w w N_w = \sum_w w \frac{1}{|G|} \sum_{g \in G} I_w(g) = \frac{1}{|G|} \sum_{g \in G} \sum_w w I_w(g).$$

Применив (1), получим:

$$\sum_F W(F) = \frac{1}{|G|} \sum_{g \in G} \sum_{f,\, fg=f} W(f). \tag{3}$$

Как отмечалось в § 1, подстановка g разбивает множество D на орбиты, элементы которых циклически переставляются данной подстановкой. Если $fg = f$, то на каждой такой орбите функция f постоянна:

$$\forall\, d \in D \quad f(d) = fg(d) = f(gd) = f(g^2 d) = f(g^3 d) = \ldots .$$

Верно и обратное. Пусть функция f постоянна на каждой орбите, порожденной подстановкой g. Тогда $f(d) = f(g(d))$ для любого элемента $d \in D$, что означает: $f = fg$.

Таким образом, множество функций, инвариантных относительно g, совпадает с множеством функций, принимающих постоянные значения на орбитах, порожденных подстановкой g (обозначим их $D_1, \ldots, D_k$). Поэтому можно применить соотношение (3) из предыдущего параграфа:

$$\sum_{f,\, fg=f} W(f) = \prod_{i=1}^{k} \sum_{r \in R} w(r)^{|D_i|}.$$

Если у подстановки g тип $(k_1, k_2, \ldots)$ (т. е. имеется k_1 орбит длины 1, k_2 орбит длины 2 и т. д.), то, перегруппировав множители в последнем произведении, получим:

$$\sum_{f,\, fg=f} W(f) = \left(\sum_{r \in R} w(r)\right)^{k_1} \cdot \left(\sum_{r \in R} w^2(r)\right)^{k_2} \cdot \ldots .$$

Найденное произведение можно рассматривать как результат замены переменных $x_1, x_2, \ldots$ в цикловом индексе подстановки g, равном $x_1^{k_1} x_2^{k_2} \ldots$, значениями сумм соответствующих степеней весов элементов $r \in R$. Таким образом, согласно (3) сумма весов классов эквивалентности есть среднее арифметическое (по множеству G) цикловых индексов подстановок $g \in G$ при указанных значениях переменных $x_1, x_2, \ldots$:

$$\sum_{F} W(F) = P_G\left(\sum_{r \in R} w(r), \sum_{r \in R} w^2(r), \sum_{r \in R} w^3(r), \ldots\right).$$

Теорема доказана. ►

§ 5. Примеры

В этом параграфе теорема Пойа будет применена к решению ряда комбинаторных задач.

1. Начнем с задачи о числе *существенно различных* раскрасок вершин тетраэдра в k цветов (решенной ранее с помощью леммы Бернсайда). Здесь

D — множество вершин тетраэдра;

R — множество цветов, $|R| = k$;

G — группа подстановок вершин тетраэдра, порожденных вращениями тетраэдра;

R^D — множество раскрасок.

Класс эквивалентности в множестве R^D составляют раскраски, которые переходят друг в друга в результате вращений тетраэдра. Таким образом, задача сводится к подсчету числа классов эквивалентности. Цикловой индекс группы G был найден в § 1:

$$P_G(x_1, x_2, x_3, x_4) = \frac{1}{12}\left(x_1^4 + 8x_1x_3 + 3x_2^2\right).$$

Применив следствие из теоремы Пойа, получим тот же ответ, что и ранее (см. § 2):

$$\frac{1}{12}(k^4 + 11k^2).$$

Заметим, что применение теоремы Пойа позволяет найти не только общее число существенно различных раскрасок, но и определить число таких раскрасок при фиксированном распределении цветов. Если известно, какое количество вершин каким цветом должно быть покрашено, то тем самым задан вес раскраски. Коэффициент в инвентаре (сумме весов) классов эквивалентности при соответствующем весе и есть искомое число.

2. Задача о перечислении изомеров органических молекул заданной структуры (рис. 3), где C — атом углерода, а места, обозначенные крестиками, могут занимать метил (CH_3), этил (C_2H_5), водород (H) и хлор (Cl). Математическая модель этих молекул — тетраэдр, в центре которого расположен атом углерода. Расположение в вершине тетраэдра определенной группы атомов будем считать покраской вершины в определенный цвет (один из четырех). Таким образом, задача сведена к предыдущей (при $k = 4$). Общее число молекул равно $\frac{1}{12}(4^4 + 11 \cdot 4^2) = 36$. Для того чтобы подсчитать число молекул с фиксированным числом атомов водорода, положим:

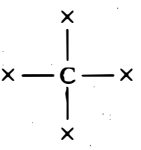


Рис. 3

$$w(\mathrm{H}) = x, \quad w(\mathrm{Cl}) = w(\mathrm{CH_3}) = w(\mathrm{C_2H_5}) = 1.$$

Тогда вес молекулы с i атомами водорода будет равен x^i. Применяя теорему Пойа, найдем инвентарь множества изомеров молекул:

$$P_G(x + 3, x^2 + 3, x^3 + 3) = x^4 + 3x^3 + 6x^2 + 11x + 15.$$

Значит, существует 1 молекула CH_4 (метан), 3 молекулы с 3 атомами H, 6 молекул с 2 атомами H, 11 молекул с 1 атомом H, 15 молекул без атома H.

3. Задача о компостере. *Компостером* назовем двоичную матрицу 4×4. Здесь D — множество позиций элементов в матрице, $|D| = 16$; $R = \{0, 1\}$. Группа G подстановок множества D определяется группой самосовмещений квадрата (см. § 6 гл. LXVII) и состоит из 8 элементов:

- тождественная подстановка ε (порождающая 16 единичных орбит; ее цикловой индекс (ц. и.) x_1^{16});
- две подстановки, соответствующие поворотам на 90° по и против часовой стрелки (4 орбиты длины 4; цикловой индекс каждой из подстановок x_4^4);
- подстановка, соответствующая центральной симметрии (8 орбит длины 2; ц. и. x_2^8);
- две подстановки, соответствующие осевым симметриям относительно вертикальной и горизонтальной осей (ц. и. x_2^8);
- две подстановки, соответствующие симметриям относительно диагоналей (4 элемента остаются на месте, остальные разбиваются на пары; ц. и. $x_1^4 x_2^6$).

Цикловой индекс группы G равен

$$P_G(x_1, x_2, \ldots) = \frac{1}{8}\left(x_1^{16} + 2x_4^4 + 3x_2^8 + 2x_1^4 x_2^6\right).$$

Если отождествить компостеры, которые получаются друг из друга указанными преобразованиями[2], то число *различных* компостеров определится так:

$$P_G(2, 2, 2, \ldots) = \frac{1}{8}\left(2^{16} + 2 \cdot 2^4 + 3 \cdot 2^8 + 2 \cdot 2^4 \cdot 2^6\right) = 8548.$$

Если читателю задача о числе компостеров кажется неактуальной, то можно указать на сводящуюся к ней задачу о фотошаблонах рисунков соединений интегральных схем (чипов).

4. Задача о числе ожерелий. Имеется неограниченный запас бусинок k цветов. Сколько можно составить различных ожерелий из n бусинок (ожерелья, получающиеся друг из друга плоскими вращениями, не будем различать)?

Считая, что бусинки располагаются в вершинах правильного n-угольника, сведем задачу к задаче о числе геометрически различных (т. е. не получающихся друг из друга вращениями в плоскости) раскрасок вершин правильного n-угольника в k цветов. При этом D — множество вершин, R — множество цветов, $|D| = n$, $|R| = k$; R^D — множество раскрасок. Отношение эквивалентности на множестве R^D задается с помощью G — группы подстановок вершин, порожденной вращениями правильного n-угольника; $|G| = n$ (см. § 6 гл. LXVII).

Пусть $G = \{g_1, g_2, \ldots, g_n\}$, где g_j — подстановка, возникающая в результате поворота на угол $\frac{2\pi}{n} j$ $(j = 1, \ldots, n)$ (в частности, тождественная подстановка $\varepsilon = g_n$). Тогда, если отождествить вершину с ее номером, положив $D = \{1, 2, \ldots, n\}$ (номера проставляются по порядку против часовой стрелки), то подстановка g_j описывается соотношениями:

$$g_j(i) = \begin{cases} i + j, & \text{если } i + j \leqslant n; \\ i + j - n, & \text{если } i + j > n. \end{cases}$$

Подстановка g_j сводится к увеличению номера вершины на j по модулю n:

$$\forall i, j \quad g_j(i) \equiv i + j (\mathrm{mod}\, n).$$

Длину орбиты произвольного элемента можно найти как наименьшее натуральное число k, для которого kj делится на n. Если (n, j) — наибольший общий делитель j и n, то $j = j_1(n, j)$, $n = n_1(n, j)$, где j_1 и n_1 — взаимно простые числа. Поэтому $kj = kj_1(n, j)$ делится на $n = n_1(n, j)$ тогда и только тогда, когда k делится на n_1, наименьшее натуральное k с таким свойством равно $n_1 = \frac{n}{(n,j)}$. Итак, при повороте на угол $\frac{2\pi j}{n}$ все орбиты имеют длину $\frac{n}{(n,j)}$, стало быть, число орбит равно (n, j). Запишем цикловой индекс группы подстановок:

$$P_G(x_1, x_2, \ldots) = \frac{1}{n} \sum_{j=1}^{n} x_{n/(n,j)}^{(n,j)}.$$

[2] Практическая задача, которой соответствует описываемая математическая постановка, очевидна: множеству D отвечают места возможных дырок, которые пробивает *реальный* компостер; 1(0) отвечает наличию (отсутствию) дырки в соответствующем месте; наконец, эквивалентные компостеры характерны тем, что по пробитому абонементу невозможно определить, на каком из них он был прокомпостирован.

По следствию из теоремы Пойа общее число раскрасок N выражается формулой:

$$N = \frac{1}{n}\sum_{j=1}^{n} k^{(n,j)}.$$

В полученной сумме показатели степеней k принимают значения делителей числа n. Несложно видеть, что общее количество чисел из множества $\{1, 2, \ldots, n\}$, для которых их наибольший делитель с n равен d, где $d|n$, совпадает с количеством натуральных чисел, не превосходящих число $\frac{n}{d}$ и взаимно простых с ним, т. е. с $\varphi\left(\frac{n}{d}\right)$ (φ — функция Эйлера). Таким образом,

$$\boxed{N = \frac{1}{n}\sum_{d|n} k^d \varphi\left(\frac{n}{d}\right).}$$

Замечание. Задача не слишком усложнится, если не отличать друг от друга также ожерелья, переходящие друг в друга в результате выполнения осевых симметрий; вместо группы вращений правильного n-угольника нужно будет рассматривать группу его симметрий.

Упражнения

1. Пусть $S = \{a, b, c, d\}$ и $G = \{\pi_1, \pi_2, \pi_3, \pi_4\}$ — группа подстановок, действующая на множестве S:

$$\pi_1 = \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}, \quad \pi_2 = \begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix},$$

$$\pi_3 = \begin{pmatrix} a & b & c & d \\ a & b & d & c \end{pmatrix}, \quad \pi_4 = \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}.$$

   1) Убедиться в том, что G — группа, составив для нее квадрат Кэли.
   2) Отношение эквивалентности на S порождается группой G. С помощью леммы Бернсайда найти число классов эквивалентности.
   3) Выписать классы эквивалентности в явном виде.

2. Составляются трехбуквенные слова из букв a и b. Два различных слова считаются эквивалентными, если они получаются друг из друга при перемене местами крайних букв; например, $abb \sim bba$. Определить число классов эквивалентности, пользуясь леммой Бернсайда. Выписать классы эквивалентности в явном виде.
3. Вокруг стола рассаживаются n человек. Сколько существует различных расположений, если отождествлять такие, которые получаются одно из другого сдвигом всех людей по часовой стрелке на произвольное, но одинаковое для всех число мест?
4. На листках бумаги пишут числа от 00000 до 99 999 (числа, меньшие 10 000, дополняют слева нулями). Будем считать, что при переворачивании цифры 0, 1, 8 не меняются, а цифры 6 и 9 переходят друг в друга. Например, для чисел 06981 и 18 690 можно приготовить только один листок. Сколько всего листков понадобится?
5. Составляются ожерелья из бусин трех цветов. Каждое ожерелье состоит из 1) 5; 2) 6 бусин. Не будем различать ожерелья, получающиеся друг из друга поворотом в плоскости. Пользуясь леммой Бернсайда, найти число различных ожерелий.
6. Решить предыдущую задачу в предположении, что не различаются ожерелья, получающиеся друг из друга поворотом в пространстве.

7. Решить задачи 5, 6 с помощью следствия из теоремы Пойа.
8. Сколько ожерелий можно составить из двух красных, двух зеленых и двух синих бусин в предположениях задач 5 и 6?
9. Завод выпускает погремушки в виде кольца с надетыми на него p красными и q синими шариками. Сколько различных погремушек может быть выпущено? Две погремушки считаются одинаковыми, если могут быть получены друг из друга передвижением шариков по кольцу или переворачиванием.
10. Доказать, что цикловой индекс группы подстановок на множестве вершин правильного n-угольника, порожденных его вращениями в плоскости, есть

$$P_G(x_1, x_2, \ldots, x_n) = \frac{1}{n} \sum_{d|n} x_d^{\frac{n}{d}} \varphi(d).$$

11. Составляются ожерелья из n_1 бусинок 1-го вида, n_2 бусинок 2-го вида, ..., n_m бусинок m-го вида. Не считаются различными ожерелья, которые могут быть получены друг из друга вращением в плоскости. Доказать, что число различных ожерелий равно

$$\frac{1}{n} \sum \varphi(d) \frac{(n/d)!}{(n_1/d)!(n_2/d)! \ldots (n_m/d)!},$$

где суммирование ведется по всем числам d, одновременно являющимся делителями чисел $n_1, n_2, \ldots, n_m$.
12. Найти цикловой индекс группы подстановок на множестве вершин правильного n-угольника, порожденных группой его симметрий.
13. Сколькими способами можно раскрасить в k цветов
    1) ребра;
    2) грани тетраэдра, который может свободно вращаться в пространстве?
14. Сколькими способами можно раскрасить в k цветов
    1) вершины;
    2) ребра;
    3) грани куба, который может свободно вращаться в пространстве?
15. Сколькими геометрически различными способами можно раскрасить вершины куба в два цвета так, чтобы вершин каждого цвета было поровну?
16. Сколькими способами можно раскрасить 5 ребер куба в синий цвет, а остальные ребра в красный цвет?
17. Найти число существенно различных способов размещения восьми одинаковых пометок на шахматной доске размера 8×8. Два способа разметки считаются существенно различными, если их нельзя преобразовать друг в друга вращением доски или отражением относительно любой из четырех осей симметрии.
18. Конструктор интегральных схем строит чипы с 16 элементами, расположенными в виде матрицы 4×4. Чтобы реализовать различные схемы, эти элементы нужно соединять; непосредственно соединяются только элементы, соседние по горизонтали или по вертикали (рис. 4).

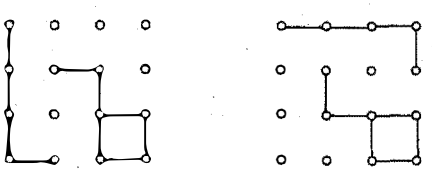


Рис. 4

Чтобы напылить межкомпонентные соединения, необходим фотошаблон рисунка соединений. Для двух рисунков, показанных выше, используется один и тот же фотошаблон (схемы симметричны относительно диагонали). Сколько требуется фотошаблонов для того, чтобы на этих чипах реализовать все возможные рисунки соединений?

19. Следующие две картинки (рис. 5) называются соответственно «Звезда Давида» и «Мечи Магомета».

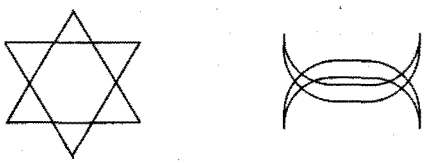


Рис. 5

Представим себе, что эти фигуры составлены из кусков проволоки, спаянных в точках пересечений. Сколько существует различных звезд и мечей с точки зрения вида пересечений? Две фигуры отождествляем, если одну из них можно переместить в пространстве так, что они становятся неразличимыми по виду пересечений (рис. 6).

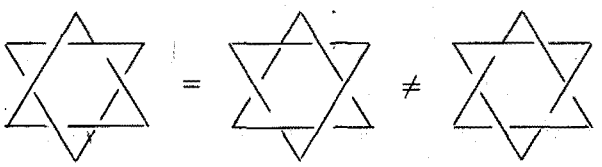


Рис. 6

Ответы

3. $(n-1)!$. **4.** 98475. **8.** 16 и 11 соответственно.

10. Как известно,

$$P_G(x_1, x_2, \ldots) = \frac{1}{n}\sum_{j=1}^{n} x_{n/(n,j)}^{(n,j)}.$$

В полученной сумме нижний индекс при x принимает значения всех делителей числа n. В качестве упомянутого индекса число d встретится столько раз, сколько есть чисел j от 1 до n, для которых $(n, j) = n/d$. Такие числа имеют вид $j = kn/d$, где число k взаимно просто с d и не превосходит d. Значит, d будет в качестве нижнего индекса ровно $\varphi(d)$ раз.

11. Применив теорему Пойа, выражение для циклового индекса из предыдущей задачи и полиномиальную формулу, получим:

$$P_G\Big(\sum w_i,\ \sum w_i^2,\ \ldots\Big) = \frac{1}{n}\sum \varphi(d) \sum_{k_1+\ldots+k_m=n/d} w_1^{k_1 d}\ldots w_m^{k_m d}\frac{(n/d)!}{k_1!\ldots k_m!}.$$

Нас интересует коэффициент при $w_1^{n_1}\ldots w_m^{n_m}$. Указанное произведение возникает лишь при d, делящем одновременно $n_1, \ldots, n_m$. Дальнейшее просто.

12. Если n четно, то

$$P_G = \frac{1}{2n}\left(\sum_{d|n} x_d^{n/d}\varphi(d) + \frac{n}{2}x_1^2 x_2^{(n/2)-1} + \frac{n}{2}x_2^{n/2}\right).$$

Если n нечетно, то

$$P_G = \frac{1}{2n}\left(\sum_{d|n} x_d^{n/d}\varphi(d) + nx_1 x_2^{(n-1)/2}\right).$$

17. $\frac{1}{8}\left(C_{64}^8 + 2C_{16}^2 + 3C_{32}^4 + 2\left(C_{28}^4 + C_8^2 C_{28}^3 + C_8^4 C_{28}^2 + C_8^6 C_{28}^1 + C_8^8\right)\right) = 553\,332\,533.$

18. $\frac{1}{8}(2^{24} + 2\cdot 2^6 + 3\cdot 2^{12} + 2\cdot 2^4\cdot 2^{10}) = 2\,102\,800.$

19. 13 звезд и 88 мечей.

Глава LXX

ВВЕДЕНИЕ В ТЕОРИЮ ГРАФОВ

История становления теории графов интересна и поучительна.

Первая известная публикация была ответом на головоломку, подобную тем, которыми в разное время любили скрашивать свой досуг. Отнесясь к вопросу, поставленному в письме коллеги (о том, как именно можно пройти по семи мостам славного города Кёнигсберга) вполне серьезно, Леонард Эйлер, как он сам писал позже в одном из своих писем, «после долгих размышлений нашел простое правило», позволившее ему решить предложенную и значительно более сложные задачи, придуманные им самим. Однако несмотря на стремительно нарастающий научный авторитет Эйлера, эта публикация (*Euler L.* Solutio problematis ad geometriam situs pertinentes, Commentarii Academiae Petropolitanae. 8. 1736. P. 128–140) не привлекла внимания ни современных ему ученых, ни нескольких последующих поколений исследователей. Во всяком случае никаких следов проявления интереса к заявленной проблематике до 1856 года не замечено.

Придуманная тогда Уильямом Гамильтоном игрушка в виде утыканного гвоздиками деревянного додекаэдра также долгое время оставалась предметом досужих размышлений, и никто не думал, что через несколько десятков лет две эти развлекательные задачи займут достойное место в востребованной ныне теории графов (сам этот термин появился лишь в 1936 году).

Конечно, этой востребованности в немалой степени способствовали серьезные работы Густава Кирхгофа по исследованию электрических цепей и Артура Кэли при описании строения углеводородов, а также заметно увеличивавшийся поток задач, возникавших в различных областях науки и техники.

Оказалось, что при помощи графов можно вполне успешно моделировать и решать самые разнообразные задачи.

Все это потребовало обоснований, необходимость построения которых вылилась в новую теорию. Не были забыты ни Эйлер, ни Гамильтон. Их имена носят графы с весьма интересными свойствами.

Так и возникли два естественных направления работы с графами:

- первое — изучение свойств собственно графов (терминология, утверждения, доказательства, формулы, т.е. все, как и положено в любой математической теории),
- второе — применение графов в других науках и в прикладных задачах (вот только некоторые из них: деревья вероятностей и деревья решений, сетевые задачи: оценка временных затрат на выполнение больших проектов и пропускной способности различных коммуникаций, поиск кратчайших маршрутов и др.).

В этой небольшой главе мы постарались уделить внимание обоим из указанных направлений.

§ 1. Определения и примеры

Простым графом называется упорядоченная пара $G = \langle V, E\rangle$, где V — непустое конечное множество (элементы V — *вершины* графа); E — конечное множество неупорядоченных пар различных элементов V (элементы E — *ребра*[1] графа).

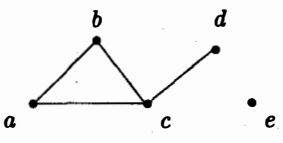


Рис. 1

Графы удобно представлять рисунками, в которых вершины изображаются точками, а ребра — линиями, соединяющими соответствующие точки[2]. Например, на рис. 1 изображен простой граф с множеством вершин $V = \{a, b, c, d, e\}$ и множеством ребер

$$E = \big\{\{a, b\}, \{a, c\}, \{b, c\}, \{c, d\}\big\}.$$

Граф — упорядоченная пара $G = \langle V, E\rangle$, где V — непустое конечное множество (элементы V — *вершины* графа); E — конечное *мультимножество* неупорядоченных пар элементов V (необязательно различных) (элементы E — *ребра*).

Термин *мультимножество* говорит о том, что элементы в E могут повторяться; повторяющиеся элементы называют *кратными ребрами*.

Если в графе имеется ребро $e = uv$, то говорят:

вершины u и v — *смежные*, или

ребро e *инцидентно* вершинам u и v; вершины u и v *инцидентны* ребру e, или

ребро e *соединяет* вершины u и v, или

вершины u и v — *концы* ребра e.

Два различных ребра называются *смежными*, если они имеют по крайней мере одну общую вершину. На рис. 2 изображен граф с множеством вершин $V = \{a, b, c, d, e\}$ и мультимножеством ребер E: ab, ac, ac, bc, bb, cd.

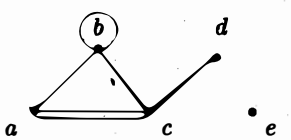


Рис. 2

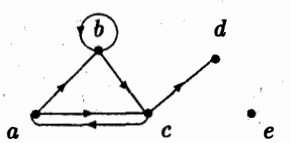


Рис. 3

Ребро вида uu (соединяющее некоторую вершину саму с собой) называют *петлей*. Таким образом, простой граф — это граф без петель и кратных ребер.

Ориентированный граф — упорядоченная пара $G = \langle V, A\rangle$, где V — непустое конечное множество — множество вершин; A — конечное мультимножество *упорядоченных* пар элементов V (необязательно различных) — мультимножество *дуг*[3].

---

[1] Поясним выбор обозначений для множеств вершин и ребер. По-английски вершина — vertex, ребро — edge.

[2] Сам термин *граф* возник как сокращение слова graphic (график) и был введен в 1936 г. венгерским математиком Д. Кёнигом.

[3] A — первая буква слова arc — дуга (англ.).

На рис. 3 изображен граф с множеством вершин $V = \{a, b, c, d, e\}$ и мультимножеством дуг A: (a, b), (a, c), (c, a), (b, c), (b, b), (c, d). К ориентированным графам мы вернемся лишь в конце данной главы.

Степенью вершины графа называется число инцидентных ей ребер. При подсчете степени вершины петлю будем учитывать дважды. Обозначение степени вершины v: $\rho(v)$. Вершина v называется *изолированной*, если $\rho(v) = 0$, и *висячей*, если $\rho(v) = 1$. Имеет место следующее простое утверждение.

Теорема 1 (лемма о рукопожатиях). *Сумма степеней всех вершин графа равна удвоенному числу ребер:*

$$\sum_{v \in V} \rho(v) = 2|E|.$$

Действительно, каждое ребро дает вклад 2 при подсчете суммы степеней всех вершин. В частности, если несколько человек обменялись рукопожатиями, то общее число рукопожатий будет четным (графовая модель для данной задачи очевидна).

Следствие. *В любом графе число вершин нечетной степени четно.*

Графы $G_1 = \langle V_1, E_1 \rangle$ и $G_2 = \langle V_2, E_2 \rangle$ называются *изоморфными*, если существует такое взаимно однозначное соответствие $\varphi : V_1 \to V_2$, при котором для любых двух вершин первого графа $u, v \in V_1$ число соединяющих их ребер равно числу ребер, соединяющих соответствующие им вершины второго графа $\varphi(u), \varphi(v)$. На рис. 4 изображены изоморфные графы (соответствующие друг другу вершины в них обозначены одинаковыми номерами).

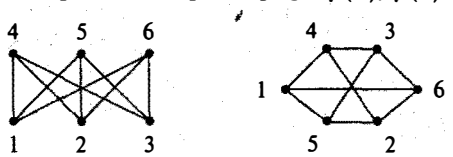


Рис. 4

Ясно, что в изоморфных графах одинаковое число вершин, ребер (а также петель и кратных ребер). Однако данное условие не является достаточным для изоморфности. Два графа, изображенные на рис. 5, не являются изоморфными (хотя бы потому, что в одном графе имеется «треугольник», а во втором — нет).

Отношение изоморфизма графов обладает свойствами рефлексивности, симметричности и транзитивности, т. е. является отношением эквивалентности.

Граф $G' = \langle V', E' \rangle$ называют *подграфом* графа $G = \langle V, E \rangle$ (обозначение $G' \subset G$), если $V' \subset V$, $E' \subset E$. Заметим, что если G_1 и G_2 — изоморфные графы, то для любого подграфа G_1 найдется изоморфный ему граф, являющийся подграфом G_2.

Рис. 5

Порядок графа — число его вершин. Граф порядка n называется *помеченным*, если его вершинам присвоены *метки* — числа от 1 до n (причем у разных вершин — разные метки). Часто мы будем отождествлять вершину с ее меткой. *Матрицей смежности* помеченного графа называется матрица $A = (a_{ij})$, где a_{ij} — число ребер, соединяющих вершины i и j. На рис. 6 изображен помеченный

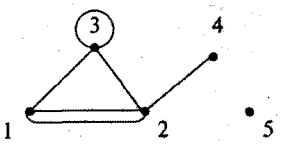


Рис. 6

граф 5-го порядка и приведена его матрица смежности

$$\begin{pmatrix} 0 & 2 & 1 & 0 & 0 \\ 2 & 0 & 1 & 1 & 0 \\ 1 & 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Свойства матрицы смежности

1) Каждый элемент матрицы — неотрицательное целое число.
2) Матрица является симметричной: $A^T = A$ (символ ^{T} означает операцию транспонирования).
3) Сумма элементов i-й строки равна степени вершины i:

$$\boxed{\sum_j a_{ij} = \rho(i).}$$

4) Пусть A и A' — матрицы смежности изоморфных графов. Тогда найдется такая матрица перестановок[4] P, что

$$\boxed{A' = PAP^{-1}.}$$

Первые три свойства очевидны; докажем последнее свойство. Пусть φ — функция, устанавливающая изоморфное соответствие между графами G' и G с матрицами смежности соответственно A' и A:

$$\forall\, i, j \quad a'_{ij} = a_{\varphi(i),\varphi(j)}. \tag{1}$$

Сформируем матрицу P следующим образом: в i-й строке поставим единицу в $\varphi(i)$-й столбец. Тогда матрица $B = PA$ получается из матрицы A такой перестановкой ее строк, что i-й строкой становится строка с номером $\varphi(i)$ матрицы A ($i = 1, \ldots, n$; n — порядок графа). Легко проверить, что матрица, обратная к матрице перестановок, совпадает с транспонированной к ней: $P^{-1} = P^T$. Матрица $BP^T = PAP^{-1}$ получается из матрицы B такой перестановкой ее столбцов, что j-м столбцом становится столбец с номером $\varphi(j)$ матрицы B ($j = 1, \ldots, n$). Таким образом, число, стоящее в i-й строке и j-м столбце матрицы PAP^{-1}, совпадает с числом, которое находится в $\varphi(i)$-й строке и $\varphi(j)$-м столбце матрицы A ($i, j = 1, \ldots, n$). В силу (1) отсюда и вытекает требуемое: $A' = PAP^{-1}$.

Реберным графом $L(G)$ графа G называется граф, множество вершин которого находится во взаимно однозначном соответствии с множеством ребер G, причем две вершины в $L(G)$ смежны тогда и только тогда, когда смежны соответствующие им ребра графа G. Примеры реберных графов см. на рис. 7, где ребра графов G, G_1, G_2 помечены теми же номерами, которые имеют соответствующие им вершины реберных графов. Очевидно, что из изоморфности графов

[4] Матрица перестановок — матрица, в каждой строке и каждом столбце которой находится ровно по одной единице, а остальные элементы нули.

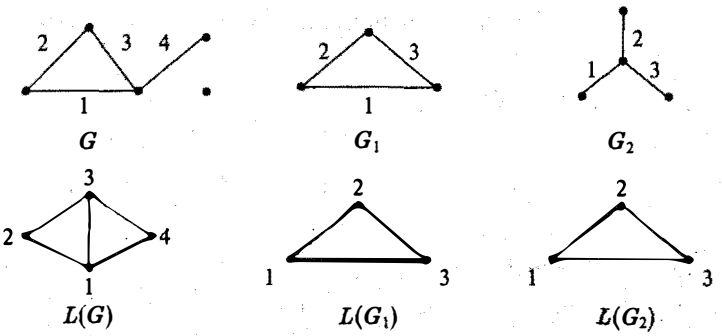


Рис. 7

вытекает изоморфность их реберных графов. Обратное, вообще говоря, неверно (см. примеры)[5].

Граф, в котором нет ребер, называют *пустым*. Пустой граф порядка n будем обозначать N_n. Все вершины пустого графа являются изолированными.

Простой граф, в котором любые две вершины смежны, называют *полным*. Обозначение полного графа порядка n: K_n. Число ребер в K_n равно

$$C_n^2 = \frac{n(n-1)}{2}.$$

Граф называется *регулярным степени* r, если степени всех его вершин равны r. Графы K_n и N_n являются регулярными, их степени соответственно $n-1$ и 0. Регулярный граф степени 3 называют *кубическим*. В частности, кубическим будет граф, вершины и ребра которого соответствуют вершинам и ребрам куба. Кубическим является и *граф Петерсена*, изображенный на рис. 8.

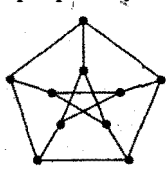


Рис. 8

Платоновыми графами называют графы, образованные вершинами и ребрами платоновых тел — правильных многогранников. Все они являются регулярными.

Граф называется *двудольным*, если множество его вершин V представимо в виде объединения двух непересекающихся непустых множеств V_1 и V_2, и при этом каждое ребро графа соединяет какую-либо вершину из V_1 с какой-либо вершиной из V_2. Множества вершин V_1 и V_2 будем называть *долями* графа. Заметим, что вершины двудольного графа можно «раскрасить»[6] в два цвета так, что каждое ребро будет иметь концы разного цвета (вершины одного цвета будут при этом составлять одну долю). *Полным двудольным графом* $K_{n,m}$ называется двудольный граф, в которым доли имеют соответственно n и m вершин, и любые две вершины, входящие в разные доли, смежны. $K_{n,m}$ содержит nm ребер. *Звездным* называют граф $K_{1,n}$. В нем n висячих вершин и одна вершина степени n. На рис. 9 изображены двудольные графы.

[5] Оказывается, что приведенный контрпример является единственным исключением: из связных графов только G_1 и G_2, будучи неизоморфными, имеют изоморфные реберные графы.

[6] То есть каждой вершине приписать некоторый цвет.

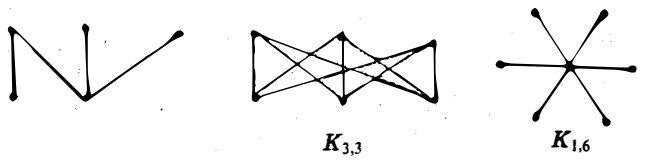


Рис. 9

Операции над графами

Объединением графов $G_1 = \langle V_1, E_1\rangle$ и $G_2 = \langle V_2, E_2\rangle$ называется граф $G_1 \cup G_2 = \langle V_1 \cup V_2, E_1 \cup E_2\rangle$. Объединение графов — *дизъюнктное*, если объединяемые графы не имеют общих вершин: $V_1 \cap V_2 = \varnothing$. Очевидно, что операция объединения графов ассоциативна; поэтому употребление записей вида $G_1 \cup G_2 \cup G_3$ или $\cup_i G_i$ не будет приводить к недоразумениям.

Соединение графов $G_1 = \langle V_1, E_1\rangle$ и $G_2 = \langle V_2, E_2\rangle$ — граф $G_1 + G_2$, который получается из дизъюнктного объединения графов $G_1 \cup G_2$ добавлением всевозможных ребер вида v_1v_2, где $v_1 \in V_1$, $v_2 \in V_2$. Например, $N_n + N_m = K_{n,m}$. *Дополнением* к простому графу $G = \langle V, E\rangle$ называют граф $\overline{G} = \langle V, \overline{E}\rangle$, в котором множество вершин совпадает с множеством вершин исходного графа G, и вершины смежны тогда и только тогда, когда они не смежны в графе G. Например, $\overline{N}_n = K_n$, $\overline{K}_n = N_n$. Несложно видеть, что дополнение к дополнению G совпадает с G: $\overline{\overline{G}} = G$. Если граф G с n вершинами рассматривать как подграф полного графа K_n, то можно сказать, что граф $\overline{G}$ получается из K_n выбрасыванием ребер графа G. Отметим также, что дополнение к регулярному графу есть регулярный граф.

Граф называется *связным*, если его нельзя представить в виде дизъюнктного объединения двух графов и *несвязным* в противном случае. Любой граф можно представить в виде дизъюнктного объединения связных графов, каждый из которых называют *компонентой связности* исходного графа. На рис. 10 граф G_2 — связный, граф G_1 — несвязный (содержит 3 компоненты связности).

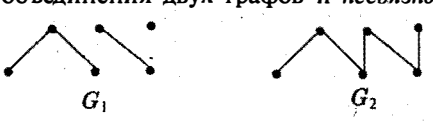


Рис. 10

Циклический граф — это связный регулярный граф степени 2. Циклический граф порядка n обозначают C_n. Граф

$$W_n = N_1 + C_{n-1} \quad (n \geqslant 3)$$

называют *колесом*. Примеры циклического графа и колеса — на рис. 11.

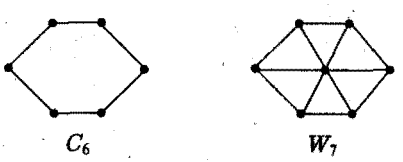


Рис. 11

§ 2. Связные графы

Маршрутом в графе называется последовательность ребер вида

$$v_0v_1, v_1v_2, \ldots, v_{m-1}v_m.$$

Каждому маршруту соответствует последовательность его вершин $v_0, v_1, \ldots, v_m$; v_0 называют *начальной вершиной* маршрута, а v_m — *конечной вершиной*; при этом

говорят о *маршруте из* v_0 *в* v_m. Маршрут удобно обозначать в следующем виде:

$$v_0 \to v_1 \to v_2 \to \ldots \to v_m.$$

Длиной маршрута называется число входящих в него ребер. *Тривиальный маршрут* имеет длину 0 (он не содержит ребер и определяется начальной вершиной v_0).

Маршрут называется *цепью*, если все его ребра различны, и *простой цепью*, если все его вершины различны, за исключением, может быть, начальной и конечной. Если в цепи $v_0 = v_m$, то цепь называют *замкнутой*.

Цикл в графе — замкнутая цепь, содержащая по крайней мере одно ребро.

Две вершины графа u и v назовем *связанными*, если в графе существует маршруг из u в v. Заметим, что если две вершины связаны, то существует соединяющая их простая цепь. Действительно, пусть имеется некоторый маршрут из u в v, не являющийся простой цепью, тогда найдется вершина маршрута w, встречающаяся в нем не менее двух раз, и маршрут имеет вид:

$$u \to \ldots \to w \to w_1 \to \ldots \to w \to \ldots \to v.$$

Удалив из маршрута участок $w_1 \to \ldots \to w$, вновь получим маршруг из u в v. Если при этом он не будет простой цепью, то указанную процедуру можно повторить. Бесконечное число раз она выполняться не будет, так как число ребер графа конечно. В результате получим простую цепь из u в v.

Отношение связанности на множестве вершин графа является отношением эквивалентности. Рефлексивность проистекает из того факта, что каждая вершина связана сама с собой тривиальным маршрутом. Симметричность следует из того, что взяв вершины маршрута из u в v в обратном порядке, получим маршруг из v в u. Транзитивность также очевидна: объединив маршруты из u в v и из v в w, получим маршрут из u в w.

Отношение связанности разбивает множество вершин графа на классы эквивалентности. Очевидно, что вершины из одного класса эквивалентности вместе с соединяющими их ребрами образуют компоненту связности графа (определение которой дано в конце предыдущего параграфа). Поскольку связный граф характеризуется тем, что имеет одну компоненту связности, приходим к выводу: *граф является связным тогда и только тогда, когда любые две его вершины — связанные.*

Разделяющим множеством графа называется такое множество его ребер, удаление которых приводит к увеличению числа компонент связности графа. *Разрез* — минимальное разделяющее множество (т. е. такое, что никакое его собственное подмножество не является разделяющим множеством). Ребро называется мостом, если оно образует разрез.

Пример. Для графа, изображенного на рис. 12, $\{e_1, e_2, e_3\}$ — разделяющее множество (но не разрез); $\{e_1, e_2\}$ — разрез; ребра e_6 и e_{10} являются мостами.

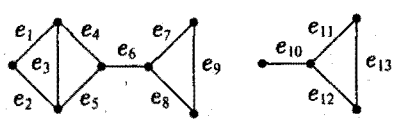


Рис. 12

Лемма 1. *Ребро в графе является мостом тогда и только тогда, когда оно не входит ни в один цикл.*

◀ Пусть ребро $e = uv$ — мост. Ясно, что при этом $u \neq v$. Предположим существование цикла, содержащего ребро e. Возьмем две произвольные вершины x

и y из той компоненты связности графа, которой принадлежит ребро e. Покажем, что они останутся связанными и после удаления ребра e. Действительно, если ребро e входит в некоторый маршрут, соединяющий x и y, то e можно заменить последовательностью ребер, составляющих вместе с e цикл (рис. 13). Таким образом, отношение связанности не меняется после удаления e, что противоречит определению моста.

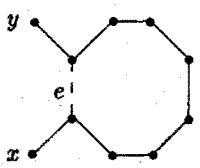


Рис. 13

Обратно. Пусть ребро $e = uv$ не входит ни в один цикл. Если при удалении e вершины u и v останутся связанными, это будет говорить о существовании соединяющей их простой цепи. Объединив ее с ребром e, получим цикл в исходном графе — противоречие! Таким образом, число компонент связности при удалении e увеличивается; e — мост. ►

Следующее утверждение уточняет понятие моста.

Лемма 2. *Удаление моста увеличивает число компонент связности графа на единицу.*

◄ Пусть $e = uv$ — мост. Рассмотрим компоненту связности, содержащую e. Через H_u обозначим множество ее вершин x, для которых существует маршрут из x в u, не содержащий ребра e. Остальные вершины составят множество H_v. Эти множества не пусты, так как $u \in H_u$ (вершина u связана сама с собой тривиальным маршрутом) и $v \in H_v$ (если бы существовал маршрут из v в u, не содержащий ребра e, то добавив к нему это ребро, получили бы цикл, что противоречит лемме 1). Удалим из графа ребро e. Любые две вершины x, y из H_u останутся связанными между собой маршрутом вида $x \to \ldots \to u \to \ldots \to y$. Для произвольных вершин z, t из H_v любые простые цепи, связывающие их с вершиной u в исходном графе, заканчивались ребром $e = vu$; значит, после удаления этого ребра z и t связаны маршрутом вида $z \to \ldots \to v \to \ldots \to t$. Таким образом, удаление e привело к образованию двух компонент связности (с множествами вершин H_u и H_v). Лемма доказана. ►

Теорема 2. *Пусть в простом графе n вершин, m ребер и k компонент связности. Тогда справедливы неравенства*

$$n - k \leqslant m \leqslant \frac{(n-k)(n-k+1)}{2}.$$

◄ Неравенство $n - k \leqslant m$ будем доказывать индукцией по числу ребер.

База индукции. При $m = 0$ имеем $n = k$ — неравенство выполняется.

Индукционный шаг. Предположим, что доказываемое неравенство справедливо для всех графов с s ребрами, где $s < m$. Будем в графе с n вершинами, m ребрами и k компонентами связности последовательно удалять ребра так, чтобы не изменялось число компонент связности, до тех пор, пока это возможно. В результате получим граф с прежним количеством вершин и компонент связности и $m' \leqslant m$ ребрами, причем каждое ребро будет мостом. Удалим еще одно ребро. В силу леммы 2 число компонент связности станет равным $k + 1$. Так как граф будет иметь $m' - 1 \leqslant m - 1 < m$ ребер, к нему применимо предположение

индукции: $n-(k+1) \leqslant m'-1$. Стало быть, $n-k \leqslant m'$, и так как $m' \leqslant m$, то $n-k \leqslant m$, что и требовалось доказать.

Для того чтобы оценить сверху число ребер графа через число его вершин и компонент связности, дополним каждую компоненту связности графа до полного графа. Граф после этого будет представлять собой дизъюнктное объединение полных графов $G_1 \cup \ldots \cup G_k$. Пусть в i-й компоненте n_i вершин $(i = 1, \ldots, k)$. Можно ли еще увеличить число ребер, не меняя при этом числа вершин и компонент связности? Можно, если найдутся две компоненты, в каждой из которых не менее двух вершин. Пусть $2 \leqslant n_i \leqslant n_j$. «Отберем» одну вершину у G_i (потеряв при этом $n_i - 1$ ребер) и «передадим» ее графу G_j (приобретя зато n_j ребер). Количество ребер увеличится на величину $n_j - (n_i - 1) = n_j - n_i + 1 \geqslant 1$. Повторяя описанную процедуру, пока это возможно, придем в конце концов к графу с $k-1$ изолированными вершинами и компонентой связности, представляющей собой полный граф с $n-k+1$ вершинами. Полученный граф имеет $\frac{(n-k+1)(n-k)}{2}$ ребер. Поскольку при каждом проведенном преобразовании число ребер возрастало, получим требуемое соотношение: $m \leqslant \frac{(n-k+1)(n-k)}{2}$; причем равенство достигается только для дизъюнктного объединения полного графа и пустых графов. ►

Следствие. *Если в простом графе n вершин и m ребер и $m > \frac{(n-1)(n-2)}{2}$, то граф связен.*

◄ Действительно, если бы граф не был связен и число его компонент $k \geqslant 2$, то число ребер удовлетворяло бы неравенству

$$m \leqslant \frac{(n-k)(n-k+1)}{2} \leqslant \frac{(n-1)(n-2)}{2},$$

что противоречит условию. ►

§ 3. Метрические характеристики графа

Пусть $G = \langle V, E \rangle$ — связный граф. Через $d(u, v)$ обозначим длину кратчайшей цепи, связывающей вершины u и v. Покажем, что $d(u, v)$ обладает свойствами *метрики*.

Симметричность.

$$\forall\, u, v \in V \quad d(u, v) = d(v, u).$$

Свойство очевидно.

Неравенство треугольника.

$$\forall\, u, v, w \in V \quad d(u, v) \leqslant d(u, w) + d(w, v).$$

Действительно, объединив кратчайшие цепи из u в w и из w в v, получим маршрут из u в v длиной $d(u, w) + d(w, v)$, длина кратчайшей цепи из u в v будет не более этой величины.

Невырожденность.

$$\forall u, v \in V \quad d(u, v) \geqslant 0; \quad d(u, v) = 0 \iff u = v.$$

Непосредственно вытекает из определения $d(u, v)$.

Таким образом, на множестве вершин связного графа введена структура *метрического пространства*. $d(u, v)$ будем называть *расстоянием* между вершинами u и v.

Эксцентриситетом вершины u называется наибольшее из расстояний от u до других вершин графа:

$$e(u) = \max_{v \in V} d(u, v).$$

Минимальный эксцентриситет вершин графа называют *радиусом графа*:

$$r(G) = \min_{u \in V} e(u),$$

а максимальный эксцентриситет — *диаметром*:

$$d(G) = \max_{u \in V} e(u).$$

Другими словами, диаметр графа — это наибольшее из расстояний между двумя вершинами графа. Если эксцентриситет вершины совпадает с радиусом графа, то вершину называют *центральной*. Центральные вершины графа составляют его *центр*. Вершина называется *периферийной*, если ее эксцентриситет равен диаметру графа.

Несколько примеров. В полном графе K_n $(n > 1)$ расстояние между любыми двумя (разными) вершинами равно 1, поэтому $r(K_n) = d(K_n) = 1$. В полном графе каждая вершина является и периферийной, и центральной.

Последнее свойство имеет место и для циклического графа C_n, для которого радиус также совпадает с диаметром:

$$r(C_n) = d(C_n) = \left[\frac{n}{2}\right]$$

($[\cdot]$ — обозначение целой части).

Для колеса W_n радиус равен единице, а диаметр — двум, одна вершина является центральной, а остальные — периферийные.

Установим соотношения между радиусом и диаметром графа.

Теорема 3. *Для произвольного графа G справедливы неравенства*:

$$r(G) \leqslant d(G) \leqslant 2r(G).$$

◄ Первое неравенство следует непосредственно из определений:

$$r(G) = \min_u e(u) \leqslant \max_u e(u) = d(G).$$

Чтобы доказать второе неравенство, положим:

$$d(u, v) = d(G); \quad e(w) = r(G).$$

Применяя неравенство треугольника, получим:

$$d(G) = d(u, v) \leqslant d(u, w) + d(w, v) \leqslant e(w) + e(w) = 2r(G).$$

Теорема доказана. ►

§ 4. Гамильтоновы графы

У. Гамильтон — ирландский математик и астроном — в 1859 году придумал головоломку «Кругосветное путешествие», состоявшую в следующем: каждой вершине додекаэдра приписано имя известного города; необходимо по ребрам проложить замкнутый путь, который проходил бы через все города, причем каждый город должен встретиться ровно один раз. В честь Гамильтона графы, в которых существуют маршруты с подобным свойством, были названы гамильтоновыми.

Перейдем к точным определениям. Граф G — *гамильтонов*, если в нем существует простая замкнутая цепь, проходящая через все вершины графа; указанную цепь называют при этом *гамильтоновым циклом*. Если в приведенных определениях отказаться от требования *замкнутости*, то придем к понятиям *полугамильтонова графа* и *гамильтоновой цепи*.

На рис. 14 граф G_1 не является гамильтоновым (и даже полугамильтоновым), G_2 — полугамильтонов граф, G_3 — гамильтонов.

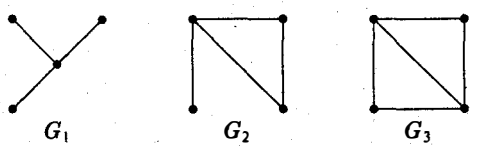


Рис. 14

Приведем примеры задач, сводящихся к нахождению гамильтоновых циклов в графе.

1) *На обед за круглым столом приглашены гости. Требуется рассадить их так, чтобы сидящие рядом были в дружеских отношениях.*
Рассмотрим граф, в котором вершины — гости, а наличие ребра, соединяющего вершины u и v, говорит о «дружбе» между u и v. Гостей следует рассадить за круглым столом в таком порядке, чтобы соответствующие им вершины были последовательными вершинами некоторого гамильтонова цикла.

2) **Задача Эйлера о коне.** *Обойти ходом коня шахматную доску, посетив при этом каждую клетку ровно один раз и последним* (64-*м*) *ходом вернуться в начальную клетку.*
Здесь граф содержит 64 вершины (клетки доски). Две вершины соединяются ребром, если возможен ход коня с одной клетки в другую. Степени вершин варьируются от 2 до 8. Эта задача достаточно широко описана в занимательной математической литературе. Есть что-то притягательное в задаче Эйлера о коне, если даже на студенческих партах можно встретить наряду с традиционными жанрами «наскального изобразительного искусства» изображения шахматной доски, клетки которой пронумерованы в соответствие с маршрутом коня!

3) **Задача коммивояжера.** *Бродячий торговец*[7] (*коммивояжер*) *должен посетить n пунктов. Известна стоимость проезда между любыми двумя пунктами. Требуется выбрать наиболее «дешевый» замкнутый путь, проходящий через все пункты.*

[7] В англоязычной литературе для задачи коммивояжера используется термин Traveling salesman problem (TSP).

Вместо стоимости проезда можно говорить, конечно, о времени или расстоянии. В любом случае, каждому ребру графа приписан некоторый «вес»; задача состоит в нахождении гамильтонова цикла минимального веса (*вес цикла* — сумма весов составляющих его ребер). Задача коммивояжера является классической задачей дискретной оптимизации, относится к классу так называемых NP-полных задач.

Обозначим через $P(n)$ множество всех простых помеченных графов с n вершинами, а через $P_h(n)$ — множество всех простых помеченных гамильтоновых графов с n вершинами. В 1969 г. советский математик В. А. Перепелица доказал, что

$$\lim_{n\to\infty} \frac{|P_h(n)|}{|P(n)|} = 1.$$

Таким образом, вероятность того, что «случайный» граф с n вершинами является гамильтоновым, стремится к единице с ростом n. Не установлено простых критериев гамильтоновости графа. Приведем одно из достаточных условий гамильтоновости.

Теорема 4 (О. Оре, 1960 г.). *Если в простом графе с n вершинами ($n \geqslant 3$) для любой пары несмежных вершин u и v выполняется неравенство*

$$\rho(u) + \rho(v) \geqslant n,$$

то граф является гамильтоновым.

Предварительно докажем следующее утверждение.

Лемма. *Пусть G — простой негамильтонов граф, содержащий $n \geqslant 3$ вершин, в котором несмежные вершины u и v соединяет гамильтонова цепь. Тогда*

$$\rho(u) + \rho(v) \leqslant n - 1.$$

◀ Доказательство леммы. В гамильтоновой цепи $u \to \ldots \to v$, где вершины u и v не смежны, произвольная вершина, смежная с u (обозначим ее u'), не может следовать за вершиной (например, v'), смежной с v. Действительно, гамильтонова цепь $u \to \ldots \to v' \to u' \to \ldots \to v$ легко преобразуется в гамильтонов цикл $u \to \ldots \to v' \to v \to \ldots \to u' \to u$. Поэтому число вершин, не смежных с u, не меньше числа вершин, смежных с v, то есть $n - 1 - \rho(u) \geqslant \rho(v)$, или $\rho(u) + \rho(v) \leqslant n - 1$. ▶

◀ Доказательство теоремы 4. Предположив, что граф не является гамильтоновым, будем последовательно добавлять к нему ребра до тех пор, пока он не станет гамильтоновым. Удалив последнее добавленное ребро uv, получим полугамильтонов граф G', не являющийся гамильтоновым. В нем существует гамильтонова цепь $u \to \ldots \to v$, причем вершины u и v не смежны. Применение леммы дает: $\rho'(u) + \rho'(v) \leqslant n - 1$, где $\rho'(u)$, $\rho'(v)$ — степени вершин u и v в графе G'. Осталось заметить, что $\rho'(u) \geqslant \rho(u)$, $\rho'(v) \geqslant \rho(v)$, откуда $\rho(u) + \rho(v) \leqslant \rho'(u) + \rho'(v) \leqslant n - 1 < n$. Получено противоречие с условием. ▶

Следствие (Г. Дирак, 1952 г.). *Если в простом графе порядка $n \geqslant 3$ степень каждой вершины не меньше $n/2$, то граф является гамильтоновым.*

§ 5. Эйлеровы графы

Связный граф называется *эйлеровым*, если в нем существует замкнутая цепь, содержащая все ребра графа; указанную цепь называют при этом *эйлеровым циклом*. Если в приведенных определениях снять требование *замкнутости*, то придем к понятиям *полуэйлерова графа* и *эйлеровой цепи*.

На рис. 15 граф G_1 не является эйлеровым (и даже полуэйлеровым), G_2 — полуэйлеров граф, G_3 — эйлеров.

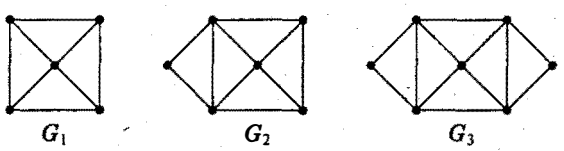


Рис. 15

Узнать, является ли граф эйлеровым, очень просто ввиду следующей теоремы.

Теорема 5 (Л. Эйлер, 1736 г.). *Связный граф является эйлеровым тогда и только тогда, когда каждая его вершина имеет четную степень.*

◄ *Необходимость.* Начнем движение по эйлерову циклу с «середины» произвольного ребра и будем подсчитывать (по ходу движения) степени вершин. При прохождении через вершину ее (текущая) степень увеличивается на 2. Поэтому степени всех вершин эйлерова графа четны.

Достаточность. Сначала докажем утверждение, которое пригодится нам и в дальнейшем.

Лемма. *Пусть все вершины графа имеют четную степень. Тогда через каждую неизолированную вершину графа проходит некоторый цикл.*

◄ Доказательство леммы. Будем строить цикл, исходя из произвольной неизолированной вершины v. Если в графе имеется петля vv, то требуемый цикл уже есть. Пусть теперь vv_1 — произвольное ребро (не являющееся петлей), инцидентное вершине v. Поскольку степень v_1 не меньше двух, существует ребро v_1v_2, отличное от vv_1. Если $v_2 \neq v$, то маршрут $v \to v_1 \to v_2$ можно нарастить некоторым ребром v_2v_3. Из-за четности степени каждой вершины маршрут можно удлинять всякий раз, если попадаем в вершину, отличную от v. В силу конечности множества ребер через конечное число шагов описанной процедуры возникнет замкнутая цепь $v \to v_1 \to \ldots \to v$. ►

Продолжение доказательства теоремы. Поскольку в данном графе циклы есть, и количество их конечно, существует самый длинный из них. Пусть $C : v \to v_1 \to \ldots \to v$ — цикл наибольшей длины. Нужно доказать, что он содержит все ребра графа. Пусть это не так. Тогда после удаления ребер, составляющих цикл C, возникнет непустой граф G', в котором степени всех вершин по-прежнему четны. Если при этом вершины, через которые проходил цикл C, станут изолированными, то исходный граф не связен, что противоречит условию. Значит, в G' найдется неизолированная вершина w. Согласно лемме, через нее проходит некоторый цикл C', составленный из ребер графа G'. Объединив циклы C и C' (а это возможно, поскольку у них есть общая вершина и нет общих ребер), получим цикл длиннее C — противоречие. ►

Следствие. *Связный граф является полуэйлеровым тогда и только тогда, когда в нем не более двух вершин имеют нечетную степень.*

◄ *Необходимость* доказывается так же, как в теореме.

Достаточность. Если вершин нечетной степени нет, то граф является эйлеровым, а, значит, и полуэйлеровым. По следствию из леммы о рукопожатиях ровно одной вершины нечетной степени не может быть. Пусть теперь в графе ровно две вершины имеют нечетную степень. Соединив эти две вершины новым ребром, получим, согласно теореме, эйлеров граф. Построим в новом графе эйлеров цикл; удаление ранее добавленного ребра приводит к эйлеровой цепи в исходном графе. ►

Задача о кенигсбергских мостах

Во времена Леонарда Эйлера семь мостов города Кёнигсберга (ныне Калининград) были расположены на реке Прегель так, как показано на рис. 16. Мог ли житель этого города, выйдя из дома, вернуться обратно, пройдя по каждому мосту ровно один раз? Рассмотрим граф, вершины которого отвечают связным участкам суши (двум берегам реки и двум островам), а ребра — мостам. Все четыре вершины графа имеют нечетную степень, стало быть, ответ к задаче отрицательный.

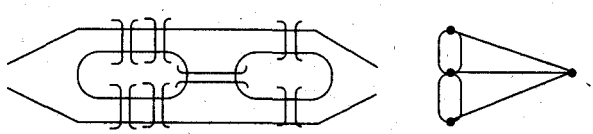


Рис. 16

Приведенное выше доказательство теоремы об эйлеровых графах имеет неконструктивный характер — оно не дает эффективного метода нахождения эйлерова цикла (генерирование всевозможных циклов — явно не лучший способ действий). Приведем один из алгоритмов нахождения эйлерова цикла.

Алгоритм Флери построения эйлерова цикла

1. Начать цикл с произвольной вершины u. Присвоить произвольному ребру uv, инцидентному u, номер 1. Удалить из графа ребро uv, перейти в вершину v.

2. Пусть после k шагов мы находимся в вершине w. Выбрать произвольное ребро wt, причем мост выбирается только в том случае, если нет другой возможности. Ребру wt присвоить номер $k+1$. Удалить из графа ребро wt, перейти в вершину t.

Число шагов в описанном алгоритме совпадает с числом ребер в графе. По окончании работы алгоритма ребра исходного графа будут пронумерованы в порядке их следования в эйлеровом цикле. Докажем *корректность* предложенного алгоритма.

Теорема 6. *Применение алгоритма Флери к произвольному эйлерову графу всегда приводит к построению эйлерова цикла.*

◀ Пусть G — эйлеров граф. Тогда степень каждой его вершины четна. В силу этого алгоритм может закончить свою работу лишь в начальной вершине u, построив при этом некоторый цикл C. Нужно доказать, что цикл C включает в себя все ребра графа G. Если это не так, то после удаления ребер C граф распадается на компоненты связности, хотя бы одна из которых (назовем ее B) содержит ребра. Обозначим через A семейство всех ребер цикла C, инцидентных вершинам B. Пусть a — наибольший номер ребра (полученный в результате работы алгоритма Флери) из A, тогда к моменту удаления данного ребра из графа оно было мостом; однако это противоречит правилу выбора очередного ребра: поскольку в компоненте B степень каждой вершины четна (это легко видеть), то в ней существует цикл, идя по которому (напомним, любое ребро цикла — не мост) можно было избежать преждевременного удаления моста. Корректность алгоритма Флери доказана. ▶

В заключение параграфа отметим, что для *случайным образом* построенного графа вероятность его эйлеровости (при большом числе вершин) мала.

Теорема 7 (Р. Рейд, 1962 г.). *Пусть $P(n)$ — множество всех простых помеченных графов с n вершинами, $P_e(n)$ — множество всех простых помеченных эйлеровых графов с n вершинами. Тогда*

$$\lim_{n\to\infty} \frac{|P_e(n)|}{|P(n)|} = 0.$$

◀ Пусть $P_0(n)$ — множество всех простых помеченных графов с n вершинами, степень каждой из которых четна. Связные графы из $P_0(n)$ составляют, как известно, $P_e(n)$; поэтому $P_e(n) \subset P_0(n)$ и $|P_e(n)| \leqslant |P_0(n)|$. Каждый граф из $P(n)$ определяется некоторым подмножеством ребер полного графа K_n, содержащего C_n^2 ребер; в силу этого $|P(n)| = 2^{C_n^2}$. Нетрудно подсчитать и мощность $P_0(n)$. Установим взаимно однозначное соответствие между $P(n-1)$ и $P_0(n)$: если все вершины нечетной степени произвольного графа из $P(n-1)$ (число их по следствию из леммы о рукопожатиях четно) соединить с n-й вершиной, то получим граф из $P_0(n)$. Таким образом,

$$|P_0(n)| = |P(n-1)| = 2^{C_{n-1}^2}.$$

Дальнейшее просто:

$$\frac{|P_e(n)|}{|P(n)|} \leqslant \frac{|P_0(n)|}{|P(n)|} = \frac{2^{C_{n-1}^2}}{2^{C_n^2}} = 2^{\frac{(n-1)(n-2)-n(n-1)}{2}} = 2^{1-n}.$$

Так как $2^{1-n} \to 0$ при $n \to \infty$, то и $\lim\limits_{n\to\infty} \frac{|P_e(n)|}{|P(n)|} = 0$. ►

§ 6. Деревья и леса

Граф, не содержащий циклов, называют *ациклическим* графом, или *лесом*. Заметим, что в ациклическом графе отсутствуют петли и кратные ребра, в силу чего он является простым графом. *Дерево* — это связный ациклический граф. Таким образом, компоненты связности леса являются деревьями, т. е. лес — дизъюнктное объединение деревьев.

В следующей серии теорем вскрываются важные свойства ациклических графов; при их доказательстве часто будут использоваться леммы из § 2.

Теорема 8. *Граф является лесом тогда и только тогда, когда каждое ребро графа — мост.*

◄ Граф G — лес $\iff$ в G нет циклов $\iff$ ни одно ребро не входит ни в какой цикл $\iff$ (по лемме 1) все ребра G — мосты. ►

Теорема 9. *Дерево с n вершинами содержит $n-1$ ребро.*

◄ Пусть G — дерево с n вершинами. В силу предыдущей теоремы каждое ребро G (и всех его подграфов) является мостом. Будем последовательно удалять ребра G, при этом каждый раз число компонент связности увеличивается на 1 (по лемме 2). Первоначально имелась одна компонента связности (так как дерево — связный граф). После удаления всех ребер граф будет иметь n изолированных вершин, т. е. n компонент связности. Таким образом, в указанной процедуре был выполнен $n-1$ шаг; значит G содержит $n-1$ ребро. ►

Следствие 1. *Пусть в лесе n вершин, m ребер и k компонент связности. Тогда $m = n - k$.*

◄ Пусть в i-й компоненте связности леса n_i вершин и m_i ребер ($i = 1, \ldots, k$); по теореме 9 для каждого i справедливо $m_i = n_i - 1$. Подсчитаем общее число ребер леса:

$$m = \sum_{i=1}^{k} m_i = \sum_{i=1}^{k} (n_i - 1) = \sum_{i=1}^{k} n_i - k = n - k. \ ►$$

Следствие 2. *Если в лесе число ребер на* 1 *меньше числа вершин, то этот лес является деревом.*

◄ Действительно, в силу следствия 1 число компонент связности леса равно разности числа вершин и числа ребер (в нашем случае — единице). ►

Объединив формулировки теоремы 9 и следствия 2, получим следующее утверждение: *лес является деревом тогда и только тогда, когда число его ребер на* 1 *меньше числа вершин.*

Следствие 3. *В дереве, которое содержит по меньшей мере две вершины, не менее двух висячих вершин.*

◄ Пусть в дереве $n \geqslant 2$ вершин: $v_1, \ldots v_n$, тогда оно содержит $m = n - 1$ ребро. По лемме о рукопожатиях

$$\rho(v_1) + \ldots + \rho(v_n) = 2m = 2(n-1).$$

Можно считать, что вершины упорядочены по их степеням:

$$\rho(v_1) \leqslant \rho(v_2) \leqslant \ldots \leqslant \rho(v_n).$$

Докажем, что $\rho(v_1) = \rho(v_2) = 1$. Предполагая противное, легко получить противоречие: если $\rho(v_2) > 1$, т. е. $\rho(v_2) \geqslant 2$, то

$$2(n-1) = \rho(v_1) + \rho(v_2) + \ldots + \rho(v_n) \geqslant 1 + (n-1)\rho(v_2) \geqslant 1 + 2(n-1). \ \blacktriangleright$$

Из следствия 3 вытекает

Следствие 4. *В лесе, содержащем хотя бы одно ребро, не менее двух висячих вершин.*

Теорема 9 может быть обращена следующим образом.

Теорема 10. *Пусть в связном графе число ребер на* 1 *меньше числа вершин. Тогда этот граф — дерево.*

◄ Пусть в графе G n вершин, $m = n - 1$ ребер. По теореме 2 в простом графе $m \geqslant n - k$, где k — число компонент связности. Для рассматриваемого графа $k = 1$ и имеет место равенство $m = n - k$. Отсюда ясно, что граф является простым, так как в противном случае удалив все петли и (лишние) кратные ребра (сделав граф простым), мы уменьшили бы m, не меняя при этом n и k, что привело бы к нарушению упомянутого неравенства. Итак, граф G — простой и для него $m = n - k$. Удаление любого ребра графа приведет к нарушению неравенства $m \geqslant n - k$, если при этом не изменится число компонент связности k; поэтому удаление произвольного ребра изменяет k, то есть каждое ребро графа есть мост, в силу чего (по теореме 8) G — ациклический граф. Так как при этом G по условию связный граф, G — дерево. Теорема доказана. ►

Теорема 11. *Граф является деревом тогда и только тогда, когда любые две его вершины соединены ровно одной простой цепью.*

◄ *Необходимость.* Пусть G — дерево. Тогда G — связный граф, и любые две его вершины соединены простой цепью (§ 2), при этом двух различных цепей с таким свойством не может быть, так как их объединение дает цикл, в то время как в дереве циклов нет.

Достаточность. Если в графе любые две вершины соединены цепью, то, как известно, граф является связным. Ацикличность графа также очевидна: если бы в графе был цикл, то любые две вершины этого цикла соединены по меньшей мере двумя простыми цепями. ►

Теорема 12. *Лес является деревом в том и только в том случае, когда добавление любого ребра приводит к образованию ровно одного цикла.*

◄ Пусть ациклический граф связен. В силу теоремы 11 любые две вершины u и v соединены ровно одной простой цепью. Поэтому добавление ребра uv приводит к образованию цикла, причем ровно одного, так как если бы их образовалось хотя бы два, то объединяя соответствующие «участки» этих циклов, можно было бы построить цикл, не содержащий ребра uv, что противоречило бы ацикличности исходного графа.

Обратно. Если при добавлении ребра uv образуется цикл, то удаляя из этого цикла ребро uv, мы получим цепь, связывающую вершины u и v, значит, любые две вершины графа связаны, т. е. граф связен и является деревом (так как по условию он ациклический). ►

§ 7. Теорема Кэли о числе помеченных деревьев

Обозначим через P_n число помеченных деревьев с n вершинами. Ясно, что $P_1 = P_2 = 1$. Помеченное дерево с тремя вершинами полностью определяется своей центральной вершиной, поэтому $P_3 = 3$. Если в дереве 4 вершины, то оно представляет собой либо полный двудольный граф $K_{1,3}$, либо простую (незамкнутую) цепь длины 4. Первого типа имеется 4 различных помеченных дерева, а второго — 12 ($C_4^2 \cdot 2$); крайние вершины цепи выбираются C_4^2 способами, после чего для нумерации двух оставшихся вершин остается две возможности; таким образом, $P_4 = 4 + 12 = 16$. Дерево с 5 вершинами имеет один из трех видов, представленных на рис. 17.

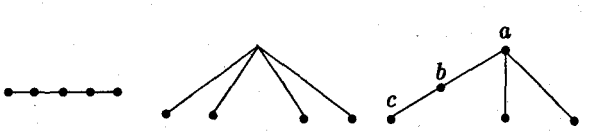


Рис. 17

Количество деревьев типа «цепь» равно $C_5^3 \cdot 3! = 60$, типа $K_{1,4}$ — 5. Произвольное дерево третьего типа определяется пометками вершин a, b, c (см. обозначения на рисунке); поэтому их число равно $A_5^3 = 60$. Итак, $P_5 = 60+5+60 = 125$. Последовательность 1, 1, 3, 16, 125 может быть задана соотношением $P_n = n^{n-2}$. Количество помеченных деревьев с 6 вершинами также нетрудно подсчитать «вручную» (читателю рекомендуется выполнить это полезное упражнение), после чего высказанная гипотеза получит новое подтверждение. И в общем случае имеет место

Теорема 13 (А. Кэли, 1897 г.). *Число помеченных деревьев с n вершинами равно n^{n-2}.*

Существует много способов доказательства этой знаменитой теоремы. Мы приведем не самое богатое в идейном плане, но, возможно, самое простое доказательство.

Покажем, что существует взаимно однозначное соответствие между множеством помеченных n-вершинных деревьев и множеством размещений с повторениями из n элементов по $n-2$; поскольку $\overline{A_n^{n-2}} = n^{n-2}$, это будет доказывать теорему. Сопоставление дереву упорядоченного набора (называемого *кодом Прюфера*) $(a_1, a_2, \ldots, a_{n-2})$ (где для каждого i $a_i \in \{1, 2, \ldots, n\}$) будем называть *кодированием дерева* (или *кодировкой*), а обратный процесс (получения по указанному набору дерева) — *декодированием* (или *декодировкой*).

Кодирование дерева выполняется с помощью следующего алгоритма.

1. Положить $i = 1$.
2. Пусть v_i — висячая вершина дерева с наименьшей меткой; тогда a_i — метка смежной с ней вершины.
3. Удалить из дерева вершину v_i и инцидентное ей ребро. Если в дереве осталось более двух вершин, увеличить i на 1 и перейти к п. 2, иначе — закончить.

Очевидно, что разные деревья имеют разные коды.

Декодирование дерева. Пусть $B_0 = \{1, 2, \ldots, n\}$, а b_1 — наименьшее число из B_0, не встречающееся в наборе $(a_1, \ldots, a_{n-2})$. Тогда b_1 — номер висячей вершины, смежной с a_1, и дерево содержит ребро (b_1, a_1).

Набор $(a_2, \ldots, a_{n-2})$ кодирует дерево T_1 с множеством пометок $B_1 = B_0 \setminus \{b_1\}$ (T_1 получается из T удалением вершины b_1 и инцидентного ей ребра (a_1, b_1)).

В качестве b_2 возьмем наименьшее число из B_1, не встречающееся в последовательности $(a_2, \ldots, a_{n-2})$. Дерево T_1 (значит, и T) должно содержать ребро (b_2, a_2). Теперь набор $(a_3, \ldots, a_{n-2})$ описывает дерево T_2 с множеством пометок $B_2 = B_1 \setminus \{b_2\}$. И так далее.

На k-м шаге процедуры рассматривается дерево T_{k-1} с множеством пометок B_{k-1}. В множестве B_{k-1} выбирается наименьшее число (b_k), не входящее в набор $(a_k, \ldots, a_{n-2})$, после чего констатируется наличие в дереве T ребра (b_k, a_k). После $n-2$ шагов будут выявлены $n-2$ ребра дерева T; при этом множество B_{n-2} будет содержать два числа — пометки вершин последнего, $(n-1)$-го, ребра, включаемого в дерево. (Дерево T_{n-2}, содержащее две вершины, строится однозначно, и поэтому не нуждается в кодировке.)

Осталось еще убедиться в том, что полученный после декодирования граф действительно является деревом. В самом деле, граф T_{k-1} получается из графа T_k добавлением ребра (b_k, a_k), причем вершина b_k не принадлежит графу T_k. Поэтому

Таблица 1

k	B_k	код T_k	(b_k, a_k)
0	{1, 2, 3, 4, 5, 6, 7, 8}	(2, 4, 1, 2, 4, 4)	
1	{1, 2, 4, 5, 6, 7, 8}	(4, 1, 2, 4, 4)	(3, 2)
2	{1, 2, 4, 6, 7, 8}	(1, 2, 4, 4)	(5, 4)
3	{1, 2, 4, 7, 8}	(2, 4, 4)	(6, 1)
4	{2, 4, 7, 8}	(4, 4)	(1, 2)
5	{4, 7, 8}	(4)	(2, 4)
6	{4, 8}		(7, 4)
7			(4, 8)

из ацикличности T_k следует ацикличность T_{k-1}. Поскольку T_{n-2} — дерево, то деревьями являются и графы $T_{n-3}, \ldots, T_2, T_1, T$.

Пример. Дерево, изображенное на рис. 18, имеет код (2, 4, 1, 2, 4, 4).

По коду (2, 4, 1, 2, 4, 4) восстановим дерево. Процесс декодировки отражен в табл. 1.

Как и следовало ожидать, получено дерево, закодированное выше.

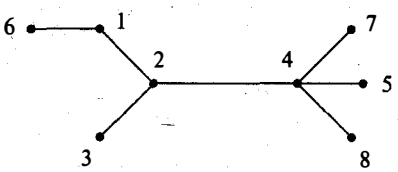


Рис. 18

§ 8. Стягивающие деревья

Стягивающим (или *остовным*) *деревом* связного графа G называется произвольный его подграф, содержащий все вершины G и являющийся деревом.

Остовным лесом графа G называется произвольный его подграф, содержащий все вершины G и являющийся лесом. Таким образом, компоненты связности остовного леса графа G являются стягивающими деревьями компонент G.

Построить остовный лес нетрудно: достаточно последовательно удалять из графа ребра, входящие в циклы, до тех пор, пока не будет построен ациклический граф (лес), который, очевидно, будет остовным для исходного графа.

Граф называется *взвешенным*, если каждому его ребру l поставлено в соответствие неотрицательное число $\mu(l)$ (*вес ребра*). *Весом графа* $G = \langle V, E \rangle$ называют сумму весов всех его ребер:

$$\mu(G) = \sum_{l \in E} \mu(l).$$

Рассмотрим следующую задачу. *Имеется n пунктов. Для любой пары пунктов i и j известна стоимость сооружения дороги между ними — c_{ij}. Требуется выбрать сеть дорог такую, чтобы любые два пункта соединялись каким-либо маршрутом и при этом стоимость ее сооружения была наименьшей.*

Если рассмотреть полный граф порядка n, вершины которого будут соответствовать указанным (географическим) пунктам, а ребра будут иметь вес, равный стоимости сооружения дороги между соответствующими пунктами, то на языке теории графов данная задача будет формулироваться так: *в данном графе найти стягивающее дерево наименьшего веса*. Отметим, что согласно теореме Кэли в полном графе K_n имеется n^{n-2} различных стягивающих деревьев, и, в принципе, рассматриваемая задача может быть решена перебором по всем таким деревьям. Ясно, однако, что с *практической* точки зрения подобный алгоритм решения не выдерживает никакой критики. Существуют эффективные алгоритмы нахождения стягивающего дерева минимального веса в связном взвешенном графе. При описании следующих алгоритмов $G = \langle V, E\rangle$ будет обозначать исходный граф, а $T = \langle V, P\rangle$ — искомое дерево.

Алгоритм Д. Краскала (1956 г.)

1. Положить $P = \varnothing$, $n = |E|$. Следующий шаг выполнять $n - 1$ раз.
2. Включить в T ребро графа G наименьшего веса, обладающее тем свойством, что при добавлении его в графе T не образуется циклов. Исключить из G данное ребро.

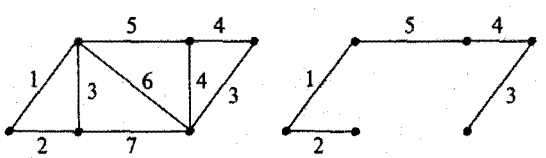


Рис. 19

На рис. 19 изображены взвешенный граф (числа показывают веса соответствующих ребер) и стягивающее дерево, полученное в результате работы алгоритма.

Обоснование корректности алгоритма Краскала

Заметим сначала, что в результате работы алгоритма строится стягивающее дерево исходного графа (граф T ациклический по построению и в нем число ребер на 1 меньше числа вершин, поэтому в силу следствия 2 из теоремы 9 он является деревом). Пусть $P = \{e_1, e_2, \ldots, e_{n-1}\}$ (будем считать, что ребра записаны «в порядке поступления»), а $S = \langle V, M\rangle$ — *произвольное* стягивающее дерево исходного графа. Нужно доказать, что $\mu(S) \geqslant \mu(T)$. Если $S \neq T$, то $P \neq M$ и существует такое k, что $e_1, e_2, \ldots, e_{k-1} \in M$, $e_k \notin M$. Добавим к дереву S ребро e_k, при этом образуется цикл, обозначим его C. В цикле C найдется ребро e, принадлежащее множеству M и не входящее в P. Удалив это ребро, получим граф $S' = \langle V, M'\rangle$, где $M' = M \cup \{e_k\}\backslash\{e\}$. Этот граф связен и в нем ребер на единицу меньше, чем вершин. По теореме 10 граф S' — дерево. Сравним веса деревьев S' и S: $\mu(S') = \mu(S) + \mu(e_k) - \mu(e)$. Так как в силу алгоритма Краскала $\mu(e_k) \leqslant \mu(e)$, имеем $\mu(S') \leqslant \mu(S)$. Итак, в дереве S' по сравнению с деревом S число ребер, общих с деревом T, на 1 больше, причем вес S' не больше веса S. Указанную процедуру будем повторять до тех пор, пока не получим дерево T. В результате будет построена последовательность деревьев $S, S', S'', \ldots, T$, в которой каждое

последующее дерево имеет вес, не больший, чем предыдущее:

$$\mu(S) \geqslant \mu(S') \geqslant \mu(S'') \geqslant \ldots \geqslant \mu(T),$$

откуда и следует требуемое: $\mu(S) \geqslant \mu(T)$.

Алгоритм Р. Прима (1957 г.)

Данный алгоритм похож на алгоритм Краскала; основное различие состоит в том, что в этом алгоритме строится «разрастающееся» дерево, более точно: последовательность деревьев

$$S_1 \subset S_2 \subset \ldots \subset S_n,$$

где дерево $S_i = \langle V_i, E_i \rangle$ содержит i вершин $(i = 1, \ldots, n)$.

1. Пусть $V_1 = \{x_1\}$, где $x_1 \in V$ — произвольная вершина G, $E_1 = \varnothing$. Следующий шаг выполнять для $i = 2, \ldots, n$.
2. Получить дерево S_i из дерева S_{i-1} добавлением ребра графа G наименьшего веса (среди тех ребер, при добавлении которых к S_{i-1} вновь образуется дерево). Исключить из G данное ребро.

Обоснование корректности алгоритма Прима такое же, как и алгоритма Краскала.

Сравним трудоемкость описанных алгоритмов для графа с n вершинами и m ребрами. В первом из них основные затраты времени падают на сортировку ребер по их весу; известно, что для выполнения сортировки m объектов требуется

```
/* n ⩾ 2 — число вершин графа; */
/* V = {x_1, ..., x_n} — множество вершин; */
/* V_r — множество вершин, еще не включенных в дерево; */
/* E_s — множество ребер строящегося дерева; */
V_r = V \ {x_1}; E_s = ∅;
/* Расстановка начальных пометок */
for(x_i ∈ V_r)
   if(x_i и x_1 смежны){a_i = x_1; b_i = μ(a_i x_i);};
   else {a_i = 0; b_i = ∞};
/* k — порядковый номер ребра, включаемого в дерево */
for(k = 1; k < n;)
{
   /* определение нового ребра */
   b_i* = min_{x_i ∈ V_r} b_i;
   E_s = E_s ∪ {a_i*, x_i*};
   V_r = V_r \ {x_i*};
   /* пересчет пометок */
   if(++k < n)
     for(x_i ∈ V_r)
        if(x_i смежно с x_i* и μ(x_i x_i*) < b_i){b_i = μ(x_i, x_i*); a_i = x_i*;}
}
```

Рис. 20. Алгоритм Прима нахождения стягивающего дерева наименьшего веса

Таблица 2

шаг	1	2	3	4	5
V_r	$\{x_2, \ldots, x_6\}$	$\{x_3, \ldots, x_6\}$	$\{x_4, x_5, x_6\}$	$\{x_4, x_5\}$	$\{x_4\}$
$[a_2, b_2]$	$[x_1, 4]$	—	—	—	—
$[a_3, b_3]$	$[x_1, 4]$	$[x_2, 3]$	—	—	—
$[a_4, b_4]$	$[0, \infty]$	$[0, \infty]$	$[x_3, 7]$	$[x_6, 3]$	$[x_5, 2]$
$[a_5, b_5]$	$[0, \infty]$	$[0, \infty]$	$[0, \infty]$	$[x_6, 1]$	—
$[a_6, b_6]$	$[x_1, 5]$	$[x_1, 5]$	$[x_1, 5]$	—	—
$\min b_i$	b_2	b_3	b_6	b_5	b_4
новое ребро	x_1x_2	x_2x_3	x_1x_6	x_6x_5	x_5x_4

порядка $m \log_2 m$ операций сравнения. Во втором алгоритме на i-м шаге среди $n-i$ вершин, еще не включенных в дерево, нужно выбрать ту, чье «подключение» к дереву обойдется наиболее «дешево» (ребро, соединяющее новую вершину с одной из «старых», должно быть наименьшего веса); для этого требуется порядка $n-i-1$ операций. Суммируя по i, получим оценку трудоемкости алгоритма Прима: $O(n^2/2)$ операций сравнения. Понятно, что для полных графов (где число ребер $m = \frac{n(n-1)}{2}$) алгоритм Прима менее трудоемок, чем алгоритм Краскала.

Опишем эффективную реализацию алгоритма Прима. На каждом шаге алгоритма каждой вершине x_i, еще не включенной в дерево, сопоставляется *пометка* — пара чисел $[a_i, b_i]$, где b_i — наименьший вес ребра, соединяющего x_i с какой-либо вершиной, уже включенной в дерево, a_i — номер соответствующей вершины. Таким образом, $b_i = \mu(x_i a_i)$. Шаг алгоритма состоит в выборе $b_{i^*} = \min(b_i)$ и добавлении к дереву ребра $a_{i^*}x_{i^*}$. На рис. 20 дан набросок программной реализации алгоритма (с использованием конструкций языка программирования Си).

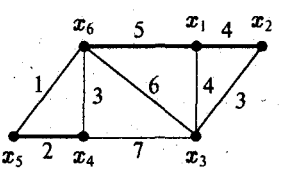


Рис. 21

Пример. Работа алгоритма для графа, изображенного на рис. 21, показана в табл. 2.

§9. Фундаментальная система циклов

Термин *фундаментальная система* (решений) используется для обозначения базиса в пространстве решений системы линейных однородных (алгебраических) уравнений, либо в пространстве решений однородного дифференциального уравнения. В каждом из этих случаев через элементы фундаментальной системы оказывается возможным выразить, и при том единственным образом, элементы некоторого бесконечного множества. В (конечном) графе число циклов конечно, но может быть достаточно велико (по сравнению с порядком графа). Например, в полном графе K_n можно указать $\frac{A_n^k}{2k} = \frac{n!}{2(n-k)!k}$ различных циклов[8] длины k $(k = 3, \ldots, n)$,

[8] В этом параграфе мы будем отождествлять цикл с множеством его ребер.

представляющих собой *простые* замкнутые цепи, а общее количество таких циклов имеет порядок $(n-1)!$. Поэтому задача выражения всех циклов графа через некоторые фиксированные циклы достаточно интересна; о практическом приложении решения такой задачи будет упомянуто в конце параграфа.

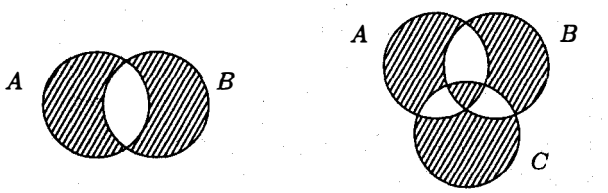
Поговорим сначала об операции, позволяющей по одним циклам получать другие.

9.1. Симметрическая разность множеств

Симметрической разностью множеств A и B называют множество

$$A \triangle B = (A \cup B) \setminus (A \cap B).$$

Операция нахождения симметрической разности коммутативна: $A \triangle B = B \triangle A$ (это очевидно) и ассоциативна: $(A \triangle B) \triangle C = A \triangle (B \triangle C)$ (попробуйте доказать это с помощью рис. 22). В силу ассоциативности при записи симметрической разности нескольких множеств скобки (указывающие порядок выполнения данной операции над множествами) можно не расставлять.



$A \triangle B$ $\qquad$ $(A \triangle B) \triangle C = A \triangle (B \triangle C)$

Рис. 22. Симметрическая разность двух и трех множеств

Пусть A — произвольное множество. Множество всех подмножеств A с операцией симметрической разности $\langle \beta(A), \triangle \rangle$ образует коммутативную группу; в роли нейтрального элемента группы выступает пустое множество, каждый элемент группы является обратным самому себе.

Лемма 3. *При произвольном натуральном* n *симметрическая разность* n *множеств*

$$\bigtriangleup_{i=1}^{n} A_i = A_1 \triangle A_2 \triangle \ldots \triangle A_n$$

состоит в точности из тех элементов данных множеств, которые принадлежат нечетному их числу.

◄ Доказательство проводится индукцией по числу множеств. База индукция очевидна.

Индукционный шаг. Пусть доказываемое утверждение справедливо для всех $n \leqslant k$. Симметрическая разность $k+1$ множеств имеет вид $B = B_1 \triangle B_2$, где $B_1 = A_1 \triangle \ldots \triangle A_p$, $B_2 = A_{p+1} \triangle \ldots \triangle A_{p+q}$, причем $p, q \leqslant k$, $p+q = k+1$. Множество B состоит из элементов, принадлежащих B_1 (значит, по индуктивному предположению, принадлежащих нечетному числу множеств из $A_1, \ldots, A_p$) и не принадлежащих B_2 (то есть входящих в четное число множеств из $A_{p+1}, \ldots, A_{p+q}$)

или, наоборот, не принадлежащих B_1 и принадлежащих B_2 (т. е. принадлежащих четному числу множеств из $A_1, \ldots, A_p$ и нечетному числу множеств из $A_{p+1}, \ldots, A_{p+q}$). В любом случае множество B составляют те и только те элементы, которые входят в нечетное число множеств из данных $k+1$ множеств: $A_1, \ldots, A_{k+1}$. Лемма доказана. ►

9.2. Псевдоциклы

Симметрическая разность двух циклов в графе в общем случае не является циклом. Множество ребер $C \subset E$ графа $G = \langle V, E\rangle$ назовем *псевдоциклом*, если в графе $\langle V, C\rangle$ каждая вершина имеет четную степень. (Обычный) цикл графа и пустое множество — примеры псевдоциклов. Оказывается, множество всех псевдоциклов графа замкнуто относительно симметрической разности.

Лемма 4. *Для любого натурального n симметрическая разность n псевдоциклов есть псевдоцикл.*

◄ Доказательство ведется индукцией по n. База индукции (утверждение для $n = 1$) очевидна. Обоснование индукционного шага сводится к рассмотрению случая двух псевдоциклов. Пусть C_1 и C_2 — псевдоциклы. Для произвольной вершины v графа обозначим через $S_i(v)$ множество ребер цикла C_i, инцидентных v ($i = 1, 2$). Степени вершины v в графах $\langle V, C_1\rangle$, $\langle V, C_2\rangle$, $\langle V, C_1 \triangle C_2\rangle$ равны мощностям множеств $S_1(v), S_2(v), S_1(v) \triangle S_2(v)$ соответственно. Из определения симметрической разности и с помощью формулы мощности объединения двух множеств получаем:

$$|S_1(v) \triangle S_2(v)| = |S_1(v) \cup S_2(v)| - |S_1(v) \cap S_2(v)| = |S_1(v)| + |S_2(v)| - 2|S_1(v) \cap S_2(v)|.$$

Из четности $|S_1(v)|$ и $|S_2(v)|$ вытекает четность $|S_1(v) \triangle S_2(v)|$. Лемма доказана. ►

Обсудив некоторые «технические» моменты, мы можем теперь заняться основным вопросом данного параграфа.

9.3. Фундаментальная система циклов

Пусть $G = \langle V, E\rangle$ — связный граф, $\langle V, T\rangle$ — его стягивающее дерево. Если граф G содержит n вершин, то в T — $n - 1$ ребер. Если к стягивающему дереву

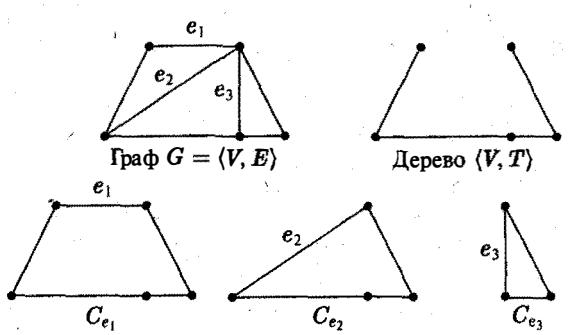


Рис. 23. Фундаментальная система циклов

добавить произвольное ребро $e \in E \setminus T$, то (по теореме 12) образуется ровно один цикл, обозначим его C_e. Множество всех циклов такого вида $\{C_e \mid e \in E \setminus T\}$ будем называть *фундаментальной системой циклов* графа $G = \langle V, E\rangle$ относительно стягивающего дерева $\langle V, T\rangle$. Пример см. на рис. 23.

Теорема 14. *Произвольный цикл C связного графа $G = \langle V, E\rangle$ представим в виде симметрической разности некоторых циклов из фундаментальной системы циклов G относительно любого стягивающего дерева $\langle V, T\rangle$. Такое представление единственно и имеет вид:*

$$C = \bigtriangleup_{e \in C \setminus T} C_e. \qquad (1)$$

Мы докажем даже более сильное утверждение, считая C псевдоциклом.

◀ Пусть $G = \langle V, E\rangle$ — связный граф, $\langle V, T\rangle$ — некоторое фиксированное стягивающее дерево G. Ребра этого дерева будем называть *ветвями*, а остальные ребра графа G — *хордами*. Заметим, что каждый цикл C_e содержит *ровно одну* хорду, а именно — e. Поэтому в симметрической разности (различных) фундаментальных циклов, равной C, должны присутствовать все циклы, отвечающие хордам из $C \setminus T$, и только они. Таким образом, если представление псевдоцикла C в виде симметрической разности фундаментальных циклов *существует*, то оно единственно и имеет вид (1). Докажем теперь, что равенство (1) действительно имеет место. Пусть

$$B = \bigtriangleup_{e \in C \setminus T} C_e.$$

По лемме 4 B — псевдоцикл; как уже показано, из хорд B содержит только хорды, принадлежащие C. Применяя леммы 3 и 4, получаем, что симметрическая разность $B \bigtriangleup C$ — псевдоцикл, не содержащий хорд (так как каждая хорда одновременно либо принадлежит, либо не принадлежит B и C, т. е. число ее вхождений в данные два множества четно); стало быть, $B \bigtriangleup C \subset T$. Осталось доказать, что в $B \bigtriangleup C$ нет и ветвей. Действительно, если подграф дерева не пуст, то согласно следствию 4 теоремы 9 он имеет не менее двух висячих вершин, в то же время — по определению псевдоцикла — он не содержит висячих вершин. Итак, мы выяснили: $B \bigtriangleup C = \varnothing$, что равносильно совпадению множеств $B = \bigtriangleup_{e \in C \setminus T} C_e$ и C. Теорема доказана. ▶

На множестве всех псевдоциклов связного графа можно ввести структуру *линейного пространства* над полем $GF(2)$, где в роли «сложения» выступает симметрическая разность, а умножение на скаляр определяется естественным образом — для произвольного псевдоцикла C имеем: $C \cdot 1 = C$, $C \cdot 0 = \varnothing$ (здесь через 0 и 1 обозначены элементы поля $GF(2)$; напомним, что в этом поле $0 + 0 = 1 + 1 = 0$, $1 + 0 = 1$, $0 \cdot 1 = 0 \cdot 0 = 0$, $1 \cdot 1 = 1$). Как показано выше, базисом в данном линейном пространстве будет фундаментальная система циклов относительно любого стягивающего дерева.

Выделение фундаментальной системы циклов находит применение при анализе электрических цепей. Если электрической цепи сопоставить граф, ребра которого соответствуют источникам ЭДС, сопротивлениям, индуктивностям и т. д., а вершины — узлам соединений элементов цепи, то при использовании закона

Кирхгофа для напряжений, гласящего: *сумма падения напряжений вдоль цикла равна нулю*, необходимо найти фундаментальную систему циклов. Уравнения, отвечающие этим циклам, не будут зависеть друг от друга, в то же время их выполнение будет гарантировать выполнение уравнений для всех циклов графа.

§ 10. Укладки графов

Один и тот же граф можно изобразить по-разному. На рис. 24 представлены два варианта изображения полного графа K_4. В первом случае отрезки, соответствующие ребрам графа, пересекаются, а во втором случае — нет. При решении ряда задач эта разница является принципиальной. Например, при изготовлении микросхем печатным способом электрические цепи наносятся на плоскую поверхность изоляционного материала; при этом проводники не должны пересекаться. Менее глобальный пример — **задача о трех домиках и трех колодцах.** *Хозяева трех соседних домиков хотят проложить дорожки к трем колодцам (от каждого домика к каждому колодцу) так, чтобы дорожки не пересекались. Удастся ли им осуществить свое намерение?*

Рис. 24

Перейдем к определениям. *Жордановой кривой* называют непрерывную кривую без самопересечений. *Плоским графом* назовем граф, вершины которого — точки плоскости, а ребра — жордановые кривые (лежащие в той же плоскости), соединяющие соответствующие вершины так, что никакие два ребра не имеют общих точек, за исключением инцидентной им обоим вершины. Граф будем называть *планарным*, если он изоморфен некоторому плоскому графу. Примеры планарных графов: K_4, C_n, W_n (для любого n). Задачу о домиках и колодцах теперь можно сформулировать так: *планарен ли граф* $K_{3,3}$? Отметим очевидные **свойства планарных графов:**

1. Любой подграф планарного графа является планарным.
2. Граф является планарным тогда и только тогда, когда тем же свойством обладает каждая его компонента связности.

Про планарный граф говорят также, что он *имеет плоскую укладку*, или *укладывается в плоскость*. Более общее определение: граф *укладывается в множество* L, если его вершины можно изобразить точками из множества L, а ребра — жордановыми кривыми, лежащими в L и имеющими общими только точки, изображающие соответствующие вершины графа. В последующих рассуждениях мы часто будем отождествлять граф и его укладку — «изображение» графа в каком-либо множестве.

Теорема 15. *Любой граф укладывается в* $\mathbb{R}^3$.

◄ Вершины графа будем изображать точками некоторой прямой l. Рассмотрим пучок плоскостей, проходящих через данную прямую. Каждому ребру графа сопоставим некоторую плоскость данного пучка так, чтобы разным ребрам соответствовали разные плоскости. Ребра будем изображать кривыми с концами

в соответствующих вершинах и лежащими в соответствующих плоскостях, при этом для изображения петель будем брать окружности, касающиеся l, а для остальных ребер — полуокружности. Ясно, что данная конструкция дает требуемую укладку графа. ►

Теорема 16. *Граф является планарным тогда и только тогда, когда он укладывается на сфере.*

◄ *Необходимость.* Имея укладку графа на сфере, выберем на сфере точку N так, чтобы она не совпадала ни с одной из вершин и не лежала ни на одном из ребер. Через противоположную точку сферы проведем к ней касательную плоскость α и осуществим *стереографическую проекцию* сферы на данную плоскость с центром в точке N: каждая точка T сферы проецируется в точку пересечения луча NT с плоскостью α. При данном отображении жорданова кривая на сфере переходит в жорданову кривую на плоскости. Стереографическая проекция устанавливает взаимно однозначное соответствие между сферой с выколотой точкой N и плоскостью; поэтому граф, полученный при проектировании, — плоский (его ребра имеют общие точки только в соответствующих вершинах) и изоморфен исходному графу, который, таким образом, является планарным.

Достаточность доказывается обратным ходом рассуждений. ►

§ 11. Формула Эйлера

Связным множеством (на плоскости) называется такое множество, любые две точки которого можно соединить жордановой кривой, целиком лежащей в данном множестве. Примеры связных множеств: многоугольник, круг, кольцо. Пример *несвязного* (т. е. не являющегося связным) множества: объединение двух непересекающихся кругов. *Грань* плоского графа — связная часть плоскости, ограниченная ребрами графа и не содержащая внутри себя других ребер. Среди всех граней графа ровно одна является неограниченной, ее называют внешней. Граф, изображенный на рис. 25 *а*, имеет три грани, внешняя грань помечена цифрой 3. У плоского ациклического графа только одна грань — внешняя. Заметим, что *планарный граф можно так изобразить на плоскости, что внешней будет любая его наперед заданная грань.* Вот как это можно сделать. От произвольной плоской укладки данного графа следует перейти к сферической (проектируя плоскость вместе с плоским графом на какую-либо сферу, касающуюся плоскости); далее осуществить стереографическую проекцию с центром во внутренней точке выбранной грани, при этом данная грань перейдет во внешнюю грань полученного плоского графа. На рис. 25 приведено три варианта плоской укладки одного и того же графа.

Теорема 17 (Л. Эйлер, 1758 г.). *Для любого связного плоского графа справедливо соотношение*

$$n - m + f = 2, \tag{1}$$

где n, m, f — число вершин, ребер, граней соответственно.

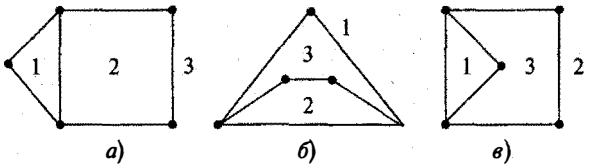


Рис. 25. Грани плоского графа

◄ Пусть $G = \langle V, E\rangle$ — произвольный связный плоский граф с n вершинами, m ребрами и f гранями. Рассмотрим его стягивающее дерево $T = \langle V, M\rangle$. Оно имеет n вершин, $n-1$ ребер и одну грань — равенство (1) для T выполняется. Будем последовательно добавлять к графу T «недостающие» ребра графа G (то есть ребра из множества $E \setminus M$). При добавлении одного ребра число граней также увеличивается на единицу, так как новое ребро делит грань, на границе которой лежат его вершины, на две грани; таким образом, после каждого шага предложенной процедуры соотношение (1) для графа T остается верным. После добавления $m-n+1$ ребер граф T перейдет в граф G, для которого равенство (1), таким образом, также справедливо. ►

Следствие 1 (формула Эйлера для выпуклых многогранников). *Пусть в выпуклом многограннике n вершин, m ребер и f граней. Тогда $n - m + f = 2$.*

◄ Поместим выпуклый многогранник внутрь некоторой сферы S и спроектируем многогранник на S из какой-либо его внутренней точки. Проекции вершин и ребер многогранника будут вершинами и ребрами некоторого графа, уложенного на сфере. Как показывает теорема 16, такой граф является планарным; для его плоской укладки выполняется требуемое соотношение между числом вершин, ребер и граней. Осталось заметить, что композиция двух преобразований (проектирование многогранника на сферу плюс переход от сферической укладки к плоской) задает взаимно однозначное соответствие между вершинами, ребрами, гранями многогранника и вершинами, ребрами, гранями связного плоского графа. ►

Следствие 2. *Число граней f плоского графа определяется формулой $f = m+k-n+1$, где m, n обозначают то же, что и выше, а k — число компонент связности графа.*

◄ Число граней i-й компоненты связности плоского графа выражается формулой $f_i = m_i - n_i + 2$ (m_i, n_i — число граней и ребер i-й компоненты; $i = 1, \ldots, k$). При суммировании f_i по i от 1 до k внешняя грань графа будет учитываться k раз, поэтому

$$f = \sum_{i=1}^{k} f_i - k + 1 = \sum_{i=1}^{k} (m_i - n_i + 2) - k + 1 =$$
$$= m - n + 2k - k + 1 = m - n + k + 1,$$

что и требовалось доказать. ►

Следствие 3. *Для любого простого связного планарного графа с $n \geqslant 3$ вершинами и m ребрами выполняется неравенство $m \leqslant 3n - 6$.*

◀ Рассмотрим какую-нибудь плоскую укладку рассматриваемого графа. Если в графе всего два ребра, то выполнение неравенства проверяется непосредственно; поэтому будем считать, что $m \geqslant 3$. Пусть у (плоского) графа f граней, а i-я грань ограничена m_i ребрами ($i = 1, \ldots, f$). Поскольку в рассматриваемом графе нет петель и кратных ребер, а ребер не меньше 3, то $\forall\, i \quad m_i \geqslant 3$ и

$$\sum_{i=1}^{f} m_i \geqslant 3f.$$

Если ребро графа является мостом, то оно входит в границу только внешней грани, в противном случае ребро входит в границу ровно двух граней. Значит, при вычислении суммы $\sum\limits_i m_i$ каждое ребро графа учитывается не более двух раз и

$$\sum_{i=1}^{f} m_i \leqslant 2m.$$

Следствием полученных оценок для $\sum m_i$ является неравенство $3f \leqslant 2m$, или, с учетом формулы Эйлера, $3(m - n + 2) \leqslant 2m$, откуда $m \leqslant 3n - 6$. ▶

Следствие 4. *В любом простом планарном графе есть вершина степени не больше 5.*

◀ Достаточно доказать утверждение для простого плоского связного графа $G = \langle V, E \rangle$, в котором число вершин больше 6. Используя предыдущее следствие (вместе с его обозначениями), имеем: $m \leqslant 3n - 6$. Предположим противное тому, что требуется доказать: $\forall\, v_i \in V \quad \rho(v_i) \geqslant 6$; тогда, применяя лемму о рукопожатиях, получим:

$$2m = \sum_{i=1}^{n} \rho(v_i) \geqslant 6n,$$

или $m \geqslant 3n$, что противоречит следствию 3. ▶

Следствие 5. *Граф K_5 не является планарным.*

◀ Действительно, в полном графе K_5 $n = 5$ вершин и $m = C_5^2 = 10$ ребер; неравенство следствия 3 не выполняется — стало быть, граф K_5 не планарен. ▶

Следствие 6. *Граф $K_{3,3}$ не является планарным.*

◀ В полном двудольном графе $K_{3,3}$ $n = 6$ вершин и $m = 9$ ребер; если бы этот граф был планарным, то его плоская укладка содержала бы $f = m - n + 2 = 5$

граней. Используя обозначения, введенные при доказательстве следствия 3, получим: $\sum_i m_i = 2m = 18$. С другой стороны, легко видеть, что в двудольном графе нет циклов длины 3, поэтому каждая грань должна быть ограничена не менее чем 4 ребрами, т. е. $\forall i \quad m_i \geqslant 4$, откуда $\sum_{i=1}^{5} m_i \geqslant 20$. Предположение о планарности $K_{3,3}$ привело к противоречию. ►

§ 12. Критерий планарности графа

Подразбиением ребра uv называют его замену на два ребра uw и wv, где w — некоторая новая вершина графа. Два графа *гомеоморфны*, если они могут быть получены из одного и того же графа с помощью подразбиения ребер. Например, любые два циклических графа C_k и C_l $(k, l \geqslant 2)$ гомеоморфны, так как могут быть получены подразбиением ребер из графа C_2. Другой пример приведен на рис. 26. Ясно, что гомеоморфные плоские графы имеют одинаковое число граней. Понятие гомеоморфизма позволяет сформулировать критерий планарности графа.

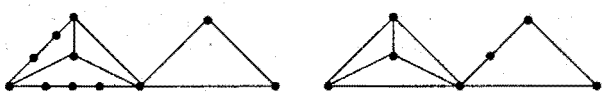


Рис. 26. Гомеоморфные графы

Теорема 18 (Л. С. Понтрягин, 1927 г.; К. Куратовский, 1930 г.). *Граф является планарным тогда и только тогда, когда он не содержит подграфа, гомеоморфного* K_5 *или* $K_{3,3}$.

◄ *Необходимость.* Очевидно, что подразбиение ребра никак не влияет на планарность или непланарность графа; поэтому два гомеоморфных графа либо оба планарны, либо оба непланарны. Непланарность графов K_5 и $K_{3,3}$ доказана в предыдущем параграфе.

Доказательство *достаточности* сформулированного условия планарности очень громоздкое; его мы опустим. ►

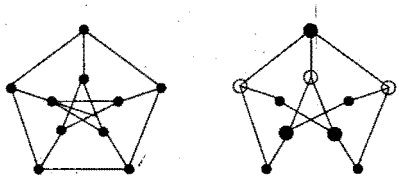


Рис. 27. Граф Петерсена и его подграф, гомеоморфный $K_{3,3}$

Пример. Граф Петерсена не является планарным — см. рис. 27.

§ 13. Ориентированные графы

Напомним, что *ориентированный граф* (сокращенно: *орграф*) — это упорядоченная пара $G = \langle V, A \rangle$, где V — непустое конечное множество — множество вершин; A — конечное мультимножество *упорядоченных* пар необязательно различных элементов V — мультимножество *дуг*. *Основанием* орграфа $G = \langle V, A \rangle$ называют

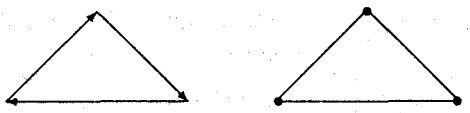


Рис. 28. Орграф и его основание

(неориентированный) граф $\langle V, E\rangle$, который получается из G заменой дуг ребрами (каждая дуга (u, v) заменяется ребром $\{u, v\}$). Пример — на рис. 28. Орграфы называются *изоморфными*, если существует изоморфизм между их основаниями, сохраняющий порядок вершин на каждой дуге.

Через $\Gamma(v)$ обозначим множество вершин, *к которым* ведут дуги с началом в вершине v: $\Gamma(v) = \{u \in V \mid (v, u) \in A\}$. Число таких дуг называют *полустепенью исхода* вершины v: $\overleftarrow{\rho}(v) = |\Gamma(v)|$. Вершину с нулевой полустепенью исхода называют *стоком*.

Через $\Gamma^{-1}(v)$ обозначим множество вершин, *из которых* ведут дуги к вершине v: $\Gamma^{-1}(v) = \{u \in V \mid (u, v) \in A\}$. Число таких дуг называют *полустепенью захода* вершины v: $\overrightarrow{\rho}(v) = |\Gamma^{-1}(v)|$. Вершину с нулевой полустепенью захода называют *источником*.

Степенью вершины орграфа называют сумму полустепеней исхода и захода: $\rho(v) = \overleftarrow{\rho}(v) + \overrightarrow{\rho}(v)$. Подсчитав двумя способами число дуг орграфа $\langle V, A\rangle$, получим следующее утверждение.

Лемма о рукопожатиях для орграфов

$$|A| = \sum_{v \in V} \overleftarrow{\rho}(v) = \sum_{v \in V} \overrightarrow{\rho}(v).$$

Вполне очевидным образом переносятся на случай ориентированных графов такие понятия (известные по предыдущим параграфам этой главы), как *смежность вершин*, *матрица смежности*, *простой граф* и многие другие. Термин *маршрут* заменим термином *путь*. Итак, *путь* в орграфе — последовательность дуг вида

$$(v_0, v_1),\ (v_1, v_2),\ \ldots,\ (v_{m-1}, v_m),$$

которую будем записывать также в виде $v_0 \to v_1 \to \ldots \to v_m$ и называть *путем из v_0 в v_m*.

§ 14. Нахождение кратчайших путей в орграфе

Пусть $G = \langle V, A\rangle$ — *взвешенный* орграф, т. е. каждой его дуге $e = (u, v) \in A$ поставлено в соответствие неотрицательное число $\mu(e) = \mu(u, v)$, называемое ее *весом*. Вес пути P — сумма весов его дуг:

$$\mu(P) = \sum_{e \in P} \mu(e).$$

Кратчайшим путем из вершины s в вершину t назовем путь минимального веса, ведущий из s в t, а под *расстоянием* между вершинами s и t будем понимать вес

этого пути:

$$d(s,t) = \min_{P:s\to\ldots\to t} \mu(P).$$

Вес *тривиального* (т.е. не содержащего дуг) пути считаем равным нулю, поэтому $d(s,s) = 0$. Если не существует пути из s в t, то полагаем: $d(s,t) = \infty$. Очевидна практическая значимость задачи нахождения кратчайших путей в ориентированном графе.

Алгоритм Е. Дейкстры (1959 г.)

Данный алгоритм находит кратчайшие пути от произвольной фиксированной вершины орграфа. Алгоритм представляет собой итерационную процедуру, на каждом шаге которой каждой вершине v сопоставляется пометка $l(v)$, которая является либо *постоянной* и равной при этом расстоянию $d(s,v)$ от начальной вершины s до данной вершины, либо *временной* — числом, являющимся оценкой сверху для $d(s,v)$. В результате каждой итерации оценки уточняются, и при этом ровно одна временная пометка (а именно — наименьшая) переходит из разряда временных в разряд постоянных (после чего уже не меняется).

Перед первой итерацией начальная вершина имеет постоянную пометку $l(s) = 0$, у остальных вершин пометки временные и полагаются равными ∞. Итерация алгоритма состоит в просмотре вершин v с временными пометками, к которым ведут дуги из вершины p — вершины, последней получившей постоянную пометку (для первой итерации $p = s$). Пусть $a = l(p) + \mu(p,v)$. Если окажется, что $l(v) > a$, то a будет новым значением $l(v)$ (временная пометка данной вершины уменьшается).

Алгоритм заканчивает работу, когда заданная конечная вершина t получает постоянную пометку.

Более детальное описание алгоритма (с использованием конструкций Си, а также математической символики) — на рис. 29 (с. 132).

Обоснование корректности алгоритма Дейкстры

Алгоритм работает таким образом, что после каждой итерации пометка каждой вершины v есть вес кратчайшего из тех путей из s в v, в которых предпоследняя вершина имеет постоянную пометку. Пусть после очередной итерации вершина v^* получает постоянную пометку. Достаточно доказать, что кратчайший путь из s в v^* проходит через вершины с постоянными пометками. Предположим противное: кратчайший путь P из s в v^* проходит через некоторую вершину с временной пометкой:

$$P: s \to s_1 \to \ldots \to s_k \to w \to \ldots \to v^*,$$

пусть w — первая такая вершина. Тогда

$$\mu(P) = \sum_{e\in P} \mu(e) > \mu(s,s_1) + \ldots + \mu(s_k,w).$$

Таким образом, существует путь из s в w, проходящий только через вершины с постоянными пометками и имеющий меньший вес, чем путь из s в v^*, что противоречит выбору v^*.

```
/* Нахождение кратчайшего пути между двумя вершинами (s и t) */
/* V — множество вершин графа  */
/* s — начальная вершина       */
/* t — конечная вершина        */
/* l — пометки вершин          */

/* Расстановка начальных пометок */
l(s)=0;
for(v∈V) if(v!=s) l(v)=∞;
/* M — множество временных пометок */
M=V\{s};
/* p — вершина, последней получившая постоянную пометку */
p=s;

while(p!=t)
{
     for(v∈ M ∩ Γ(p))
     {
        a=l(p)+μ(p,v);
        if(a<l(v))
        {
          /* θ(v) — вершина, из которой идет дуга в v*/
          /* (в кратчайшем пути)                     */
          l(v)=a; θ(v)=p;
        }
     }
     l(v*)=min l(v);
           v∈M
          /* пометка v* становится постоянной */
     M=M\{v*}; p=v*;
}
d(s,t)=l(t); /* расстояние между s и t; */
/* кратчайший путь: s → ... → θ(θ(t)) → θ(t) → t */
```

Рис. 29. Алгоритм Дейкстры нахождения кратчайшего пути в орграфе

Трудоемкость алгоритма Дейкстры

Пусть граф содержит n вершин. На каждой итерации число сложений не превышает количества временных пометок, которое в начале работы алгоритма равно $n-1$, а с каждой итерацией уменьшается на единицу. Таким образом, общее число сложений не более

$$(n-1)+(n-2)+\ldots+1=\frac{n(n-1)}{2}.$$

Операции сравнения выполняются как при пересчете пометок, так и при нахождении минимальной временной пометки; нетрудно подсчитать, что их число не превосходит $n(n-1)$. Таким образом, трудоемкость алгоритма оценивается как

Таблица 3

итерация \вершина	1	2	3	4	5	6	p
0	[0]	∞	∞	∞	∞	∞	1
1	—	6	[2]	∞	∞	∞	3
2	—	5	—	7	[3]	∞	5
3	—	[5]	—	6	—	7	2
4	—	—	—	[6]	—	7	4
5	—	—	—	—	—	[7]	6

$O(n^2)$ операций. Известна модификация алгоритма Дейкстры, имеющая трудоемкость $O(m \log_2 n)$ (m — число дуг).

Для того, чтобы найти расстояния от заданной вершины s до *всех остальных* вершин орграфа, алгоритм с рис. 29 модифицируется следующим образом:

- условие продолжения итераций `p!=t` заменяется на `M`$\neq \varnothing$.

Пример. Работа алгоритма для графа, изображенного на рис. 30 (рядом с каждой дугой проставлен ее вес), показана в табл. 3 (элементы таблицы — за исключением первого и последнего столбца — пометки вершин графа; в рамку заключены постоянные пометки вершин).

Анализ таблицы показывает, что кратчайший путь от 1 вершине к 6 вершине таков: $1 \to 3 \to 5 \to 6$.

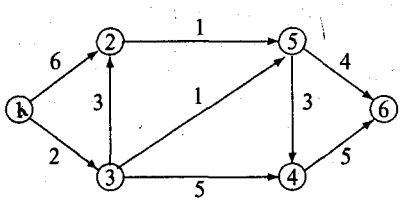


Рис. 30

Нахождение расстояний между всеми парами вершин орграфа

В принципе, данную задачу можно решить n-кратным выполнением алгоритма Дейкстры, где n — количество вершин графа. Однако существует примерно вдвое менее трудоемкий алгоритм, разработанный Р. Флойдом.

Алгоритм Р. Флойда (1962 г.)

Строится последовательность матриц $C^{(k)} = \left(c_{ij}^{(k)}\right)$, где $C^{(0)}$ — матрица весов дуг графа, т. е. для всех i и j $c_{ij}^{(0)} = \mu(v_i, v_j)$ (если в графе нет дуги (v_i, v_j), то полагаем: $\mu(v_i, v_j) = \infty$), а при $k = 1, \ldots, n$ $c_{ij}^{(k)}$ — длина кратчайшего пути из v_i в v_j такого, что в качестве промежуточных вершин могут быть лишь $v_1, v_2, \ldots, v_k$. Очевидно, что $c_{ij}^{(n)}$ — искомое расстояние между вершинами v_i и v_j. Несложно по индукции доказать следующую рекуррентную формулу, позволяющую по матрице $C^{(k-1)}$ построить матрицу $C^{(k)}$:

$$c_{ij}^{(k)} = \min\left\{c_{ij}^{(k-1)},\ c_{ik}^{(k-1)} + c_{kj}^{(k-1)}\right\}.$$

Действительно, кратчайший путь из v_i в v_j (где в качестве промежуточных вершин могут использоваться лишь $v_1, v_2, \ldots, v_k$) либо содержит вершину v_k, либо

не содержит. В первом случае он имеет вес $c_{ij}^{(k-1)}$ (так как при этом промежуточными вершинами могут быть только $v_1, \ldots, v_{k-1}$), во втором — складывается из кратчайших путей из v_i в v_k и из v_k в v_j, и его вес равен $c_{ik}^{(k-1)} + c_{kj}^{(k-1)}$.

§ 15. Задача сетевого планирования и управления (PERT)

Процесс выполнения сложного проекта удобно представить в виде орграфа, дуги которого соответствуют *этапам* (или *операциям*, *элементарным работам*) проекта, а вершины графа изображают абстрактные *события*, обозначающие начало или конец этапов; причем этапы, соответствующие дугам, исходящим из произвольной вершины графа, не могут начаться прежде, чем закончатся этапы (так называемые *опорные работы*), отвечающие дугам, заходящим в данную вершину. В проектно-конструкторских организациях подобный граф называют *сетевым графиком*.

Очевидно, что рассматриваемый граф является ациклическим.

Например, при строительстве здания в качестве этапов могут рассматриваться закладка фундамента, возведение стен, возведение крыши, вставка окон и т. д., а в качестве событий — начало строительства, окончание возведения фундамента, начало отделочных работ, окончание строительства и т. п.

Таблица 4

Этап проекта (элементарная работа)	Обозначение	Опорные работы	Время выполнения
Разработка технического задания	e_1	—	5
Конструирование оснастки	e_2	—	8
Разработка электросхемы	e_3	e_1	3
Разработка сборочных чертежей	e_4	e_1	8
Разработка технологии сборки	e_5	e_3	2
Изготовление оснастки	e_6	e_2	4
Монтаж электросхемы	e_7	e_3	7
Сборка изделия	e_8	e_4, e_5	5
Окраска изделия	e_9	e_6, e_7	2

Пример 1. Рассмотрим построение сетевого графика для планирования производства некоторого изделия. Перечень элементарных работ, их длительность и логические связи представлены в табл. 4.

Дуги сетевого графика мы будем обозначать так же, как и соответствующие работы. Источник графа будет соответствовать началу выполнения проекта, а сток — окончанию.

Из таблицы видно, что работы e_1 и e_2 являются начальными (у них нет предшествующих работ), а работы e_8 и e_9 — завершающими (они не предшествуют никаким другим). Таким образом, дуги e_1 и e_2 будут начинаться в источнике графа, а дуги e_8 и e_9 — заканчиваться в стоке.

По окончании работы e_1 начинаются работы e_3 и e_4 — значит, в графе конец дуги e_1 будет служить началом дуг e_3 и e_4. Аналогично, конец дуги e_3 — начало дуг e_5 и e_7. Поскольку работе e_8 непосредственно предшествуют работы e_4 и e_5, в графе должна быть вершина, служащая концом дуг e_4 и e_5 и началом дуги e_8.

Продолжая подобные рассуждения, в конце концов получаем следующий сетевой график (рис. 31).

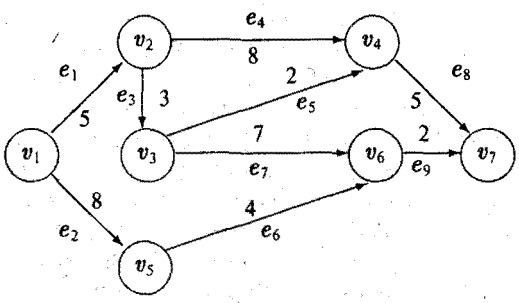


Рис. 31

Будем считать, что задано конкретное время выполнения каждого этапа [9] — вес дуги $t(v_i, v_j)$.

В задаче сетевого планирования и управления [10] требуется найти минимальное время выполнения проекта — время, за которое можно пройти по всем дугам графа, двигаясь от начальной вершины (s) к конечной вершине (t), причем движение по каждой дуге может начаться лишь после того, как пройдены все дуги, заходящие в ее начало. Другими словами, нужно найти самый длинный путь (т.е. путь наибольшего веса) от s к t.

Для решения данной задачи можно модифицировать алгоритм Дейкстры нахождения кратчайшего пути от s к t: заменить ∞ на 0, $<$ на $>$, min на max. Мы опишем более эффективный алгоритм, учитывающий ацикличность графа.

Пронумеруем вершины орграфа $G = \langle V, A \rangle$ так, чтобы каждая дуга (v_i, v_j) $(i, j = 1, \ldots, n)$ вела из вершины с меньшим номером в вершину с большим номером: $(v_i, v_j) \in A \Rightarrow i < j$ (в силу ацикличности это всегда возможно). Через $l(v_i)$ обозначим наиболее раннее время начала операций, соответствующих дугам, исходящим из вершины v_i (считая $l(v_1) = 0$), иными словами, $l(v_i)$ — длина самого длинного пути из v_1 в v_i. Минимальное время выполнения проекта тогда будет равно $l(v_n)$. Алгоритм состоит в последовательном вычислении $l(v_j)$ $(j = 2, \ldots, n)$ по очевидной формуле:

$$\boxed{l(v_j) = \max_{v_i \in \Gamma^{-1}(v_j)} \big(l(v_i) + t(v_i, v_j)\big)}$$

с нулевыми начальными условиями: $\forall\, i \;\; l(v_i) = 0$.

Пример 2. Для сетевого графика, построенного выше, в результате работы алгоритма находим:

$$l(v_1) = 0, \quad l(v_2) = 5, \quad l(v_3) = 8,$$
$$l(v_4) = \max\{l(v_2) + t(v_2, v_4),\ l(v_3) + t(v_3, v_4)\} = \max\{5 + 8, 8 + 2\} = 13,$$
$$l(v_5) = 8,$$
$$l(v_6) = \max\{l(v_3) + t(v_3, v_6),\ l(v_5) + t(v_5, v_6)\} = \max\{8 + 7, 8 + 4\} = 15,$$
$$l(v_7) = \max\{l(v_4) + t(v_4, v_7),\ l(v_6) + t(v_6, v_7)\} = \max\{13 + 5, 15 + 2\} = 18.$$

Таким образом, если считать, что время выполнения работ проекта было задано в днях, то минимальное время выполнения всего проекта равно 18 дням.

---

[9] В более общем случае время выполнения этапа — *случайная величина*.

[10] В англоязычной литературе принят термин PERT (Project Evaluation Research Task).

Путь наибольшей длины от начальной вершины графа к конечной называют *критическим путем.* В рассмотренном примере критическим является путь $v_1 \to v_2 \to v_4 \to v_7$. В общем случае, в графе может быть несколько критических путей. Для того чтобы проект был выполнен за минимальное время, операция, отвечающая каждой дуге критического пути, должна начинаться сразу после того, как закончится предшествующая ей операция (на указанном пути). Если дуга не принадлежит никакому критическому пути, то соответствующая ей операция может начать выполняться с некоторым запаздыванием, которое не отразится на общем времени выполнения проекта. Обозначим через $L(v_i)$ самое позднее время начала операций, отвечающих дугам, исходящим из вершины v_i, при котором весь проект все еще может быть выполнен за минимальное время. Для нахождения $L(v_i)$ поменяем ориентацию каждой дуги (при этом поменяются местами начальная и конечная вершины) и, повторив предыдущий алгоритм, найдем $l'(v_i)$ — самый длинный путь от v_n до v_i; нетрудно видеть, что $L(v_i) = l(v_n) - l'(v_i)$. Теперь для каждой операции (v_i, v_j) можно определить *резерв времени* $r(v_i, v_j)$ — на сколько единиц времени можно отложить начало ее выполнения, чтобы проект мог быть выполнен за минимальное время (при отсутствии других задержек):

$$\boxed{r(v_i, v_j) = L(v_j) - l(v_i) - t(v_i, v_j).}$$

Для последнего примера имеем:

Таблица 5

i	1	2	3	4	5	6	7
$l(v_i)$	0	5	8	13	8	15	18
$l'(v_i)$	18	13	9	5	6	2	0
$L(v_i)$	0	5	9	13	12	16	18

Для расчета резервов времени работ, не входящих в критический путь, составим табл. 6.

Таблица 6

v_iv_j	$L(v_j)$	$l(v_i)$	$t(v_iv_j)$	$r(v_i, v_j) = L(v_j) - l(v_i) - t(v_i, v_j)$
v_2v_3	9	5	3	1
v_3v_4	13	8	2	3
v_3v_6	16	8	7	1
v_1v_5	12	0	8	4
v_5v_6	16	8	4	4
v_6v_7	18	15	2	1

В заключение параграфа заметим, что более детальное и подробное изложение теории сетевого планирования (включающее в себя, в частности, предположение о том, что время выполнения каждой работы является случайной величиной со своим законом распределения) содержится в специальных руководствах.

§ 16. Потоки в сетях

Пусть $G = \langle V, A\rangle$ — орграф без петель[11], имеющий единственный источник (будем обозначать его v_1) и единственный сток (v_n). Все остальные вершины графа будем называть *промежуточными*. Если каждой дуге графа $a \in A$ поставлено в соответствие неотрицательное целое число $c(a)$ (*пропускная способность дуги*), то говорят, что задана *транспортная сеть* (или просто: *сеть*) $\langle G, c\rangle$.

Функция φ: $A \to \mathbb{N}_0$ (определенная на семействе дуг орграфа и принимающая неотрицательные целые значения) называется *потоком в сети* $\langle G, c\rangle$, если выполняются следующие условия:

1) для любой дуги $a \in A$ $\varphi(a) \leqslant c(a)$;
2) для любой промежуточной вершины графа v

$$\sum_{u \in \Gamma^{-1}(v)} \varphi(u, v) = \sum_{u \in \Gamma(v)} \varphi(v, u).$$

Величину $\varphi(a)$ будем называть *потоком по дуге* a. Таким образом, 1) поток по каждой дуге не должен превышать ее пропускной способности; 2) сумма потоков по дугам, заходящим в произвольную промежуточную вершину, равен сумме потоков по дугам, исходящим из этой вершины. Другими словами, поток не возникает и не накапливается в промежуточных вершинах. Данная математическая модель описывает поведение газа или жидкости в трубопроводе, транспортные потоки в сети дорог, пересылку товаров на рынок по различным каналам и т. д.

Величиной потока $W(\varphi)$ назовем сумму потоков по дугам, исходящим из источника:

$$W(\varphi) = \sum_{v \in \Gamma(v_1)} \varphi(v_1, v).$$

Покажем, что она равна сумме потоков по дугам, заходящим в сток. Действительно, суммируя равенства из условия 2) потока по всем промежуточным вершинам, получаем:

$$\sum_{v \in V \setminus \{v_1, v_n\}} \sum_{u \in \Gamma^{-1}(v)} \varphi(u, v) = \sum_{v \in V \setminus \{v_1, v_n\}} \sum_{u \in \Gamma(v)} \varphi(v, u).$$

Если вычесть из обеих частей равенства потоки через дуги, оба конца каждой из которых являются промежуточными вершинами (каждый такой поток слева и справа от знака равенства встречается ровно один раз), то получим:

$$W(\varphi) = \sum_{v \in \Gamma(v_1)} \varphi(v_1, v) = \sum_{v \in \Gamma^{-1}(v_n)} \varphi(v, v_n).$$

Поток в транспортной сети, имеющий наибольшую возможную величину, называют *максимальным потоком*. В одной и той же сети может быть несколько максимальных потоков (их величины, разумеется, должны совпадать).

Пусть φ — поток в сети $\langle G, c\rangle$. Дуга $a \in A$ называется *насыщенной*, если поток по ней равен ее пропускной способности: $\varphi(a) = c(a)$. Поток φ называется *полным*, если любой путь в орграфе G из v_1 в v_n содержит по меньшей мере

[11] *Петля* в орграфе — дуга вида (u, u).

одну насыщенную дугу. Очевидно, что всякий максимальный поток является полным (иначе увеличив потоки по ненасыщенным дугам, составляющим путь $v_1 \to \ldots \to v_n$, на 1, мы не нарушим условий 1) и 2) потока и получим поток с большей на 1 величиной, чем у данного потока).

В дальнейшем будем считать, что орграф $G = \langle V, A\rangle$ — *антисимметрический*, т. е. он не содержит кратных дуг и если $(u, v) \in A$, то $(v, u) \notin A$. Это предположение не является сильно ограничительным, поскольку *подразбиением* дуг (введением дополнительных «фиктивных» вершин) всегда можно по данной сети построить сеть с антисимметрическим орграфом и той же величиной потока.

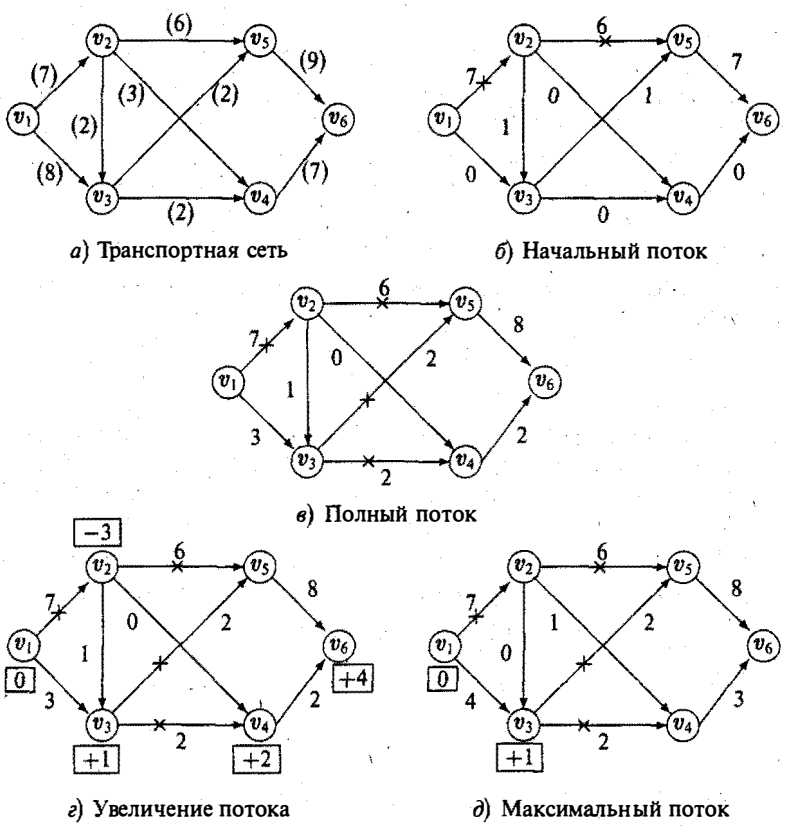
Максимальный поток можно найти с помощью следующего алгоритма.

Алгоритм Л. Форда–Д. Фалкерсона (1956 г.)

1. *Построить произвольный поток* φ в сети $\langle G, c\rangle$ (можно и нулевой).
2. *Построить полный поток.* Если поток φ не полный, то в сети существует путь из v_0 в v_n, все дуги которого не насыщены. Увеличивая потоки через все дуги такого пути P на величину $\min\limits_{a\in P}(c(a) - \varphi(a))$, получаем путь, некоторая дуга которого является насыщенной. Такую операцию следует повторять до тех пор, пока не получится полный поток.
3. *Построить максимальный поток.*
   а) **Начальные пометки.** Присвоить источнику пометку 0: $l(v_1) = 0$, а остальным вершинам пометку ∞. Следующий шаг повторять до тех пор, пока в результате его выполнения не будет помечен сток v_n либо пока не перестанут появляться новые пометки.
   б) **Пересчет пометок.** Для каждой помеченной вершины v_i, пометить символом $+i$ все непомеченные вершины v $(l(v) = \infty)$, для которых дуги (v_i, v) ненасыщенные (т. е. $\varphi(v_i, v) < c(v_i, v)$), и символом $-i$ все непомеченные вершины, для которых $\varphi(v, v_i) > 0$.
   в) **Увеличение потока.** Если сток v_n не получает новую пометку, то закончить работу алгоритма (максимальный поток найден), в противном случае существует цепь[12], $v_0 \to \ldots \to v_n$, все вершины которой помечены. Если ориентация дуги $a = (v_i, v_j)$ совпадает с направлением прохождения цепи, будем обозначать ее $\overrightarrow{a}$, в противном случае — $\overleftarrow{a}$. Если $l(v_j) = +i$ $(\overrightarrow{a} = (v_i, v_j))$, то положить $\lambda(a) = c(a) - \varphi(a)$. Если $l(v_j) = -i$ $(\overleftarrow{a} = (v_j, v_i))$, то положить $\lambda(a) = \varphi(a)$. Пусть $\varepsilon = \min(\lambda(a))$ (минимум вычисляется по всем дугам, составляющим указанную цепь). По каждой дуге $\overrightarrow{a}$ поток увеличить на ε, а по каждой дуге $\overleftarrow{a}$ поток уменьшить на ε. (При этом величина потока в сети $W(\varphi)$ увеличится на ε.) Перейти к шагу а).

Перед тем, как обосновать алгоритм Форда—Фалкерсона, проиллюстрируем его работу на примере (рис. 32, на котором насыщенные дуги помечены значком "×"). Начальный поток не является полным. В пути $v_1 \to v_3 \to v_4 \to v_6$ все дуги не насыщены; увеличение потока, проходящего через этот путь, на 2 приводит к насыщению дуги $v_3 \to v_4$. Находим, еще один путь $(v_1 \to v_3 \to v_5 \to v_6)$,

[12] Заметьте: в общем случае — не *путь*!



а) Транспортная сеть

б) Начальный поток

в) Полный поток

г) Увеличение потока

д) Максимальный поток

Рис. 32. Алгоритм Форда—Фалкерсона нахождения максимального потока

состоящий из ненасыщенных дуг; увеличение потока через каждую из этих дуг на 1 делает дугу $v_3 \to v_5$ насыщенной. Теперь получен полный поток.

Переходим к 3-му этапа алгоритма Форда—Фалкерсона. Расставляем пометки вершин, как показано на рис. 32 *г*. Получаем цепь

$$v_1 \to v_3 \to v_2 \to v_4 \to v_6.$$

Имеем:

$$\lambda(\overrightarrow{v_1, v_3}) = 5; \quad \lambda(\overleftarrow{v_3, v_2}) = 1; \quad \lambda(\overrightarrow{v_2, v_4}) = 3; \quad \lambda(\overrightarrow{v_4, v_6}) = 5; \quad \varepsilon = 1.$$

Уменьшаем поток на 1 через дугу (v_2, v_3) и увеличиваем его на 1 через остальные дуги этой цепи. При повторении процедуры (рис. 32 *д*) удается пометить только две вершины (v_1 и v_3). Максимальный поток найден: $W(\varphi) = 11$.

Доказательство корректности алгоритма Форда—Фалкерсона

Так как количество различных (целочисленных) потоков в фиксированной транспортной сети конечно, максимальный поток *существует*. Поскольку в результате каждой итерации алгоритма Форда—Фалкерсона величина потока увеличивается по меньшей мере на 1, алгоритм работает *конечное время*, т. е. рано или поздно

прекратит свою работу. Осталось доказать, что поток, который он строит, является максимальным.

Введем ряд новых понятий. Пусть B — некоторое множество вершин орграфа $G = \langle V, A\rangle$, не содержащее источник и содержащее сток ($B \subset V$, $v_1 \notin B$, $v_n \in B$). *Разрезом сети* $\langle G, c\rangle$ *относительно* B называется множество A_B^- дуг, исходящих из вершин, не принадлежащих B, и заходящих в вершины из B:

$$A_B^- = \{(u, v) \in A \mid u \notin B,\ v \in B\}.$$

Сумма пропускных способностей всех дуг разреза называется *пропускной способностью разреза*:

$$c(A_B^-) = \sum_{a \in A_B^-} c(a).$$

Разрез с минимальной пропускной способностью называют *минимальным разрезом*. Из «физических» соображений кажется почти очевидным, что *величина потока в сети не превосходит пропускной способности любого разреза* (значит, и минимального). Для строгого доказательства этого факта нам понадобится

Лемма 5. *Для любого множества B вершин орграфа G, среди которых есть сток и нет источника, справедливо следующее равенство*:

$$\sum_{a \in A_B^-} \varphi(a) - \sum_{a \in A_B^+} \varphi(a) = W(\varphi), \tag{1}$$

где

$$A_B^- = \{(u, v) \in A \mid u \notin B, v \in B\},$$
$$A_B^+ = \{(u, v) \in A \mid u \in B, v \notin B\}.$$

◄ Прибавив к уменьшаемому и вычитаемому в разности (1) сумму потоков по всем дугам, исходящим из B и заходяшим в B, получим равенство, равносильное (1):

$$\sum_{(u,v) \in A,\ v \in B} \varphi(u, v) - \sum_{(u,v) \in A,\ u \in B} \varphi(u, v) = W(\varphi). \tag{2}$$

Вклад стока v_n в левую часть (2) равен $W(\varphi)$, а вклад каждой из остальных вершин из множества B (так как среди них нет и источника, все они — промежуточные) равен 0 в силу условия 2) потока. Соотношение (2), а вместе с ним и (1), доказано. ►

Дальнейшее рассуждение очевидно:

$$W(\varphi) = \sum_{a \in A_B^-} \varphi(a) - \sum_{a \in A_B^+} \varphi(a) \leqslant \sum_{a \in A_B^-} \varphi(a) \leqslant \sum_{a \in A_B^-} c(a) = c(A_B^-).$$

Итак, мы выяснили, что величина потока в сети не превосходит пропускной способности минимального разреза. После окончания работы алгоритма Форда—Фалкерсона в сети не существует цепи $v_1 \to \ldots \to v_n$, вдоль которой возможно увеличение потока. Пусть B — множество вершин, которые не получают (конечной)

пометки на последней итерации алгоритма. Заметим, что $v_1 \notin B, v_n \in B$. Рассмотрим разрез сети относительно B. Пусть u — помеченная вершина ($u \notin B$), а v — непомеченная ($v \in B$). Если дуга имеет вид (u, v), то согласно алгоритму эта дуга является насыщенной: $\varphi(u, v) = c(u, v)$. Если дуга имеет вид (v, u), то согласно алгоритму поток по этой дуге равен нулю: $\varphi(v, u) = 0$. Применим теперь лемму 5:

$$W(\varphi) = \sum_{a \in A_B^-} \varphi(a) - \sum_{a \in A_B^+} \varphi(a) = \sum_{a \in A_B^-} c(a) = c(A_B^-).$$

Таким образом, в результате работы алгоритма построен поток, величина которого *равна* пропускной способности некоторого разреза сети; поэтому поток — максимальный. Мы доказали следующее утверждение:

Теорема 19 (Л. Форд–Д. Фалкерсон, 1956 г.). *Величина максимального потока в сети равна пропускной способности минимального разреза.*

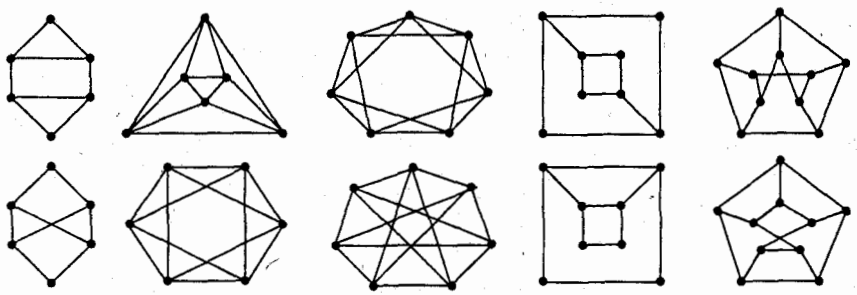
В заключение параграфа — несколько замечаний.

1. Приведенное выше доказательство теоремы Форда—Фалкерсона показывает, как найти один из минимальных разрезов. Это разрез составляют дуги, ведущие из помеченных вершин в непомеченные на последнем этапе работы алгоритма Форда—Фалкерсона. Например, для транспортной сети, изображенной на рис. 32*а*, минимальный разрез образуют дуги v_1v_2, v_3v_4, v_3v_5.
2. Если величина пропускной способности дуги не обязательно является неотрицательным целым числом, то, как показали сами Форд и Фалкерсон, если «неудачно» выбирать *увеличивающие цепи*, то процесс выполнения алгоритма может никогда не кончиться, более того, величина текущего потока может все время не превосходить четверти максимального потока. В настоящее время известен эффективный алгоритм нахождения максимального потока трудоемкости $O(n^3)$.
3. Можно рассмотреть и более общую постановку задачи, допускающую наличие в сети нескольких источников и стоков. В этом случае следует ввести *фиктивный* источник, от которого идут дуги к (настоящим) источникам (последние перейдут в разряд промежуточных вершин), и *фиктивный* сток, к которому идут дуги от (настоящих) стоков (также становящихся промежуточными вершинами). Так задача будет сведена к задаче с одним источником и одним стоком.

Упражнения

Определения и примеры

1. Пусть G_n — простой граф с множеством вершин $\{v_1, \ldots, v_n\}$, в котором вершины v_i и v_j смежны тогда и только тогда, когда числа i и j взаимно просты. Изобразить графы G_4 и G_6 и найти их матрицы смежности. Показать, что если $m < n$, то $G_m \subset G_n$.
2. Для графов из каждой пары графов, изображенных на рис. 33, выяснить, изоморфны ли они.



а) *б*) *в*) *г*) *д*)

Рис. 33

3. Найти все (с точностью до изоморфизма) простые графы, в которых не более пяти вершин.
4. Сколько существует попарно неизоморфных простых графов с 10 вершинами и 1) 44; 2) 43 ребрами?
5. Сколько существует помеченных простых графов с n вершинами? Сколько из них имеет m ребер?
6. Доказать, что в простом графе с не менее чем двумя вершинами найдутся две вершины одинаковой степени.
7. Показать, что реберные графы $L(K_n)$ и $L(K_{n,m})$ являются регулярными.
8. Доказать, что при $n > 2$ звездный граф $K_{1,n}$ не является реберным графом.
9. Пусть $\rho_1, \rho_2, \ldots, \rho_n$ — степени вершин графа G. Сколько вершин и ребер содержит реберный граф $L(G)$?
10. Доказать, что простой граф изоморфен своему реберному графу тогда и только тогда, когда он является дизъюнктным объединением циклических графов.
11. Привести примеры (когда это возможно)
    1) двудольного графа, являющегося регулярным;
    2) кубического графа с 9 вершинами;
    3) (для каждого n) простого графа с n вершинами и $\dfrac{(n-1)(n-2)}{2}$ ребрами;
    4) (для каждого n) простого графа с n вершинами, изоморфного своему реберному графу;
    5) связных графов, являющихся регулярными графами степени 4.
12. Какие из платоновых графов являются двудольными?
13. **[Теорема Кёнига.]** *Граф является двудольным тогда и только тогда, когда все его циклы имеют четную длину.* Доказать.
14. Доказать, что в непустом двудольном регулярном графе доли содержат равное число вершин.
15. Может ли регулярный степени выше 1 двудольный граф иметь мосты?
16. В связном графе степени четырех вершин равны 3, а степени остальных вершин равны 4. Доказать, что нельзя удалить ребро так, чтобы граф распался на две изоморфные компоненты связности.
17. Пусть в графе среди любых четырех вершин найдется вершина, смежная с тремя остальными. Доказать, что радиус графа равен единице.
18. Найти дополнения к графам, соответствующим тетраэдру, кубу и октаэдру.

19. Вычислить:

1) $C_4 + N_2$; 2) $K_n + K_m$; 3) $\overline{K}_{n,m}$; 4) $\overline{G + H}$ (G и H — простые графы).

20. Пусть G, H и K — простые графы; доказать или опровергнуть следующие равенства:

1) $G \cup (H + K) = (G \cup H) + (G \cup K)$;
2) $G + (H \cup K) = (G + H) \cup (G + K)$.

21. Найти матрицы смежности графов K_n, N_n и C_n.

22. Чем характерна матрица смежности двудольного графа?

23. Какова связь между матрицами смежности простого графа и его дополнения?

24. Пусть A — матрица смежности регулярного графа степени k. Доказать, что k есть собственное значение матрицы A. Найти отвечающий ему собственный вектор.

25. В графе Петерсена найти циклы длины 5, 6, 8 и 9.

26. В графе Петерсена найти разрезы из 3, 4 и 5 ребер.

27. Доказать, что дополнение к (простому) несвязному графу есть связный граф.

28. Доказать, что реберный граф связного графа связен.

29. Пусть G — граф с множеством вершин $\{v_1, \ldots, v_n\}$ и матрицей смежности A. Доказать, что число маршрутов длины k из v_i в v_j равно (i, j)-му элементу матрицы A^k. Показать также, что если G — простой граф, то число *треугольников* (циклов длины 3) в G равно $\operatorname{tr} \dfrac{A^3}{6}$ (где $\operatorname{tr} A = \sum\limits_{i=1}^{n} a_{ii}$ — *след* матрицы A). Верно ли, что число циклов длины 4 равно $\operatorname{tr} \dfrac{A^4}{8}$?

30. Основываясь на результате предыдущей задачи, предложите алгоритм определения диаметра графа по его матрице смежности.

31. **[Экстремальная теорема Турана.]** Пусть G — простой граф с $2n$ вершинами, не содержащий треугольников. Доказать, что в G не более n^2 ребер и привести пример, когда эта верхняя граница достигается.

32. Найти максимальное число ребер в простом графе с $2n+1$ вершинами, не содержащем треугольников.

33. Найти радиус и диаметр графа Петерсена.

34. Для каждого n построить пример графа, центр которого состоит из n вершин и не совпадает с множеством всех вершин.

35. Пусть а) $n = 4$; б) $n = 5$.

1) Найти цикловой индекс группы подстановок на множестве ребер полного графа с n вершинами, порожденных перестановками вершин.
2) С помощью теоремы Пойа найти число попарно неизоморфных простых графов с n вершинами и m ребрами.

Гамильтоновы и эйлеровы графы

36. Для каких чисел m и n следующие графы являются а) эйлеровыми; б) гамильтоновыми:

1) K_n; 2) $K_{m,n}$; 3) W_n?

37. Привести пример эйлерова графа, не являющегося гамильтоновым, и гамильтонова графа, не являющегося эйлеровым.

38. Пусть G — двудольный граф, доли которого содержат m и n вершин соответственно. Доказать, что

1) если G — гамильтонов граф, то $m = n$;
2) если G — полугамильтонов граф, то $|m - n| \leqslant 1$.

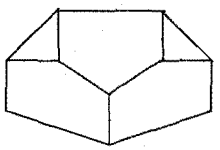


Рис. 34

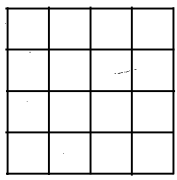


Рис. 35

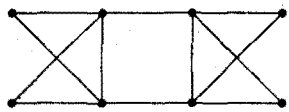


Рис. 36

39. Может ли а) конь; б) король; в) ладья побывать на каждой клетке шахматной доски размером 8×8 ровно один раз и последним ходом возвратиться в исходную позицию? Решить такую же задачу для доски 7×7.

40. Можно ли прогуляться по парку и его окрестностям (рис. 34) так, чтобы при этом перелезть через каждый забор ровно один раз?

41. Доказать, что если граф G связен и имеет $k > 0$ вершин нечетной степени, то минимальное число не имеющих общих ребер цепей, объединение которых содержит каждое ребро графа G, равно $k/2$.

42. Дан кусок проволоки длиной 120 см. Какое наименьшее число раз придется ломать проволоку, чтобы изготовить каркас куба с ребром 10 см?

43. Можно ли сетку, составленную из единичных квадратов (рис. 35), представить в виде объединения 1) восьми ломаных длины 5; 2) пяти ломаных длины 8?

44. С помощью алгоритма Флери найти эйлеров цикл в графе на рис. 36.

45. Доказать, что реберный граф простого эйлерова графа является одновременно эйлеровым и гамильтоновым.

46. Доказать, что реберный граф простого гамильтонова графа является гамильтоновым.

Деревья

47. Найти все (с точностью до изоморфизма) деревья, в которых не более семи вершин.

48. Волейбольная сетка имеет вид прямоугольника 50×600 клеток. Какое наибольшее количество веревочек можно перерезать так, чтобы сетка не распалась на куски?

49. Доказать, что каждое дерево является двудольным графом. Какие деревья являются полными двудольными графами?

50. Если в дереве не менее двух ребер, то его радиус меньше диаметра. Доказать.

51. Доказать, что центр дерева состоит из одной вершины, если диаметр дерева есть четное число, и двух вершин в противном случае.

52. Верно ли, что в дереве с нечетным диаметром любые две простые цепи наибольшей длины имеют хотя бы одно общее ребро?

53. Выразите радиус дерева через его диаметр.

54. Пусть n — количество вершин дерева, r — его радиус. Доказать, что $n \geqslant 2r$.

55. Верно ли, что если диаметр графа равен $k > 2$, то граф имеет стягивающее дерево диаметра k?

56. Для каждого из указанных ниже графов найти какое-нибудь стягивающее дерево и фундаментальную систему циклов относительно него.

1) K_5; 2) $K_{3,3}$; 3) W_5; 4) C_6; 5) граф Петерсена.

57. Пусть T_1 и T_2 — стягивающие деревья связного графа G. Показать, что для любого ребра e из T_1 существует ребро f из T_2 такое, что после «замены» в T_1 ребра e на ребро f вновь получится стягивающее дерево. (С помощью подобной процедуры можно построить последовательность стягивающих деревьев $T_1, \ldots, T_2$, в которой каждое дерево получается из предыдущего заменой одного ребра).

58. Доказать, что число реберно-помеченных деревьев с $n \geqslant 3$ вершинами (в которых помечены не вершины, а ребра) равно n^{n-3}.

59. Показать, что при больших n вероятность того, что случайным образом выбранная вершина дерева с n вершинами является висячей, приближенно равна $1/e$.

60. Найти стягивающее дерево минимального веса для каждого графа на рис. 37.

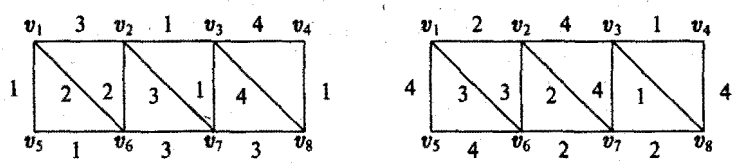


Рис. 37

61. Необходимо построить систему нефтепроводов, которые должны соединять семь нефтеочистительных заводов, принадлежащих некоторой компании, с портом ($П$), куда поступает сырая нефть. Известны (табл. 7) предполагаемые ежегодные затраты на эксплуатацию нефтепровода между соответствующими пунктами.

Таблица 7

	П	1	2	3	4	5	6	7
П	0	5	6	8	2	6	9	10
1	5	0	4	10	5	8	6	10
2	6	4	0	11	8	4	9	10
3	8	10	11	0	10	3	6	7
4	2	5	8	10	0	2	5	9
5	6	8	4	3	2	0	10	5
6	9	6	9	6	5	10	0	8
7	10	10	10	7	9	5	8	0

Найти систему нефтепроводов, позволяющую осуществлять переброску нефти от порта ко всем заводам с минимальными годовыми эксплуатационными затратами.

Корневые деревья

Дерево с выделенной вершиной (**корнем**) *называют* ***корневым деревом.***

62. Найти число помеченных корневых деревьев с n вершинами.

В книгах, посвященных исследованию структур данных, корневое дерево определяют рекурсивно следующим образом.

Корневое дерево T *— это непустое конечное множество* T *с элементами, называемыми вершинами, такими, что*

1) *имеется выделенная вершина, называемая корнем данного дерева;*
2) *если множество остальных вершин непусто, то оно разбивается на* m *множеств* $T_1, \ldots, T_m$, *каждое из которых в свою очередь является корневым деревом.*

*Деревья $T_1, \ldots, T_m$ называются **поддеревьями** данного корня. Из определения следует, что каждая вершина дерева является корнем некоторого своего дерева. Число поддеревьев дерева с корнем r — **порядок** вершины r. Вершины нулевого порядка называют **листьями**; остальные вершины называют **внутренними**.*

63. Сколько листьев имеет дерево с k внутренними вершинами, порядок каждой из которых равен двум?

64. В турнире по олимпийской системе («проигравший выбывает») участвует n человек. Сколько встреч будет проведено?

65. Некто купил курицу. После того, как она снесла два яйца, ее съели. Из яиц вывелись цыплята. Петухов съедали сразу, а куриц — после того, как они сносили по два яйца, и т. д. В какой-то момент вывелись одни петухи, и процесс закончился. Сколько куриц было съедено, если съели 97 петухов?

66. Сколько листьев имеет дерево, в котором (кроме листьев) содержится n_1 вершин порядка 1, n_2 вершин порядка 2, ..., n_s вершин порядка s?

Укладки графов

67. При каком k можно так расположить 6 точек на плоскости и соединить их попарно непересекающимися отрезками, чтобы каждая точка была соединена ровно с k другими?

68. При каких n графы G_n (определение см. в задаче 1) планарны?

69. Проверить формулу Эйлера, связывающую число вершин, ребер и граней плоского графа, для следующих графов:

1) W_n; 2) $K_{2,n}$; 3) графа, соответствующего клетчатому полю $s \times t$.

70. Всегда ли планарен реберный граф планарного графа?

71. Пусть в простом графе G не менее 11 вершин. Доказать, что граф G и его дополнение $\overline{G}$ не могут быть одновременно планарными.

72. Используя тот факт, что в простом плоском графе есть вершина степени не больше 5, доказать, что его вершины можно раскрасить не более чем в 6 цветов так, чтобы смежные вершины были разного цвета.

Ориентированные графы. Алгоритмы

73. Пусть A — матрица смежности орграфа с множеством вершин $\{v_1, \ldots, v_n\}$. Какой смысл имеют суммы строк и суммы столбцов матрицы A? Доказать, что (i, j)-й элемент матрицы A^k равен числу путей длины k из v_i в v_j.

74. В дереве с n вершинами ребра ориентируются случайным образом. Какова вероятность того, что найдется вершина, из которой ведут пути ко всем остальным вершинам?

75. Пусть G — связный граф. Зафиксируем некоторую его вершину v. Доказать, что можно так ориентировать ребра графа, что в получившемся орграфе существует путь от v до любой другой вершины.

*Ориентированный граф называют **сильно связным**, если для любых его вершин u и v существует путь из u в v.*

76. В связном графе степени всех вершин четны. Доказать, что можно так ориентировать ребра графа, чтобы

1) получившийся орграф был сильно связным;

2) для каждой вершины полустепень исхода была равна полустепени захода.

77. В ориентированном графе со связным основанием для каждой вершины полустепень исхода равна полустепени захода. Доказать, что орграф эйлеров.

78. Найти кратчайший путь от 1-й вершины до всех остальных (рис. 38*а, б*).

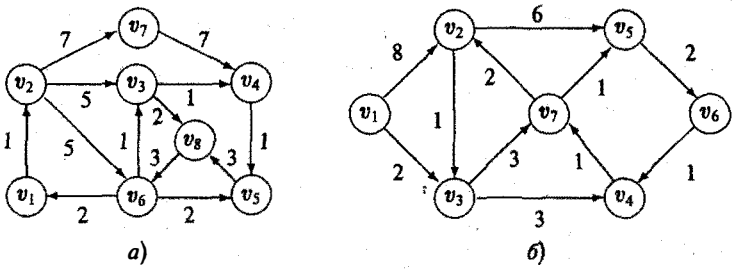


Рис. 38

79. Дана структурно-временная таблица работ по организации выставки-продажи товаров (табл. 8). Требуется построить сетевой график, найти наименьшее время выполнения проекта, определить критический путь, вычислить резервы времени для выполнения каждой операции.

Таблица 8

Этап проекта (элементарная работа)	Обозначение	Опорные работы	Время выполнения
Заказ на оборудование и товары	e_1	—	10
Разработка системы учета спроса	e_2	—	12
Отбор товаров и выписка счетов	e_3	e_1	2
Завоз товаров	e_4	e_3	3
Завоз оборудования	e_5	e_1	5
Установка оборудования	e_6	e_5	6
Выкладка товара	e_7	e_4	6
Учет наличия товара	e_8	e_4	5
Оформление зала и витрины	e_9	e_6, e_7	5
Изготовление документов учета	e_{10}	e_2, e_8	4
Репетиция выставки-продажи	e_{11}	e_9, e_{10}	2

80. Пусть проекты описываются взвешенными графами (рис. 39 *а, б*), где дуги соответствуют операциям (этапам) проекта, а вес дуги обозначает время выполнения соответствующей операции. Найти наименьшее время выполнения проектов, критические пути и резервы времени для выполнения каждой операции.

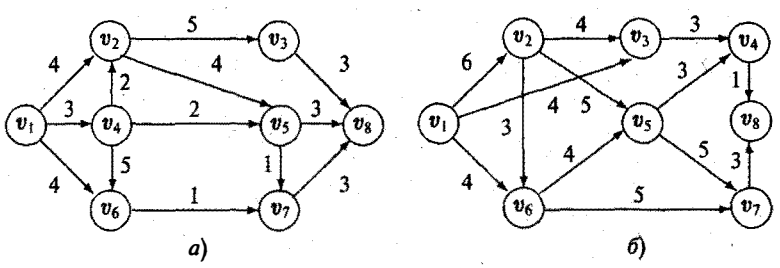


Рис. 39

81. Найти максимальные потоки и минимальные разрезы в транспортных сетях (*рис.* 40 *а, б*). Число рядом с дугой есть ее пропускная способность.

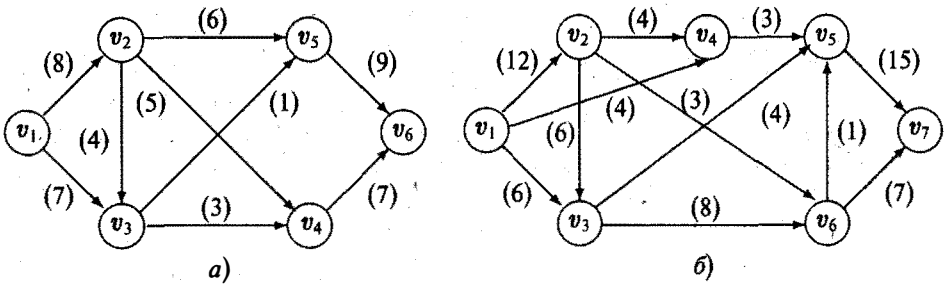


Рис. 40

82. Пусть имеется m неженатых мужчин, n незамужних женщин и k свах. У каждой свахи есть список своих клиентов; между любыми мужчиной и женщиной из этого списка сваха может устроить брак. Для i-й свахи число устроенных ею за год браков не превосходит числа b_i. Перевести задачу нахождения наибольшего числа браков, которые могут устроить свахи за год, в задачу нахождения максимального потока в некоторой сети.

Ответы

2. Изоморфны пары графов на рисунках б) и в).
3. Существует 11 простых графов с 4 вершинами и 34 — с 5 вершинами. **4.** 1) 1; 2) 2.

9. $\frac{1}{2}\sum_{i=1}^{n}\rho_i$ вершин и $\frac{1}{2}\sum_{i=1}^{n}(\rho_i^2-\rho_i)$ ребер.

Решение. Вершина реберного графа $L(G)$, отвечающая ребру v_iv_j в G, имеет степень $(\rho_i+\rho_j-2)$. В сумме $A=\sum(\rho_i+\rho_j-2)$, где суммирование ведется по всем ребрам G, степень каждой вершины ρ_i встречается ровно ρ_i раз. Поэтому удвоенное число ребер $L(G)$ равно $A=\sum\rho_i^2-2m$, где $2m=\sum\rho_i$ — удвоенное число ребер исходного графа G.

Другое решение. Ребра, инцидентные i-й вершине в графе G, образуют $C^2_{\rho_i}$ пар смежных ребер, каждой паре соответствует ребро в реберном графе. Суммируя C_{ρ_i} по всем i, вновь найдем общее число ребер $L(G)$.

10. *Достаточность* очевидна. *Необходимость*. Из предыдущей задачи следует: $\sum_{i=1}^{n}\rho_i=2n$; $\sum_{i=1}^{n}\rho_i^2=4n$, откуда $\sum_{i=1}^{n}(\rho_i-2)^2=0$, т. е. $\forall i\ \ \rho_i=2$. Связный регулярный граф степени 2 есть циклический граф.
14. Число ребер двудольного графа равно сумме степеней вершин любой его доли. **15.** Нет.
24. Пусть e — вектор-столбец, составленный из единиц. Тогда $Ae=ke$. **32.** n^2+n.
35. 1) а) $P_4(x_1,x_2,\ldots)=\frac{1}{24}\left(x_1^6+9x_1^2x_2^2+8x_3^2+6x_2^1x_4^1\right)$; б) $P_5(x_1,x_2,\ldots)=\frac{1}{120}\left(x_1^{10}+10x_1^4x_2^3+20x_1^1x_3^3+30x_2^1x_4^2+15x_1^2+20x_1^1x_3^1x_6^1+24x_5^2\right)$.

2) Положив вес ребра равным x, а вес *неребра*[13] равным 1, получим следующие производящие функции $\sum a_mx^m$, где m — число графов с m ребрами:
а) $\sum a_mx^m=\sum W(F)=P_4(1+x,1+x^2,\ldots)=1+x+2x^2+3x^3+2x^4+x^5+x^6$;
б) $\sum a_mx^m=\sum W(F)=P_5(1+x,1+x^2,\ldots)=1+x+2x^2+4x^3+6x^4+6x^5+6x^6+4x^7+2x^8+x^9+x^{10}$. **42.** 3 раза. См. задачу 41. **43.** 1) Да; 2) нет. **48.** 30 000. **50.** Рассмотрите

[13] Неребро — это отсутствующее в графе ребро между вершинами u и v.

вершину, смежную с концом самой длинной цепи. **53.** $r = \left[\frac{d+1}{2}\right]$. **55.** Нет. **62.** n^{n-1}. **63.** $k+1$. **66.** $1+\sum\limits_{k=1}^{s} kn_k - \sum\limits_{k=1}^{s} n_k$. Из общего количества вершин нужно вычесть количество внутренних вершин. **67.** $k \leqslant 4$. **70.** Нет. **71.** Если у планарного графа n вершин и m ребер, то выполняется неравенство $m \leqslant 3n - 6$. **72.** Индукция по числу вершин. **74.** $n/2^{n-1}$. **76.** В исходном графе существует эйлеров цикл. **77.** Перенеся доказательство теоремы Эйлера на случай графа из условия задачи, можно построить замкнутый путь, содержащий все дуги орграфа.

Глава LXXI

ПАРОСОЧЕТАНИЯ

Сначала приведем формулировки двух задач, первая из которых имеет практический характер, а вторая — скорее шуточный.

1. Пусть имеется несколько работников и несколько видов работ. Известно, какие работы каждый работник может выполнять. При каких условиях можно так распределить работы между работниками, чтобы каждый выполнял какую-либо работу (при этом на каждую работу назначается не более одного работника)?
2. Имеется множество юношей, каждый из которых знаком с некоторыми девушками. При каких условиях можно одновременно женить всех юношей так, чтобы каждый из них женился на знакомой ему девушке?

С точки зрения математики эти задачи не отличаются друг от друга, поскольку их математическая модель одна и та же: выделение совершенного паросочетания в двудольном графе. Что такое двудольный граф, читатель уже знает из предыдущей главы; что же до *совершенного паросочетания*, то это множество попарно не смежных ребер, покрывающих все вершины фиксированной доли двудольного графа. В двудольном графе две доли. Ребра соединяют вершины из одной доли с вершинами из другой. В задаче 1 такую долю составляют работники, а в задаче 2 — юноши. Вторая доля в этих задачах состоит из работ и девушек, соответственно. Наконец, произвольное ребро uv графа задачи 1 описывает ситуацию «работник u может выполнять работу v», а графа задачи 2 — «юноша u знаком с девушкой v».

В историю математики задача о существовании совершенного паросочетания в двудольном графе вошла под именем «задачи о свадьбах» (формулировка задачи 2 оказалась хорошо запоминающейся), а ответ к задаче дан Филипом Холлом в 1935 г.

В 20–50-х годах XX века независимо друг от друга были доказаны несколько теорем дискретной математики, носящих *минимаксный характер*: Форда—Фалкерсона, Кёнига—Эгервари, Дилворта (в другом написании — Дилуорса), а также Менгера. В каждой из этих теорем утверждалось, что максимум одной величины совпадает с минимумом другой величины. Как выяснилось впоследствии, указанные теоремы, а также теорема Холла эквивалентны друг другу: каждая из них может быть выведена из любой другой. Было также установлено, что эти теоремы являются проявлением принципа двойственности в линейном программировании.

В комбинаторном анализе и теории сложности вычислений (как и вообще в математике) *идея сведения* одной задачи к другой является важнейшей. Поэтому интересно показать, как внешне различные утверждения переходят друг в друга в результате построения некоторых дополнительных конструкций. Понимание

таких переходов и преобразований важно и для программистов: зная, как одна задача сводится к другой, можно алгоритм решения первой задачи преобразовать в алгоритм решения второй задачи.

В этой главе мы приводим наиболее простое из известных доказательств теоремы Холла, из теоремы Холла выводим теорему Кёнига—Эгервари, а из той, в свою очередь, теорему Дилворта. Здесь рассматриваются также некоторые приложения минимаксных теорем, в том числе теорема о возможности достраивания латинского прямоугольника до латинского квадрата (результат, полученный Маршаллом Холлом в 1945 г.) и теорема о *реберно-хроматическом числе* двудольного графа (наименьшем числе паросочетаний, на которое распадается множество ребер графа).

Заключительные параграфы главы посвящены алгоритмам решения задач о двудольных графах. Базовой здесь является задача нахождения наибольшего (по мощности) паросочетания в двудольном графе. Излагаемый алгоритм ее решения позволяет попутно найти наименьшее *вершинное покрытие* и наибольшее *независимое множество вершин*.

Вернемся теперь к задаче 1 и рассмотрим следующее ее обобщение.

3. Пусть имеется несколько работников и столько же видов работ. Известна стоимость выполнения каждым работником каждой работы. Требуется так распределить работы между работниками, чтобы суммарная стоимость выполнения работ была наименьшей.

Это — один из вариантов *задачи о назначениях*. Ее математическая формулировка: найти совершенное паросочетание наименьшего веса во взвешенном двудольном графе. Мы приводим алгоритм решения этой задачи, называемый *венгерским* — в честь Гарольда Куна, предложившего этот алгоритм в 1955 г.

§ 1. Теорема Холла

Введем некоторые определения и обозначения.

Паросочетанием в графе называют множество попарно несмежных ребер.

Двудольный граф G с фиксированным разбиением множества вершин на доли V_1 и V_2 будем обозначать $G(V_1, V_2)$.

Пусть $G(V_1, V_2)$ — двудольный граф. *Совершенным паросочетанием из* V_1 *в* V_2 называется паросочетание в G, покрывающее V_1 (т.е. для всякой вершины из V_1 найдется в паросочетании инцидентное ей ребро).

Пусть $A \subset V$ — подмножество вершин графа $G = \langle V, E\rangle$. Окружением множества A называют множество

$$\Gamma(A) = \bigcup_{v \in A} \Gamma(v) \setminus A,$$

где $\Gamma(v)$ — множество вершин, смежных с v.

Теорема 1 (Ф. Холл, 1935 г.). *Совершенное паросочетание из* V_1 *в* V_2 *в двудольном графе* $G(V_1, V_2)$ *существует тогда и только тогда, когда*

$$\forall A \subset V_1 \quad |\Gamma(A)| \geqslant |A|.$$

Теорема Холла дает решение следующей задачи, упомянутой в начале главы. Напомним ее формулировку.

Задача о свадьбах. *Имеется множество юношей, каждый из которых знаком с некоторыми девушками. При каких условиях можно одновременно женить всех юношей так, чтобы каждый из них женился на знакомой ему девушке?*

Действительно, построим двудольный граф $G(V_1, V_2)$, в котором V_1 есть множество юношей, а V_2 — соответственно множество девушек, а знакомые юноши и девушки соединены ребрами. Тогда одновременно женить всех юношей означает найти в данном графе совершенное паросочетание из V_1 в V_2. Ответ на вопрос задачи о свадьбах можно сформулировать так: *задача разрешима тогда и только тогда, когда любые k юношей из данного множества знакомы в совокупности не менее чем с k девушками.*

◀ Доказательство теоремы Холла. *Необходимость* очевидна. Действительно, условия

$$|A| = k \quad \text{и} \quad |\Gamma(A)| < k$$

означают: некоторые k вершин из V_1 смежны в совокупности менее чем с k вершинами из V_2 — поэтому нет попарно несмежных ребер в $G(V_1, V_2)$, покрывающих вершины даже из $A \subset V_1$, тем более нет совершеннного паросочетания из V_1 в V_2.

Достаточность будем доказывать индукцией по числу юношей. Пусть всего имеется m юношей. *База индукции* ($m = 1$) очевидна: уж одного-то юношу, знакомого хотя бы с одной девушкой, поженить можно.

Индукционный шаг. Пусть утверждение теоремы выполняется, если юношей меньше m, и докажем его для m юношей. Рассмотрим два возможных случая.

I. *Любые h юношей ($h < m$) в совокупности знакомы не менее чем с $h + 1$ девушками.* Если в этом случае мы поженим какого-то (любого) юношу на любой знакомой ему девушке, то для любых k оставшихся юношей общее число знакомых им (незамужних) девушек или не изменится, или уменьшится на единицу — значит, не превзойдет числа k. По предположению индукции оставшихся $m - 1$ юношей поженить можно.

II. *Некоторые h юношей ($1 \leqslant h < m$) знакомы в совокупности ровно с h девушками.* По предположению индукции их можно поженить. Попробуем устроить судьбу оставшихся $m - h$ юношей. Если какие-то k юношей из их числа знакомы в совокупности менее чем с k девушками, то вместе с указанными h юношами они составят группу из $k + h$ юношей, знакомых менее чем с $k + h$ девушками, что противоречит условию теоремы. Таким образом, и к оставшимся $m - h$ юношам можно применить предположение индукции. ▶

§ 2. Венгерская теорема

Пусть имеется двоичная матрица (т.е. состоящая из нулей и единиц). Единичные элементы этой матрицы, никакие два из которых не лежат в одной строке или одном столбце, назовем *независимыми*. Строки и столбцы матрицы, содержащие в совокупности все ее единицы, назовем *покрывающими линиями*.

Например, для матрицы

$$\begin{pmatrix} \boxed{1} & 1 & 1 & 0 & 0 & 0 \\ 1 & \boxed{1} & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & \boxed{1} & 0 & 0 & 0 \\ 1 & 0 & 0 & \boxed{1} & 1 & 1 \end{pmatrix}$$

можно указать четыре независимые единицы (они заключены в прямоугольники), и не больше, а минимальное по мощности множество покрывающих линий составляют первые три столбца и последняя строка.

Теорема 2 (Д. Кёниг—Э. Эгервари, 1931 г.). *Наибольшее число независимых единиц двоичной матрицы равно наименьшему числу покрывающих линий.*

Дадим сразу перевод условия теоремы на язык теории графов. Пусть в двоичной матрице $A = (a_{ij})$ m строк и n столбцов. Такая матрица задает двудольный граф $G(V_1, V_2)$, где $V_1 = \{u_1, \ldots, u_m\}$, $V_2 = \{v_1, \ldots, v_n\}$ и в графе есть ребро $u_i v_j$ тогда и только тогда, когда $a_{ij} = 1$. Матрицу A можно рассматривать как матрицу смежности двудольного графа $G(V_1, V_2)$. Независимые единицы матрицы соответствуют попарно несмежным ребрам, т. е. паросочетанию графа, а покрывающие линии — *вершинному покрытию* графа — множеству таких его вершин, что всякое ребро графа инцидентно хотя бы одной из них.

На рис. 1 представлен граф, соответствующий матрице из примера, приведенного выше. Ребра $u_1v_1, u_2v_2, u_4v_3, u_5v_4$ составляют максимальное паросочетание, а вершины v_1, v_2, v_3, u_5 образуют минимальное вершинное покрытие.

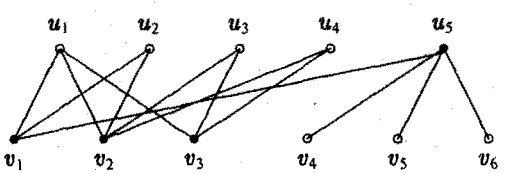


Рис. 1

Итак, венгерская теорема говорит о том, что *в двудольном графе наибольшая мощность паросочетания равна наименьшей мощности вершинного покрытия.*

◀ Доказательство венгерской теоремы. Обозначим через r наибольшее число независимых единиц, а через s наименьшее число покрывающих линий. Пусть все единицы матрицы находятся в некоторых x строках и y столбцах, причем $x + y = s$. Заметим, что если какие-то две единицы лежат (или не лежат) на одной линии, то это свойство сохранится и при любой перестановке строк или столбцов. (В графовой модели задачи перестановки линий сводятся к перенумерованию вершин в долях графа). Поэтому при указанных преобразованиях мощности интересующих нас множеств не меняются. Значит, можно считать, что все единицы

расположены в первых x строках и последних y столбцах, а матрица имеет следующий блочный вид:

$$\left(\begin{array}{c|c} A & B \\ \hline O & C \end{array}\right).$$

Рассмотрим двудольный граф $G'(V_1', V_2')$, который задается подматрицей A. В долях этого графа соответственно x и $n-y$ вершин. Если все единицы из каких-либо k строк матрицы A покрываются меньшим числом столбцов, то эти k строк можно заменить указанными столбцами и получить меньшее, чем $s = x+y$, число линий, покрывающих единицы матрицы, что приводит нас к противоречию с предположением о минимальности числа s. Таким образом, любые k вершин из доли V_1' смежны в совокупности не менее чем с k вершинами доли V_2' — выполнены условия теоремы Холла! Стало быть, в графе $G'(V_1', V_2')$ существует совершенное паросочетание из V_1' в V_2', то есть в подматрице A есть x независимых единиц.

Аналогичное рассуждение, примененное к подматрице C доказывает, что C содержит y независимых единиц.

Объединив независимые единицы из A и C, получим $x+y$ независимых единиц. Значит, максимальное число независимых единиц r не меньше числа $s = x+y$. С другой стороны, r независимых единиц нельзя покрыть менее чем r линиями (так как каждая линия покрывает не более одной независимой единицы), то есть r не больше s — минимального числа покрывающих линий. Итак, $r = s$. ▶

Терминологическое замечание. Наибольшее число независимых единиц двоичной матрицы называют ее *словарным рангом*.

§ 3. Теорема Дилворта

Сначала введем (или напомним) некоторые определения и обозначения. Пусть на некотором конечном множестве A введено *отношение порядка* $\prec$, т. е. отношение, обладающее свойствами *транзитивности* (состоящее в том, что если для элементов a, b и c множества A выполняются условия $a \prec b$ и $b \prec c$, то $a \prec c$) и *антисимметричности* (если $a \prec b$ и $b \prec a$, то $a = b$; другими словами, не существует двух различных элементов a и b, для которых одновременно выполняются условия $a \prec b$ и $b \prec a$). Всем известными примерами отношений порядка являются отношения $<, \leqslant, >, \geqslant$, заданные на любом подмножестве числовой прямой, и отношение делимости на множестве натуральных чисел. Множество вместе с введенным на нем отношением порядка называют *упорядоченным*.

Подмножество упорядоченного множества называют *цепью*, если в нем любые два элемента сравнимы по данному отношению, и *антицепью*, если никакие два различные элемента этого подмножества не сравнимы по данному отношению. Например, в множестве $\{2, 3, 6, 7, 55\}$, упорядоченном отношением делимости, есть цепи $\{2, 6\}$, $\{3, 6\}$ и антицепи $\{2, 3, 7, 55\}$, $\{6, 7, 55\}$. Одноэлементное множество — одновременно и цепь, и антицепь. Число элементов цепи (антицепи) будем называть ее *длиной*.

Очевидно, что любая цепь пересекается с любой антицепью не более чем по одному элементу. Отсюда следует, что если в упорядоченном множестве A имеется антицепь длины m, то число цепей, *покрывающих* A (т. е. их объединение есть A), не может быть меньше m.

Таким образом, *наименьшее количество цепей, покрывающих A, не меньше наибольшей длины антицепи.* Как показывает следующая теорема, на самом деле всегда имеет место равенство упомянутых величин.

Теорема 3 (Р. Дилворт, 1950 г.). *Минимальное число непересекающихся цепей, покрывающих упорядоченное множество, равно максимальной длине антицепи.*

◀ Обозначим наименьшее количество покрывающих цепей через X, а наибольшую длину антицепи через Y. Уже установлено, что $X \geqslant Y$. Покажем, что имеет место и неравенство $X \leqslant Y$.

Пусть $A = \{a_1, a_2, \ldots, a_n\}$ — упорядоченное множество с отношением $\prec$. Построим двудольный граф $G = \langle V_1 \cup V_2, E\rangle$, где

$$V_1 = \{x_1, x_2, \ldots, x_n\}, \quad V_2 = \{y_1, y_2, \ldots, y_n\} \quad \text{и} \quad x_i y_j \in E \iff (a_i \prec a_j, i \neq j).$$

В этом графе вершины x_i и y_i «представляют» элемент a_i исходного множества, а наличие ребра $x_i y_j$ свидетельствует о том, что i-й и j-й элементы множества A находятся в заданном отношении. Таким образом, построенный граф дает графическое представление (на то он и граф!) упорядоченного множества.

Возьмем наибольшее (по мощности) паросочетание в этом графе. Пусть его мощность равна k. Это паросочетание «порождает» $m = n - k$ цепей, покрывающих множество A. Покажем, как их получить. Сначала имеем n одноэлементных цепей, соответствующих n элементам A. Каждое ребро паросочетания позволяет объединить две цепи в одну (например, ребро $x_i y_j$ объединяет цепи $\ldots \to a_i$ и $a_j \to \ldots$ в цепь $\ldots \to a_i \to a_j \to \ldots$). В итоге и получим m цепей, которые не пересекаются и покрывают множество A. Отсюда следует, что *наименьшее количество покрывающих цепей X не больше m.*

Теперь рассмотрим какое-либо минимальное вершинное покрытие графа

$$T = \{x_{i_1}, x_{i_2}, \ldots, x_{i_r}, y_{j_1}, y_{j_2}, \ldots, y_{j_s}\}.$$

Покажем, что индексы всех вершин в указанном множестве различны, то есть $\forall\, t, l\ i_t \neq j_l$. Ведем рассуждение от противного. Предположим, что для каких-то t и l имеет место равенство $i_t = j_l = h$. Существует ребро вида $x_h y_c$, где $y_c \notin T$, так как в противном случае множество $T \setminus \{x_h\}$ также является вершинным покрытием, что противоречит минимальности T. Аналогично, существует и ребро вида $x_d y_h$ для некоторой вершины $x_d \notin T$. Для указанных c и d имеем $h \prec c$ и $d \prec h$, откуда в силу транзитивности $d \prec c$. Значит, в графе есть ребро $x_d y_c$, соединяющее вершины, не принадлежащие множеству T. Но тогда T не является вершинным покрытием — противоречие!

Таким образом, вершины множества T представляют в точности $r + s$ элементов множества A.

Венгерская теорема, напомним, говорит о том, что наибольшая мощность паросочетания равна минимальной мощности вершинного покрытия; в наших обозначениях получаем $k = r + s$. Заметим теперь, что элементы, не представленные в множестве T, попарно несравнимы, т.е. образуют антицепь, а число таких элементов равно

$$n - (r + s) = n - k = m.$$

Из существования антицепи мощности m вытекает, что *максимальная длина антицепи Y не меньше m*.

Итак, $X \leqslant m \leqslant Y$. Вспоминая, что $X \geqslant Y$, окончательно имеем: $X = m = Y$. ►

Замечание. Доказательство теоремы дает алгоритм нахождения минимального цепного покрытия, основанный на выделении наибольшего паросочетания в соответствующем двудольном графе.

Теорема (двойственная к теореме Дилворта)

Если в формулировке теоремы Дилворта заменить слово «цепи» на «антицепи», а «антицепь» на «цепь», то получим также верное утверждение, которое доказывается очень просто.

Теорема 4. *Минимальное число непересекающихся антицепей, покрывающих упорядоченное множество A, равно максимальной длине цепи.*

◄ Пусть m — максимальная длина цепи, а P — цепь длины m. Так как любая антицепь имеет с цепью P не более одного общего элемента, исходное множество A покрывает не менее m антицепей. Обозначим через $l(a)$ наибольшую длину цепи, начинающейся с элемента a (то есть элемент a предшествует всем другим элементам данной цепи). Очевидно, если $a \prec b$, то $l(a) > l(b)$. Таким образом, элементы a и b, для которых $l(a) = l(b)$, не сравнимы, а множество

$$A_i = \{a \mid l(a) = i\}$$

является антицепью. Осталось заметить, что в наших предположениях функция l на элементах множества P принимает все значения от 1 до m, и m — наибольшее значение функции l. Значит, имеем m непересекающихся антицепей $A_1, A_2, \ldots, A_m$, покрывающих упорядоченное множество A. ►

Из доказанной теоремы вытекает следующий интересный факт.

Теорема 5. *Если упорядоченное множество A содержит не менее $(p-1)(q-1)+1$ элементов, то в нем существует цепь длины не менее p или антицепь длины не менее q.*

◄ Если в множестве A нет цепи длины p, то есть максимальная длина цепи не превосходит $p-1$, то, согласно предыдущей теореме, найдется не более $p-1$ антицепей, покрывающих множество A. Если бы каждая из них содержала не более $q-1$ элементов, то в их объединении было бы не более $(p-1)(q-1)$ элементов, и они не покрывали бы множество A. Стало быть, длина некоторой антицепи не меньше числа q. ►

Замечание. Теорема 5 легко выводится и из самой теоремы Дилворта, но, как уже заметил читатель, она доказывается не столь просто, как двойственная теорема.

В последующих параграфах данной главы мы рассмотрим некоторые приложения минимаксных теорем.

§ 4. Совершенные паросочетания в регулярных двудольных графах

С помощью теоремы Холла получим результаты, связанные с темой параграфа.

Теорема 6. *В любом непустом регулярном двудольном графе $G(V_1, V_2)$ существует совершенное паросочетание.*

◄ Пусть степень каждой вершины графа равна $q > 0$. Возьмем произвольные k вершин первой доли $b_1, b_2, \ldots, b_k$ и смежные с ними вершины $g_1, g_2, \ldots, g_l$ второй доли и рассмотрим порожденный этими $k + l$ вершинами подграф исходного графа. В полученном графе степень любой вершины из первой доли равна q, а из второй — не больше q. Число ребер двудольного графа равно сумме степеней вершин любой из его долей. Поэтому

$$\sum_{i=1}^{k} \rho(b_i) = kq = \sum_{j=1}^{l} \rho(g_j) \leqslant lq,$$

откуда $l \geqslant k$. Таким образом, выполнены условия теоремы Холла о существовании в двудольном графе совершенного паросочетания. ►

Следствие. *Любой непустой регулярный двудольный граф распадается на совершенные паросочетания.*

◄ Пользуясь теоремой, будем последовательно одно за другим выделять в графе непересекающиеся паросочетания. ►

§ 5. Дважды стохастические матрицы

Числовая матрица называется *дважды стохастической*, если ее элементы неотрицательны, и в каждой строке и каждом столбце сумма элементов равна единице.

Сумма всех элементов такой матрицы равна, с одной стороны, числу ее строк, а, с другой стороны, числу столбцов. Значит, дважды стохастическая матрица является квадратной.

Подстановочная матрица состоит только из нулей и единиц, причем в каждой строке и каждом столбце содержится ровно одна единица. Ясно, что подстановочная матрица является дважды стохастической.

Подстановочным множеством матрицы называется множество ее элементов, содержащее по одному элементу из каждой строки и каждого столбца.

Теорема 7. *Всякая дважды стохастическая матрица $A = (a_{ij})$ имеет подстановочное множество, состоящее из ненулевых элементов.*

◄ Пусть матрица A имеет размер $n \times n$. Минимальное число линий, содержащих все ненулевые элементы матрицы A, равно n, поскольку сумма элементов всей матрицы равна n, а каждой линии — 1. Рассмотрим матрицу B, которая получается из матрицы A заменой ненулевых элементов на единицы. Минимальное число покрывающих линий матрицы B — такое же, как и для матрицы A, то есть n. По венгерской теореме в матрице B есть n независимых единиц. Эти единицы задают подстановочное множество матрицы A. ►

Очевидно, что подстановочное множество существует и для ненулевой матрицы из неотрицательных элементов с одинаковыми суммами по строкам и столбцам.

Теорема 8 (Г. Биркгоф, 1946 г.). *Всякая дважды стохастическая матрица представима в виде выпуклой комбинации подстановочных матриц.*

◄ Пусть P_1 — подстановочная матрица, порожденная подстановочным множеством M_1 из ненулевых элементов дважды стохастической матрицы A, а число c_1 — наименьший элемент в M_1. Тогда матрица $A - c_1P_1$ состоит из неотрицательных элементов и имеет одинаковые суммы по строкам и столбцам, и в ней ненулевых элементов меньше, чем у исходной матрицы. Повторяя данное преобразование, через конечное число шагов приходим к равенству

$$A = c_1P_1 + c_2P_2 + \ldots + c_kP_k, \qquad (*)$$

где $c_i > 0$ и P_i — подстановочная матрица для каждого i. Пусть матрица A имеет размер $n \times n$. Так как сумма всех элементов каждой из матриц $A, P_1, P_2, \ldots, P_k$ равна n, из $(*)$ следует: $c_1 + c_2 + \ldots + c_k = 1$. Таким образом, найденная линейная комбинация является выпуклой. ►

Замечание 1. Доказательство теоремы носит конструктивный характер. Описанный процесс получения разложения $(*)$ называют *алгоритмом Биркгофа*. Поскольку каждый шаг этого алгоритма дает требуемое значение по меньшей мере одному элементу матрицы A, а последний шаг — сразу n элементам матрицы, получаем неравенство $k \leqslant n^2 - n + 1$, где k — число подстановочных матриц, через которые линейно выражается дважды стохастическая матрица A. Известна и более точная оценка: $k \leqslant n^2 - 2n + 2$.

Замечание 2. Представим каждую дважды стохастическую матрицу размера $n \times n$ точкой в n^2-мерном пространстве. Геометрический смысл теоремы Биркгофа следующий: многогранник дважды стохастических матриц имеет своими вершинами подстановочные матрицы.

§ 6. Латинские прямоугольники

Матрица размера $m \times n$ называется *латинским прямоугольником*, если элементы каждой строки этой матрицы образуют перестановку чисел от 1 до n, и в каждом столбце все числа разные.

Очевидно, что в силу определения число строк латинского прямоугольника m не превосходит числа его столбцов n. В случае $m = n$, как легко догадаться, латинский прямоугольник называют *латинским квадратом*.

Например, матрицы

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \\ 4 & 1 & 5 & 3 & 2 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \\ 4 & 1 & 5 & 3 & 2 \\ 2 & 3 & 1 & 5 & 4 \\ 5 & 4 & 2 & 1 & 3 \end{pmatrix}$$

представляют собой латинский прямоугольник размером 3×5 и латинский квадрат 5×5. В этом примере квадрат получается из прямоугольника приписыванием двух строк. Возникает вопрос: *всегда ли латинский прямоугольник $m \times n$, где $m < n$, можно дополнить до латинского квадрата $n \times n$, приписыванием новых $n - m$ строк?* Оказывается, *всегда!* **Докажем этот факт.**

◄ Построим двудольный граф $G(V_1, V_2)$, в котором V_1 есть множество столбцов латинского прямоугольника размера $m \times n$, $V_2 = \{1, 2, \ldots, n\}$, а вершины $i \in V_1$ и $j \in V_2$ соединены ребром тогда и только тогда, когда в i-м столбце прямоугольника нет числа j.

Например, в случае прямоугольника из *рассмотренного примера* имеем граф, изображенный на рис. 2.

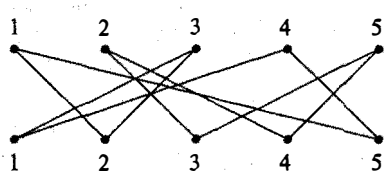


Рис. 2

Ясно, что степень любой вершины из доли V_1 равна $n - m$. С другой стороны, любое число j встречается в m строках исходного латинского прямоугольника m раз, значит, оно появляется в m столбцах и отсутствует в $n - m$ столбцах. Отсюда следует, что и степень любой вершины из V_2 также равна $n - m$.

Таким образом, двудольный граф $G(V_1, V_2)$ является непустым и регулярным. Как нам уже известно, такой граф распадается на совершенные паросочетания. Каждое совершенное паросочетание задает одну из новых строк латинского квадрата. ►

В рассмотренном выше примере переходу от прямоугольника к квадрату соответствует выделение в двудольном графе совершенных паросочетаний: $\{12, 23, 31, 45, 54\}$ и $\{15, 24, 32, 41, 53\}$.

В заключение, отметим, что латинский прямоугольник $m \times n$ (при $m \leqslant n$) существует. Действительно, сначала заполним произвольно первую строку, затем дополним прямоугольник $1 \times n$ до квадрата, и, наконец, вычеркнем любые $n - m$ строк.

§ 7. Реберная раскраска графов

Реберно-хроматическое число графа — это наименьшее число цветов, которыми можно раскрасить его ребра так, чтобы смежные ребра были разного цвета. Указанную раскраску будем называть *правильной*. Обозначают реберно-хроматическое число графа G через $\chi_e(G)$ (оставляя обозначение $\chi(G)$ для *хроматического* числа графа — наименьшего числа цветов для раскраски вершин графа, при которой смежные вершины имеют разный цвет).

Поскольку ребра одного цвета при правильной раскраске попарно не смежны, они составляют паросочетание. Таким образом, $\chi_e(G)$ — это наименьшее число паросочетаний, на которые распадается множество ребер графа G.

Обозначим через $\Delta(G)$ наибольшую степень вершины графа G. Все ребра, инцидентные фиксированной вершине графа, при правильной раскраске должны иметь разный цвет. Поэтому $\chi_e(G) \geqslant \Delta(G)$. Неожиданный факт обнаружил советский математик В. Г. Визинг:

Теорема 9 (В. Г. Визинг, 1964 г.). *Если в графе G нет петель, то*

$$\Delta(G) \leqslant \chi_e(G) \leqslant \Delta(G) + 1.$$

Вычислим реберно-хроматические числа некоторых стандартных графов.

Легко видеть, что для циклического графа C_n при $n \geqslant 2$ имеем:

$$\chi_e(C_n) = \begin{cases} 2, & \text{если } n \text{ четно;} \\ 3, & \text{если } n \text{ нечетно.} \end{cases}$$

В случае колеса W_n с $n \geqslant 4$ вершинами $\chi_e(W_n) = n - 1$. Более сложно проверяются соотношения для полного графа K_n с $n \geqslant 2$ вершинами:

$$\chi_e(K_n) = \begin{cases} n - 1, & \text{если } n \text{ четно;} \\ n, & \text{если } n \text{ нечетно.} \end{cases}$$

Если $\chi_e(K_n) = \Delta(G) = n - 1$, то каждая вершина графа инцидентна ребру (и притом одному) каждого цвета. Отсюда следует, что количество ребер одного цвета вдвое меньше общего числа вершин n, которое, стало быть, четно. Значит, при нечетном n $\chi_e(K_n) > n-1$ и, в силу теоремы Визинга, $\chi_e(K_n) = n$. Приведем, тем не менее,

Пример правильной раскраски ребер K_n при нечетном n

Изобразим K_n правильным n-угольником с диагоналями. Выберем для каждой его стороны свой цвет. Любая диагональ будет параллельна какой-то стороне, в цвет этой стороны и выкрасим диагональ. Поскольку смежные отрезки (стороны и диагонали) не параллельны, полученная раскраска будет правильной.

В случае четного n правильную раскраску в $n - 1$ цветов можно получить следующим образом. Сначала раскрасим правильным образом подграф K_{n-1}. Вершину, не вошедшую в данный подграф, обозначим v. Для каждой вершины u подграфа будем иметь $n-2$ инцидентных ребер, покрашенных во все цвета, кроме цвета противоположной (в $n-1$-угольнике) стороны. Используем этот цвет для покраски ребра uv. В результате любые два смежных ребра графа будут разного цвета.

Обратимся теперь к регулярному двудольному графу $K_{m,n}$.

Без потери общности предположим, что $m \leqslant n$. Составим латинский прямоугольник $A = (a_{ij})$ размера $m \times n$ и будем считать, что a_{ij} обозначает цвет ребра, соединяющего i-ю вершины первой доли с j-й вершиной второй доли. При этом получится правильная раскраска $K_{m,n}$ в n цветов. Поскольку $\chi_e(K_{m,n}) \geqslant \Delta(K_{m,n}) = n$, делаем вывод: $\chi_e(K_{m,n}) = n$.

В общем случае, $\chi_e(K_{m,n}) = \max\{m, n\}$. Этот результат можно существенно усилить.

Теорема 10. *Пусть G — двудольный граф. Тогда $\chi_e(G) = \Delta(G)$.*

◄ Положим $k = \Delta(G)$. Поскольку $\chi_e(G) \geqslant k$, достаточно указать способ правильной раскраски графа G в k цветов.

Покажем, как расширить граф G до регулярного двудольного графа, в котором степени всех вершин равны k.

Рассмотрим дизъюнктное объединение k экземпляров графа G, считая при этом, что первые доли указанных графов объединяются в первую долю нового графа, а вторые доли — во вторую. Возьмем произвольную вершину u первой доли исходного графа, степень которой меньше k. Введем во вторую долю строящегося графа $k - \rho(u)$ новых вершин, соединив каждую из них со всеми k «клонами» вершины u. Теперь степень клонов u станет равной k. Новые вершины также имеют эту степень. Затем аналогично поступим с вершинами второй доли, степень которых меньше k. В результате получится регулярный двудольный граф G', имеющий подграфом исходный граф G.

Результаты § 4 показывают, что граф G' распадается на k совершенных паросочетаний. Покрасив ребра каждого паросочетания в свой цвет, получим правильную раскраску графа G', а заодно и графа G. ►

Заключительные параграфы данной главы посвящены алгоритмам решения различных задач, связанных с паросочетаниями.

§ 8. Теорема Бёржа

Пусть M — паросочетание в графе G (не обязательно двудольном). Ребра, входящие в M, назовем черными, а остальные ребра графа — белыми. Простая цепь — *чередующаяся* (*относительно* M), если любые два соседних ребра в этой цепи разного цвета. Вершину, покрываемую некоторым ребром из M, назовем *насыщенной* (*относительно* M); в противном случае вершина — *ненасыщенная* (или *свободная*) (*относительно* M).

Если в графе имеется чередующаяся цепь, соединяющая две ненасыщенные вершины, то легко получить новое паросочетание, в котором на одно ребро больше, чем в M: достаточно поменять цвета ребер указанной цепи. Поэтому такую цепь называют *увеличивающей относительно* M, или M*-увеличивающей*. Очевидно теперь, что относительно наибольшего паросочетания увеличивающей цепи не существует. Оказывается, верно и обратное.

Теорема 11 (К. Бёрж, 1957 г.). *Паросочетание M в графе G является наибольшим тогда и только тогда, когда в G не существует увеличивающей относительно M цепи.*

◄ *Необходимость* уже доказана. Убедимся в *достаточности.*

Пусть паросочетание M не допускает увеличивающей относительно себя цепи, а M' — некоторое наибольшее паросочетание. Рассмотрим подграф графа G, образованный ребрами из симметрической разности $M \triangle M'$. В нем степень каждой вершины не превосходит 2, в силу чего этот подграф распадается на циклы

и простые цепи. Поскольку в цикле ребра из M и M' чередуются, цикл имеет четную длину. Чередование происходит и в каждой цепи. Цепь не является увеличивающей ни относительно M (по условию теоремы), ни относительно M' (наибольшего паросочетания). Отсюда вытекает, что длина цепи является четным числом. Стало быть, в симметрической разности $M \triangle M'$ поровну ребер из M и M', а множества M и M' равномощны, то есть M, как и M', является наибольшим паросочетанием. ▶

§ 9. Нахождение наибольшего паросочетания

Теорема Бёржа обосновывает корректность следующего способа нахождения наибольшего паросочетания в графе.

I. Построить произвольное паросочетание M.

II. Искать M-увеличивающую цепь.

III. Если такая цепь P найдена, то заменить M на $M \triangle P$ и перейти к шагу II. В противном случае закончить работу (текущее паросочетание M является наибольшим).

В случае *двудольного графа* поиск M-увеличивающих цепей происходит довольно просто. Используем для этого механизм пометок.

Алгоритм $\mathcal{A}$

1. Построить какое-нибудь паросочетание M.
2. Свободные относительно M вершины из доли V_1 пометить нулем, остальные вершины считаются непомеченными.
3. Для каждой помеченной на предыдущем шаге вершины $v_i \in V_1$ пометить ее номером i все непомеченные вершины из V_2, которые соединяются с v_i белыми ребрами.

   Если при этом окажется помеченной свободная вершина, то M-увеличивающая цепь P найдена; она восстанавливается по меткам, начиная с указанной вершины: метка вершины есть номер очередной вершины P. Увеличивающую цепь перекрасить (т.е. заменить M на $M \triangle P$) и перейти к шагу 2.

   Если же новых пометок на этом шаге не возникает, перейти к шагу 5.
4. Для каждой помеченной на предыдущем шаге вершины $u_j \in V_2$ пометить ее номером j непомеченную вершину из V_1, которая соединяется с u_j черным ребром. Если новых пометок на этом шаге не возникает, перейти к шагу 5, иначе вернуться к шагу 3.
5. Текущее паросочетание M является наибольшим. Конец работы.

Проиллюстрируем работу изложенного алгоритма на следующем примере.

Для графа на рис. 3 текущее паросочетание M состоит из ребер, изображенных двойными линиями. Напомним, что ребра из M мы называем черными, а остальные ребра графа — белыми. Свободные вершины изображены двойными кружками.

В доле V_1 только одна свободная вершина — с номером 2; она помечается нулем (пометки — это числа в прямоугольниках). Белые ребра (изображены тонкими линиями) соединяют эту вершину с вершинами 8 и 12, которые получают пометку 2.

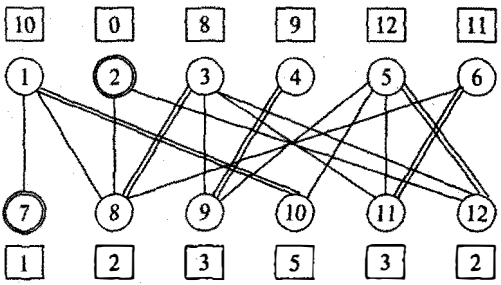


Рис. 3

Черное ребро 8–3 дает пометку 8 вершине 3; черное ребро 12–5 дает пометку 12 вершине 5.

Из вершины 3 к непомеченным вершинам ведут два белых ребра, и их другие концы — вершины 9 и 11 — получают пометку 3. Аналогично, у вершины 10 возникает пометка 5.

Далее помечаются вершины из первой доли: 4, 1 и 6.

Наконец, удается пометить свободную вершину 7 из второй доли — номером 1. Идя по пометкам, начиная с этой вершины, находим M-увеличивающую цепь: 7–1–10–5–12–2. Перекрасим ее ребра и получим новое (более мощное, чем ранее) паросочетание (рис. 4).

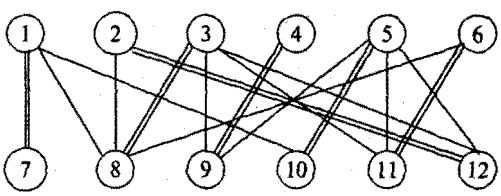


Рис. 4

Построенное паросочетание является совершенным (оно покрывает все вершины графа), значит, и наибольшим.

Замечание 1. Алгоритм $\mathcal{A}$ является, по сути, «проекцией» алгоритма Форда—Фалкерсона нахождения максимального потока в сети (см. § 16 гл. LXX).

Подробно поясним этот тезис. Превратим двудольный граф $G(V_1, V_2)$ в транспортную сеть следующим образом:

- ориентируем каждое ребро $u_i v_j$ в направлении от V_1 к V_2;
- к множеству вершин графа добавим источник a и сток b;
- проведем дуги из источника a ко всем вершинам из V_1;
- из каждой вершины доли V_2 проведем дугу к стоку b;
- положим пропускные способности всех дуг равными единице.

Существует взаимно однозначное соответствие между допустимыми целочисленными потоками в этой сети и паросочетаниями исходного двудольного графа: по каждой дуге сети, соответствующей ребру $G(V_1, V_2)$, входящему (не входящему) в паросочетание, идет единичный (соответственно нулевой) поток. При этом

максимальному (по включению) паросочетанию будет отвечать полный поток. M-увеличивающей цепи

$$u_\alpha - v_\beta - u_\gamma - \ldots - v_\omega \tag{1}$$

соответствует цепь транспортной сети:

$$a \to u_\alpha \to v_\beta \leftarrow u_\gamma \to \ldots \to v_\omega \to b. \tag{2}$$

Перекраска ребер в цепи (1) суть увеличение потока вдоль цепи (2). Например, ребро $u_\alpha - v_\beta$ было белым, а стало черным, соответственно поток по дуге $u_\alpha \to v_\beta$ из нулевого превратился в единичный; следующее ребро цепи $u_\gamma - v_\beta$ из черного стало белым, а поток по дуге $u_\alpha \to v_\beta$ стал нулевым.

Замечание 2. Несложно оценить трудоемкость данного алгоритма. Пусть n — число вершин в доле V_1 (без ограничения общности можно считать, что в V_1 вершин не более, чем в V_2), а m — число ребер графа $G(V_1, V_2)$. Тогда при работе алгоритма будет выполнено не более n итераций (итерацию составляют шаги 2, 3 и 4), а на каждой итерации порядка $O(m)$ действий. Стало быть, общее число операций есть $O(nm)$. Если $|V_1| = |V_2| = n$, то имеем оценку трудоемкости, зависящую только от числа вершин: $O(n^3)$.

Замечание 3. Разработаны весьма изощренные алгоритмы нахождения наибольшего паросочетания в произвольном графе (в общем случае, не двудольном), также имеющие трудоемкость $O(n^3)$, где n — количество вершин графа.

§ 10. Нахождение наименьшего вершинного покрытия

Вновь ограничимся случаем двудольного графа.

Оказывается, изложенный выше алгоритм $\mathcal{A}$ нахождения наибольшего паросочетания заодно позволяет обнаружить и наименьшее вершинное покрытие.

Пусть $A \subset V_1$ и $B \subset V_2$ — множества помеченных вершин обеих долей графа $G(V_1, V_2)$ по окончании работы алгоритма $\mathcal{A}$. Обозначим $\overline{A} = V_1 \setminus A$.

Теорема 12. *Множество $\overline{A} \cup B$ является минимальным вершинным покрытием графа $G(V_1, V_2)$.*

◄ Пусть M — наибольшее паросочетание в графе $G(V_1, V_2)$, построенное в результате работы алгоритма $\mathcal{A}$. Ребра, входящие в M, как и ранее, мы называем черными; а остальные ребра графа для нас белые.

Доказательство теоремы разобьем на три этапа.

1. Докажем, что *концы любого черного ребра либо оба помечены, либо оба не помечены.*

   Возьмем произвольное черное ребро uv, где $u \in V_1$, $v \in V_2$.

   Если вершина v помечена, то на шаге 4 алгоритма $\mathcal{A}$ пометку получит и вершина u.

   Рассмотрим теперь случай, когда вершина v не помечена. Тогда непомеченной будет и вершина u. Действительно, u, будучи насыщенной вершиной,

не помечается на 2-м шаге. Но и на 4-м шаге вершина u не получает пометку, так как она инцидентна единственному черному ребру — uv, а другой его конец не помечен.

Утверждение доказано.

2. Проверим, что $C = \bar{A} \cup B$ — *вершинное покрытие графа.*
Возьмем в графе $G(V_1, V_2)$ произвольное ребро $e = uv$, где $u \in V_1$, $v \in V_2$. Докажем, что $u \notin A$ или $v \in B$.
Если это не так, то $u \in A$ (то есть u — помеченная вершина) и $v \notin B$ (v — непомеченная вершина). Тогда в силу утверждения 1 ребро e не может быть черным. Но оно и не белое, поскольку при помеченной вершине u и белом ребре uv на 3-м шаге алгоритма $\mathcal{A}$ вершина v получила бы пометку. Противоречие получено.
3. Заметим, что (благодаря утверждению 1)
   1) количество черных ребер с помеченными концами равно $|B|$ — количеству помеченных вершин из доли V_2 (каждая из них инцидентна одному черному ребру);
   2) количество черных ребер с непомеченными концами равно $|\bar{A}|$ — количеству непомеченных вершин из доли V_1 (любая такая вершина насыщенная, и из нее также исходит ровно одно черное ребро).

Таким образом,

$$|M| = |B| + |\bar{A}| = |\bar{A} \cup B|,$$

то есть вершинное покрытие $\bar{A} \cup B$ равномощно наибольшему паросочетанию. В силу венгерской теоремы это означает минимальность вершинного покрытия. ▶

Как отмечалось в § 3, дополнение к наименьшему вершинному покрытию графа является его наибольшим независимым множеством вершин. Значит, множество $A \cup \bar{B}$ — наибольшее независимое. Стало быть, алгоритм $\mathcal{A}$ (имеющий, как мы выяснили, полиномиальную трудоемкость) позволяет наряду с наибольшим паросочетанием в двудольном графе найти также наименьшее вершинное покрытие и наибольшее независимое множество. Известно, что задачи определения наименьшего вершинного покрытия и наибольшего независимого множества для *произвольного графа* являются NP-полными, другими словами, для них нет эффективных алгоритмов решения (по крайней мере, они пока не известны науке). Очень важно, что для двудольных графов, возникающих во многих практических задачах, полиномиальные алгоритмы решения указанных задач существуют!

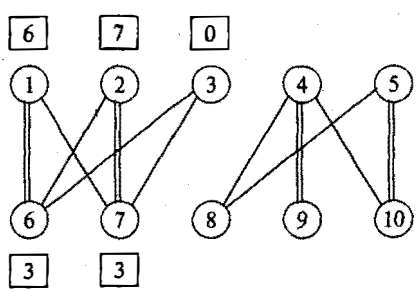


Рис. 5

Пример. На рис. 5 изображен граф, в котором выделено наибольшее паросочетание и расставлены пометки, возникающие по окончании работы алгоритма $\mathcal{A}$.

Имеем $A = \{1, 2, 3\}$; $B = \{6, 7\}$. Значит, вершины 4, 5, 6 и 7 образуют минимальное вершинное покрытие, а вершины 1, 2, 3, 8, 9, 10 — наибольшее независимое множество.

§ 11. Венгерский алгоритм

Пусть $G(V_1, V_2)$ — взвешенный полный двудольный граф $K_{n,n}$ с матрицей весов ребер $C = (c_{ij})$, где $c_{ij} \geqslant 0$ есть вес ребра, соединяющего i-ю вершину доли V_1 с j-й вершиной доли V_2.

В *задаче о назначениях* требуется найти совершенное паросочетание минимального веса (ниже будем называть такое паросочетание *оптимальным*). Название задачи объясняется следующей ее трактовкой. Пусть u_i — i-й работник, v_j — j-я работа, а c_{ij} — стоимость выполнения i-м работником j-й работы. Тогда совершенное паросочетание наименьшего веса описывает такое распределение работ между работниками (*назначение* работников на работы), при котором каждый работник выполняет ровно одну работу, а суммарная стоимость выполнения работ минимальна.

Заметим, что если к весам всех ребер, инцидентных некоторой фиксированной вершине, прибавить одно и то же число (не обязательно положительное), то упорядоченность совершенных паросочетаний графа по их весу не изменится, поскольку каждое такое паросочетание содержит ровно одно ребро с измененным весом. Назовем такую операцию *приведением*. Для матрицы весов приведение означает прибавление константы ко всем элементам некоторого столбца или строки.

С помощью операций приведения легко свести задачу к графу, в котором каждая вершина инцидентна некоторому ребру нулевого веса (будем называть такие ребра *нулевыми*), и при этом веса всех ребер остаются неотрицательными числами. Если в таком графе существует совершенное паросочетание нулевого веса (в матрице весов ему соответствуют n независимых нулей), очевидно, оно и будет решением задачи. Основная идея излагаемого ниже *венгерского алгоритма* (Г. Кун, 1955 г.) состоит в том, что в результате поиска M-увеличивающей цепи в $G(V_1, V_2)$, где M — паросочетание из нулевых ребер, удается найти такие операции приведения, в результате которых количество нулевых ребер увеличивается. В некоторый момент возникает граф, в котором есть совершенное паросочетание нулевого веса.

Алгоритм $\mathcal{B}$

1. Из каждой строки матрицы C вычесть ее минимальный элемент. Так же поступить со столбцами.
2. Пусть N — множество нулевых ребер текущего графа $G = G(V_1, V_2)$ (с матрицей весов C). Найти в графе $G' = \langle V_1 \cup V_2, N \rangle$ с помощью алгоритма $\mathcal{A}$ наибольшее паросочетание M, беря в качестве начального паросочетания текущее наибольшее паросочетание (если шаг 2 алгоритма $\mathcal{B}$ выполняется не впервые). Если найденное паросочетание M — совершенное, то конец работы.
3. Пусть $A \subset V_1$ и $B \subset V_2$ — множества помеченных вершин обеих долей графа G по окончании работы алгоритма $\mathcal{A}$ (напомним, что пометки расставляются с целью найти M-увеличивающую цепь). Вычислить d — наименьший вес ребра, соединяющего помеченную вершину из V_1 с непомеченной вершиной из V_2. Из всех строк, отвечающих вершинам из A, вычесть число d. Ко всем столбцам, отвечающим вершинам из B, прибавить число d. Перейти к шагу 1.

Обоснуем *корректность* алгоритма $\mathcal{B}$. Во-первых, применяемые в нем операции приведения не меняют множества оптимальных паросочетаний. Во-вторых,

алгоритм заканчивает работу, когда обнаруживает в двудольном графе с неотрицательными весами ребер совершенное паросочетание нулевого веса. Осталось убедиться, что такой момент непременно наступит.

После первого шага работы алгоритма получаем граф, в котором каждая вершина инцидентна хотя бы одному нулевому ребру. Поэтому после шага 2 все вершины из V_1, не покрытые текущим паросочетанием, помечены. Значит, на шаге 3 множество A непусто. С другой стороны, если найденное в результате выполнения шага 2 паросочетание не является совершенным, это означает, что не все вершины из V_2 удалось пометить — значит, непусто и множество $\overline{B} = V_2 \setminus B$. Вес любого ребра, соединяющего вершину i из A с вершиной j из $\overline{B}$, положителен, так как в противном случае по алгоритму $\mathcal{A}$ вершина j должна была бы получить пометку. Таким образом, $d > 0$.

Посмотрим, что происходит с весами ребер на шаге 3.

Веса ребер из $G(\overline{A}, \overline{B})$ не меняются.

Ребра из подграфа $G(A, B)$ сохраняют свой вес, поскольку первоначальное вычитание числа d компенсируется последующим его прибавлением.

Вес каждого ребра из $G(\overline{A}, B)$ увеличивается на d.

Поскольку $d > 0$ — наименьший вес ребра в графе $G(A, \overline{B})$, после шага 3 в этом подграфе появится хотя бы одно нулевое ребро.

Значит, после шага 3 веса всех ребер остаются неотрицательными. Как было отмечено в предыдущем параграфе, концы любого черного ребра либо оба помечены, либо нет. В первом случае ребро входит в $G(A, B)$, во втором — в $G(\overline{A}, \overline{B})$. Таким образом, после шага 3 ребра текущего максимального паросочетания M остаются нулевыми. С другой стороны, ребра из $G(A, \overline{B})$, ставшие нулевыми, при последующем выполнении шага 2 расширяют множество B. Поэтому на некоторой итерации будут найдены M-увеличивающая цепь и новое, более мощное, паросочетание M. Рано или поздно в текущем графе будет существовать совершенное паросочетание из нулевых ребер.

Проиллюстрируем работу алгоритма $\mathcal{B}$ следующим *примером*.

Пусть веса ребер графа $K_{4,4}$ задаются матрицей

$$\begin{pmatrix} 1 & 4 & 4 & 3 \\ 2 & 7 & 6 & 8 \\ 4 & 7 & 5 & 6 \\ 2 & 5 & 1 & 1 \end{pmatrix}.$$

После вычитания минимальных элементов строк и столбцов последовательно получим матрицы

$$\begin{pmatrix} 0 & 3 & 3 & 2 \\ 0 & 5 & 4 & 6 \\ 0 & 3 & 1 & 2 \\ 1 & 4 & 0 & 0 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} 0 & 0 & 3 & 2 \\ 0 & 2 & 4 & 6 \\ 0 & 0 & 1 & 2 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

Построим граф G', образованный нулевыми ребрами (текущего) графа G (рис. 6).

Выделим в нем максимальное по включению паросочетание (его ребра изобразим двойными линиями) и осуществим процесс расстановки пометок согласно алгоритму $\mathcal{A}$. Пометки последовательно получают вершины 2, 5, 1, 6, 3 (рис. 7).

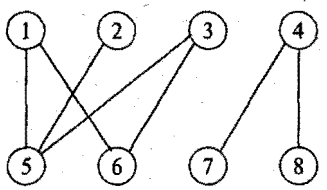


Рис. 6

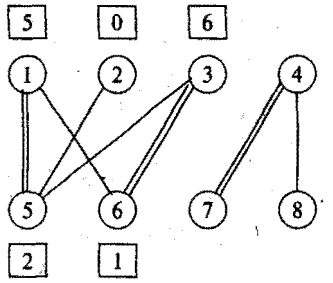


Рис. 7

Таким образом, множество помеченных вершин из V_1 и V_2 есть $A = \{1, 2, 3\}$ и $B = \{5, 6\}$ соответственно. Теперь в матрице весов подграфа $G(A, \bar{B})$, образованной тремя верхними строками и двумя последними столбцами матрицы C, находим наименьший элемент: $d = 1$. В результате вычитания числа d из строк, отвечающих A, а затем прибавления d к столбцам, отвечающим B, возникают матрицы

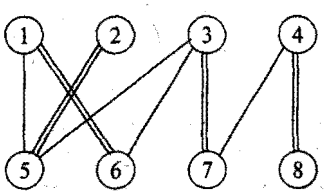


Рис. 8

$$\begin{pmatrix} -1 & -1 & 2 & 1 \\ -1 & 1 & 3 & 5 \\ -1 & -1 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \text{ и } \begin{pmatrix} 0 & 0 & 2 & 1 \\ 0 & 2 & 3 & 5 \\ 0 & 0 & 0 & 1 \\ 2 & 2 & 0 & 0 \end{pmatrix}.$$

Возвращаемся к шагу 2. Теперь имеем граф G', изображенный на рис. 8, в котором существует совершенное паросочетание. Итак, оптимальное паросочетание состоит из ребер 1–6, 2–5, 3–7, 4–8, а его вес, как легко подсчитать, равен 12 (разумеется, в исходном графе).

В заключение — несколько замечаний.

Замечание 1. Трудоемкость алгоритма $\mathcal{B}$ оценивается как $O(n^4)$ операций. Известны модификации венгерского алгоритма, имеющие трудоемкость $O(n^3)$.

Замечание 2. Часто рассматривают также задачу нахождения во взвешенном двудольном графе совершенного паросочетания *наибольшего* веса. Читателю предлагается подумать над тем, как преобразовать матрицу весов исходного графа, чтобы перейти к графу, в котором оптимальное паросочетание (наименьшего веса) соответствует паросочетанию наибольшего веса в исходном графе.

§ 12. Задача о назначениях на узкое место

Пусть на некотором конвейере (поточной линии) имеется n рабочих мест. Мастер должен расставить по этим местам n работников. Известна производительность труда c_{ij} i-го работника на j-м месте. Производительность конвейера определяется минимальной производительностью занятых на нем работников. Рабочее место, на котором реализуется минимальная производительность при заданной расстановке работников (другими словами, при заданном *назначении*), и есть *узкое* место этого назначения.

Нужно помочь мастеру «сделать узкое место как можно шире»: найти такое распределение работников по рабочим местам, при котором скорость конвейера (т. е. минимальная производительность занятых работников) будет максимальной.

На языке теории графов задача состоит в *выделении во взвешенном двудольном графе такого совершенного паросочетания, в котором наименьший вес ребра будет наибольшим.*

Другими словами, требуется найти такое наибольшее число f, при котором в графе существует совершенное паросочетание M, составленное из ребер, чей вес не меньше f (паросочетание M и будет искомым).

Это можно сделать с помощью дихотомического поиска. Суть его в том, что на каждом шаге множество, содержащее искомое значение, сокращается вдвое. В описываемом ниже алгоритме индексы a и b задают границы указанного множества.

Алгоритм $\mathcal{C}$

1. Отсортировать ребра по возрастанию веса, получив массив $w_1, w_2, \ldots, w_{n^2}$.
2. Положить $a = 1$, $b = n^2 - n + 2$.
3. Если $a = b - 1$, перейти к шагу 6.
4. Положить $k = \left[\frac{a+b}{2}\right]$, $f = w_k$.
5. С помощью алгоритма $\mathcal{A}$ искать совершенное паросочетание в подграфе G' графа G, образованном ребрами, чей вес не меньше f.
   Если такое паросочетание найдено, то объявить его текущим и положить $a = k$. В противном случае положить $b = k$.
   Перейти к шагу 3.
6. Текущее паросочетание является оптимальным. Конец работы.

Нетрудно оценить число операций при выполнении алгоритма $\mathcal{C}$. Наиболее трудоемкий шаг 5 выполняется примерно $\log_2(n^2 - n + 1) = O(\log_2 n)$ раз. Поэтому общая трудоемкость — $O(\log_2 n \cdot n^3)$ операций. В случае использования вместо $\mathcal{A}$ более эффективного алгоритма трудоемкость алгоритма $\mathcal{C}$ соответственно понизится.

Упражнения

1. *Перманент* квадратной матрицы есть сумма всевозможных произведений ее элементов, взятых по одному из каждой строки и каждого столбца. Пусть A — двоичная матрица размера $n \times n$. Доказать, что ее перманент равен нулю тогда и только тогда, когда в A существует i строк и j столбцов, где $i + j \geqslant n + 1$, на пересечении которых стоят одни нули.
2. В некотором районе, состоящем из нескольких деревень, число женихов равно числу невест. В каждой деревне общее число женихов и невест не больше половины общего их числа. Доказать: можно всех переженить так, что в каждой паре жених и невеста будут из разных деревень.
3. На танцевальном вечере каждый юноша знаком с k девушками, а каждая девушка знакома с k юношами. Доказать, что можно провести k (медленных) танцев так, чтобы каждый участник вечера станцевал со всеми своими знакомыми (противоположного пола).
4. На шахматной доске пометили 16 из 64 клеток так, что на каждой вертикали и горизонтали оказалось по две помеченные клетки. Доказать, что на помеченных клетках

можно расставить 8 черных и 8 белых фигур так, чтобы на каждой вертикали и каждой горизонтали стояло по одной белой и одной черной фигуре.

5. Вуз посылает 8 юношей и 8 девушек на стажировку по восьми специальностям в 8 зарубежных университетов, причем каждый университет принимает по два человека и учит их двум разным специальностям, и каждой из восьми специальностей учат два университета. Всегда ли можно так распределить студентов, чтобы в каждом университете стажировались юноша и девушка, и при этом как юноши, так и девушки обучались (в совокупности) по всем восьми специальностям?

6. Выполняя домашнее задание, каждый студент группы решил по 4 задачи. Известно, что каждая задача была решена четырьмя студентами. Доказать, что можно организовать разбор задач так, чтобы каждый студент рассказал решение ровно одной задачи и чтобы все задачи были разобраны (по одному разу).

7. Имеются 27 карточек с числами от 1 до 27. Двое показывают следующий фокус. Первый получает четыре карточки, выбранные случайным образом. Одну из них он убирает, а три оставшиеся выкладывает в ряд. Второй должен назвать спрятанную карточку. Могут ли участники договориться так, чтобы по выложенным карточкам можно было узнать спрятанную?

8. Пусть в двудольном графе $G(V_1, V_2)$ степень любой вершины из V_1 не меньше k, а степень любой вершины из V_2 не больше k, где k — некоторое натуральное число. Доказать, что в этом графе существует совершенное паросочетание.

9. **[Одномерная теорема Хелли.]** *Если отрезки прямой попарно пересекаются, то найдется точка, принадлежащая всем отрезкам одновременно.* Доказать.

10. На прямой расположено $mn + 1$ отрезков. Доказать, что из них можно выбрать $m + 1$ попарно непересекающихся отрезков или $n + 1$ отрезков, имеющих общую точку.

11. Доказать, что в последовательности из $n^2 + 1$ различных действительных чисел найдется монотонная подпоследовательность длины $n + 1$.

12. Имеется множество юношей, каждый из которых знаком с некоторыми девушками. Две свахи знают, кто с кем знаком. Первая сваха заявляет: «Я могу одновременно женить всех брюнетов так, чтобы каждый из них женился на знакомой ему девушке!» Вторая сваха говорит: «А я могу устроить судьбу всех блондинок: каждая сможет выйти замуж за знакомого юношу!» Этот диалог услышал любитель математики, который сказал: «В таком случае я могу сделать и то, и другое!» Прав ли он?

13. Найти наибольшее паросочетание и наименьшее вершинное покрытие в двудольных графах с матрицами смежности:

а) $\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$; б) $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$;

в) $\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$.

14. Решить задачу о назначениях для двудольных графов с матрицами весов:

а) $\begin{pmatrix} 7 & 2 & 1 & 9 & 4 \\ 9 & 6 & 9 & 5 & 5 \\ 3 & 8 & 3 & 1 & 8 \\ 7 & 9 & 4 & 2 & 2 \\ 8 & 4 & 7 & 4 & 8 \end{pmatrix}$; б) $\begin{pmatrix} 1 & 3 & 2 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \\ 1 & 3 & 2 & 5 & 4 \\ 5 & 2 & 1 & 4 & 3 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$; в) $\begin{pmatrix} 7 & 4 & \infty & 6 & 4 & 6 \\ 5 & 2 & 8 & 0 & \infty & 4 \\ 4 & \infty & 2 & 5 & 6 & 5 \\ 8 & 0 & 7 & \infty & 3 & 1 \\ 0 & 1 & 0 & \infty & 0 & 0 \\ \infty & \infty & 2 & 4 & 1 & 7 \end{pmatrix}$.

15. Найти максимальные по весу совершенные паросочетания в двудольных графах с матрицами весов:

а) $\begin{pmatrix} 7 & 2 & 1 & 9 & 4 \\ 9 & 6 & 9 & 5 & 5 \\ 3 & 8 & 3 & 1 & 8 \\ 7 & 9 & 4 & 2 & 2 \\ 8 & 4 & 7 & 4 & 8 \end{pmatrix}$; б) $\begin{pmatrix} 1 & 3 & 2 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \\ 1 & 3 & 2 & 5 & 4 \\ 5 & 2 & 1 & 4 & 3 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$; в) $\begin{pmatrix} 6 & 2 & 2 & 8 & 8 & 9 \\ 4 & 1 & 9 & 3 & 5 & 1 \\ 6 & 0 & 5 & 9 & 0 & 6 \\ 3 & 3 & 8 & 9 & 11 & 4 \\ 7 & 4 & 0 & 2 & 2 & 1 \\ 8 & 3 & 8 & 2 & 9 & 6 \end{pmatrix}$.

16. Решить задачу о назначениях на узкое место для графов из задачи 15.

Ответы

1. Докажем *необходимость* (*достаточность* устанавливается обратным ходом рассуждений).

Первое решение (венгерская теорема). По условию задачи, в матрице A не найдется n независимых единиц, то есть ее словарный ранг меньше n. Применим венгерскую теорему. Согласно этой теореме, матрицу A покрывают некоторые i' строк и j' столбцов, где $i' + j' < n$. Оставшиеся $i = n - i'$ строк и $j = n - j'$ столбцов в своем пересечении имеют только нули. Осталось заметить, что $i + j = 2n - (i' + j') > n$, откуда $i + j \geqslant n + 1$.

Второе решение (теорема Холла). Пусть строки матрицы A отвечают юношам, а столбцы — девушкам, и пусть условие $a_{kl} = 1$ означает, что k-й юноша знаком с l-й девушкой. Тогда, по условию задачи, всех юношей женить на знакомых девушках нельзя. Согласно теореме Холла, это означает, что какие-то i юношей знакомы в совокупности с не более чем $i - 1$ девушкой и не знакомы с оставшимися девушками, а последних не менее $n - i + 1$. Значит, на пересечении i строк, отвечающих указанным юношам, и $j \geqslant n - i + 1$ столбцов, отвечающих не знакомым ни с кем из них девушкам, стоят одни нули.

7. Да. **Указание.** Рассмотрите двудольный граф, одна доля которого состоит из вершин, образованных сочетаниями из 27 по 4, вершинами второй служат размещения из 27 по 3, и ребро соединяет размещение с сочетанием, если все элементы размещения входят в сочетание. Теперь нужно выяснить, существует ли совершенное паросочетание в этом графе.

9. Расположим прямую горизонтально. Искомой точкой является, например, самый левый из правых концов отрезков.

10. Считая прямую числовой, положим $[a, b] \prec [c, d]$, если $b < c$. Используйте теорему 5 и предыдущую задачу.

12. Прав. **Решение.** Отметим на прямой точки, изображающие юношей, а на параллельной прямой — точки, изображающие девушек. Точки, соответствующие брюнетам и блондинкам, покрасим соответственно в синий и желтый цвет. Остальные точки будем называть белыми. Вариант образования супружеских пар, имеющийся у первой свахи, изобразим синими отрезками, а вариант второй свахи — желтыми. Некоторые отрезки при этом станут зелеными. Наша цель — найти попарно не смежные цветные отрезки (то есть без общих концов), покрывающие в совокупности все цветные точки.

Каждый зеленый отрезок не смежен ни с каким другим цветным отрезком. Ясно также, что отрезки одного цвета попарно не смежны. Поскольку каждая цветная точка

является концом одного или двух цветных отрезков, синие и желтые отрезки образуют несколько ломаных (отрезок считаем частным случаем ломаной) без общих концов, причем цвета звеньев любой ломаной чередуются.

Если ломаная замкнутая, то ее звенья синего цвета покрывают все ее вершины, поэтому можно стереть желтые звенья этой ломаной.

Пусть теперь ломаная незамкнутая. Так как каждая цветная точка порождает свой цветной отрезок, концы ломаной не могут быть оба белыми (иначе цветных точек будет меньше, чем цветных отрезков). Возьмем цветной конец ломаной и пойдем по ней. Другой ее конец будет белым, так как в каждую цветную точку мы попадаем, идя по отрезку другого цвета, и, значит, ломаная продолжается отрезком цвета этой точки. Таким образом, звенья ломаной, имеющие цвет ее цветного конца, покрывают все ее цветные вершины. Звенья другого цвета стираем.

В результате у нас останутся цветные отрезки без общих концов, покрывающие все цветные точки. Задача решена.

13. а) $u_1v_1, u_2v_6, u_3v_2, u_4v_3, u_5v_4, u_6v_5$; $u_1, u_2, u_3, u_4, u_5, u_6$;
б) $u_1v_1, u_2v_2, u_3v_3, u_5v_4, u_6v_6$; u_6, v_1, v_2, v_3, v_4;
в) $u_1v_2, u_2v_3, u_3v_4, u_4v_5, u_5v_6, u_6v_8, u_7v_7, u_9v_1$; $u_2, u_4, u_7, u_9, v_2, v_4, v_6, v_8$.

14. а) $u_1v_3, u_2v_4, u_3v_1, u_4v_5, u_5v_2$;
б) $u_1v_1, u_2v_4, u_3v_3, u_4v_2, u_5v_5$;
в) $u_1v_2, u_2v_4, u_3v_3, u_4v_6, u_5v_1, u_6v_5$.

15. а) $u_1v_4, u_2v_3, u_3v_5, u_4v_2, u_5v_1$;
б) $u_1v_5, u_2v_3, u_3v_4, u_4v_1, u_5v_2$;
в) $u_1v_6, u_2v_3, u_3v_4, u_4v_5, u_5v_2, u_6v_1$.

Глава LXXII

МАТРОИДЫ

Матроиды были введены в 1935 г. Пионерская работа Хасслера Уитни называлась "On the abstract properties of linear dependence" («Об абстрактных свойствах линейной зависимости»). Уитни обнаружил, что понятия зависимости в линейной алгебре и теории графов можно рассматривать с единых позиций. Именно синтез идей различных областей математики и является основой плодотворного развития теории матроидов.

Матроидные структуры естественным образом возникают в теории комбинаторной оптимизации, являясь основой применения *жадных* алгоритмов. Исследования в этой области начались в конце 50-х годов прошлого века. Позднее теория матроидов нашла свое применение и при анализе надежности электрических схем.

Конец XX века ознаменовался бурным развитием криптографии. В так называемых *идеальных схемах разделения секрета* также возникли матроидные структуры.

В этой главе представлены начальные понятия теории матроидов, включая связь матроидов с жадными алгоритмами и теорией трансверсалей.

§ 1. Определения и примеры

Матроид — это упорядоченная пара $M = \langle E, J\rangle$, где E — непустое конечное множество; J — совокупность подмножеств множества E, удовлетворяющая следующим условиям (*аксиомам независимости*):

(J0) $\varnothing \in J$;

(J1) если $A \in J$ и $B \subset A$, то $B \in J$;

(J2) если $A \in J$, $B \in J$ и $|A| = |B| + 1$, то существует такой элемент e, принадлежащий A и не принадлежащий B, что $B \cup \{e\} \in J$.

Элементы множества J называют *независимыми множествами*. Таким образом, аксиома **(J1)** говорит о том, что подмножество независимого множества также является независимым, а аксиома **(J2)** утверждает: если имеются два независимых множества, мощности которых отличаются на единицу, то в более мощном множестве есть элемент, который отсутствует в менее мощном, и при добавлении которого к последнему вновь получится независимое множество.

Базис — это максимальное по включению независимое множество (то есть если A — базис, $A \subset B$ и $A \neq B$, то множество B не является независимым).

В силу конечности множества E в матроиде существует хотя бы один базис.

Ранг матроида — количество элементов в любом его базисе.

Докажем корректность последнего определения: убедимся в том, что в любых двух базисах количество элементов одинаково. От противного: пусть имеются два различных базиса A и B, и в множестве A элементов больше, чем в B. Существует подмножество $A' \subset A$ такое, что $|A'| = |B| + 1$. По аксиоме **(J1)** множество A' — независимое, а по аксиоме **(J2)** найдется элемент $e \in A' \setminus B$ такой, что множество $B \cup \{e\}$ независимо, но тогда множество B не является максимальным по включению независимым множеством, то есть базисом — противоречие!

Очевидно, что максимальное по мощности независимое множество является и максимальным по включению, то есть базисом. Таким образом, любое независимое множество в матроиде M мощности, равной его рангу, есть базис.

Взяв произвольное независимое множество B и некоторый фиксированный базис A с помощью свойства **(J2)** можно в множестве A выбрать $|A| - |B|$ элементов, при добавлении которых к множеству B получится независимое множество мощности $|A|$, то есть базис. Мы доказали, что *всякое независимое множество можно дополнить до базиса*.

Множество $A \subset E$, которое не является независимым в матроиде $M = \langle E, J \rangle$, называется *зависимым*.

Цикл — это минимальное по включению зависимое множество (то есть если A — цикл, $B \subset A$ и $B \neq A$, то множество B — независимое).

Пусть дан матроид $M = \langle E, J \rangle$. Мощность множества E называют *порядком матроида* M.

Примеры матроидов

1. **Тривиальный матроид** — матроид $\langle E, \{\varnothing\} \rangle$; в нем единственным независимым множеством (значит, и единственным базисом) является пустое множество. Ранг тривиального матроида равен нулю, а любое одноэлементное подмножество множества E является циклом.
2. **Дискретный матроид** — матроид $\langle E, \beta(E) \rangle$, где $\beta(E)$ — множество всех подмножеств множества E. В дискретном матроиде все множества являются независимыми, имеется единственный базис — само множество E, а циклов вовсе нет. Ранг дискретного матроида равен $|E|$.
3. **k-однородный матроид** — матроид $\langle E, J \rangle$, в котором любое k-элементное подмножество множества E является базисом. Здесь любое множество, в котором не более k элементов, является независимым. Проверка выполнения аксиом матроида тривиальна. Заметим, что дискретный матроид $\langle E, \beta(E) \rangle$ является $|E|$-однородным, а тривиальный матроид — 0-однородным. В k-однородном матроиде (при $k < |E|$) циклом является любое $(k+1)$-элементное множество. Ранг k-однородного матроида равен k. Имеется специальное обозначение для k-однородного матроида, заданного на n-элементном множестве: $U_{k,n}$.
4. Пусть E — конечная система векторов некоторого линейного пространства над полем F, а J состоит из всех линейно независимых систем векторов из E, а также пустого множества. Тогда, как известно из линейной алгебры,

свойства **(J1)** и **(J2)** будут выполнены. Свойство **(J0)** выполнено по определению. Поэтому $\langle E, J\rangle$ — матроид. Его называют *векторным*[1].

5. Пусть A — числовая матрица с элементами из поля F размера $m \times n$. Будем смотреть на столбцы этой матрицы как на векторы пространства F^m. Тогда столбцы матрицы A образуют векторный матроид; будем называть его *матричным матроидом*, или (точнее) *матроидом столбцов матрицы* A. Обозначение: $M[A]$. Аналогично вводится *матроид строк матрицы*. Легко видеть, что ранг матрицы A равен рангу соответствующего матричного матроида.
6. Пусть G — граф, E — множество его ребер. Объявим независимыми те подмножества E, которые состоят из ребер некоторого леса. Как известно из теории графов, свойства **(J0)**, **(J1)** и **(J2)** будут при этом выполнены. Полученный матроид называют *матроидом циклов* графа G и обозначают $M(G)$. Цикл матроида будут составлять ребра, образующие простую замкнутую цепь в графе G (то есть цикл, в котором каждая вершина встречается ровно один раз).
7. Пусть G — граф, E — множество его ребер. Объявим зависимыми те подмножества E, которые являются разделяющими множествами. Опять же из результатов теории графов следует выполнение аксиом матроида. Полученный матроид называют *матроидом разрезов* графа G и обозначают $M^*(G)$. Циклу этого матроида будет соответствовать разрез графа G, а базису — дополнение к множеству ребер любого остовного леса графа.

Изоморфизм матроидов

Матроиды $M_1 = \langle E_1, J_1\rangle$ и $M_2 = \langle E_2, J_2\rangle$ называются *изоморфными*, если существует биекция (взаимно однозначное отображение) $\varphi : E_1 \to E_2$, сохраняющая независимость; другими словами, множество $A \subset E_1$ является независимым в матроиде M_1 тогда и только тогда, когда образ этого множества при заданном отображении $\varphi(A)$ есть независимое множество в матроиде M_2.

Пример. Матроид циклов графа G, изображенного на рис. 1, изоморфен матроиду столбцов матрицы $A = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$, рассматриваемой над произвольным числовым полем.

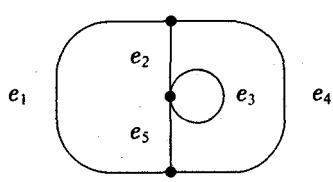


Рис. 1

Введем еще несколько определений.

Матроид — *графический*, если он изоморфен матроиду циклов некоторого графа.

Матроид — *кографический*, если он изоморфен матроиду разрезов некоторого графа.

Наконец, если матроид является одновременно графическим и кографическим, то его называют *планарным*. Это название объясняется тем, что планарный матроид изоморфен матроиду циклов планарного графа.

Для того чтобы лучше освоиться с новыми понятиями, советуем читателю решить соответствующие упражнения, помещенные в последнем параграфе этого тома.

[1] Иногда дают более узкое определение векторного матроида, предполагая, что векторы из системы E попарно различны.

§ 2. Двойственность

Пусть $M = \langle E, J\rangle$ — матроид. Обозначим через J^* множество всех подмножеств дополнений к базисам матроида M. Оказывается, что $M^* = \langle E, J^*\rangle$ — также матроид; его называют *двойственным* к M матроидом. Легко видеть, что базисы двойственного матроида — это дополнения к базисам исходного матроида. Отсюда сразу вытекает, что $(M^*)^* = M$ — матроид, двойственный двойственному M, есть M.

Теорема 1. *Для любого графа G матроид его разрезов является двойственным матроиду циклов.*

◄ Пусть E — множество ребер графа G. Можно считать, что в G нет изолированных вершин.

Рассмотрим произвольный базис B в матроиде циклов $M(G)$. Нужно доказать, что $E \setminus B$ — базис в матроиде разрезов $M^*(G)$. Базис в $M(G)$ есть остовный лес графа G. Базис в $M^*(G)$ — максимальное по включению неразделяющее множество в графе G. При удалении из графа ребер, составляющих $E \setminus B$, остается остовный лес, т. е. число компонент связности графа не изменяется — поэтому множество $E \setminus B$ не является разделяющим. Если оно не максимально по включению, то для некоторого ребра $e \notin E \setminus B$ неразделяющим будет множество $B' = E \setminus B \cup \{e\}$. Но тогда дополнение к B' содержит остовный лес W. Заметим теперь, что $|E \setminus B'| < |B|$, откуда $|W| < |B|$, в то время как любые два остовных леса (одного и того же графа) имеют одинаковую мощность.

Обратно. Пусть D — базис в $M^*(G)$. Нужно убедиться в том, что $E \setminus D$ — остовный лес. Поскольку D — неразделяющее множество, $E \setminus D$ покрывает все вершины графа G. Если в $E \setminus D$ есть цикл, возьмем ребро e, входящее в него. Тогда $D \cup \{e\}$ — также неразделяющее множество вопреки предположению. Значит, $E \setminus D$ — лес, и притом — остовный. ►

§ 3. Представимые матроиды

Матроид *представим над полем F*, если он изоморфен некоторому векторному матроиду над этим полем. Если матроид представим над любым полем, его называют *регулярным*. В случае представимости матроида над полем $GF(2)$ его называют *бинарным*, а над полем $GF(3)$ — *тернарным*.

Теорема 2. *Графический матроид является бинарным.*

◄ Нужно убедиться в том, что матроид циклов произвольного графа G представим над полем $GF(2)$. Составим матрицу $A = (a_{ij})$ инцидентности графа G. Строки этой матрицы соответствуют вершинам графа, а столбцы — ребрам. Если j-е ребро есть петля, инцидентная i-ой вершине, то $a_{ij} = 2$, иначе

$$a_{ij} = \begin{cases} 1, & \text{если } i\text{-я вершина инцидентна } j\text{-му ребру;} \\ 0 & \text{в противном случае.} \end{cases}$$

Заменим в этой матрице двойки нулями, оставив для матрицы прежнее обозначение.

Итак, мы имеем составленную из нулей и единиц матрицу A. Петле графа соответствует нулевой столбец, а столбцы, отвечающие кратным ребрам, — одинаковые. Докажем, что матроид столбцов этой матрицы над полем $GF(2)$ изоморфен $M(G)$, то есть что столбцы линейно зависимы над $GF(2)$ тогда и только тогда, когда соответствующие им ребра графа G содержат цикл.

Нетривиальная линейная комбинация векторов над указанным полем есть просто сумма некоторых из данных векторов. Значит, если некоторые столбцы матрицы A линейно зависимы, то среди них можно выделить столбцы с нулевой суммой. Рассмотрим подграф G' графа G с ребрами, соответствующими этим столбцам. Очевидно, степень каждой вершины в этом подграфе есть четное число. Стало быть, в G' есть цикл (хотя бы потому, что G' есть объединение эйлеровых графов, а в эйлеровом графе есть эйлеров цикл; впрочем, и непосредственное доказательство указанного факта весьма несложно).

Обратно. Пусть некоторое множество ребер содержит цикл. Если среди них есть петля, то отвечающий ей нулевой столбец обеспечивает линейную зависимость столбцов.

Рассмотрим теперь столбцы, отвечающие ребрам простого цикла длины больше 1. Любая строка матрицы A содержит в этих столбцах ровно две единицы. Поэтому сумма указанных столбцов (по модулю 2) равна нулевому столбцу, что означает линейную зависимость исходного множества столбцов. ►

Заметим, что имеется существенное усиление доказанной теоремы. Оказывается, *любой графический матроид является регулярным*; *то же верно и для любого кографического матроида.*

Кроме того, достаточным условием регулярности матроида является его представимость над $GF(2)$ и $GF(3)$, то есть *матроид регулярен тогда и только тогда, когда он одновременно является бинарным и тернарным.*

§ 4. Ранговая функция

Пусть $M = \langle E, J\rangle$ — матроид. Для множества $A \subset E$ определим *сужение матроида M на множество A* как матроид $M|A = \langle A, J'\rangle$, где множество J' образовано всеми подмножествами множества A, являющимися независимыми множествами матроида M:

$$J' = \{X \mid X \subset A, X \in J\}.$$

То, что $M|A$ — действительно матроид, очевидно.

Назовем ранг матроида $M|A$ *рангом* множества A (обозначение $\rho(A)$), а каждый базис этого матроида — *базой* множества A. Таким образом, $\rho(A)$ — это наибольшая мощность независимого подмножества множества A. Заметим, что $M|E = M$, и поэтому ранг матроида $M = \langle E, J\rangle$ равен рангу множества E, а базис матроида есть база множества, на котором он определен. Очевидно также, что $\rho(\varnothing) = 0$, и если $A \in J$, то $\rho(A) = |A|$ (ранг независимого множества равен его мощности).

Отметим следующие свойства ранговой функции ρ:

(ρ1) $\forall A \subset E \quad 0 \leqslant \rho(A) \leqslant |A|$;

(ρ2) если $A \subset B$, то $\rho(A) \leqslant \rho(B)$ (*монотонность*);

(ρ3) $\forall\, A, B \subset E \quad \rho(A \cup B) + \rho(A \cap B) \leqslant \rho(A) + \rho(B)$ (*полумодулярность*).

Выполнение свойств **(ρ1)** и **(ρ2)** очевидно. Докажем **(ρ3)**.

◀ Пусть X — база множества $A \cap B$. С помощью свойства **(J2)** множество X можно дополнить до базы множества A; обозначим полученную базу через Y. Аналогично, Y дополняется до базы Z множества $A \cup B$. Итак, имеем

$$X \subset Y \subset Z \quad \text{и} \quad \rho(A \cap B) = |X|, \quad \rho(A) = |Y|, \quad \rho(A \cup B) = |Z|.$$

Необходимо доказать, что

$$|Z| + |X| \leqslant |Y| + \rho(B). \qquad (*)$$

Заметим, что по построению $X \cup (Z \setminus Y) \subset B$. Отсюда $\rho(X \cup (Z \setminus Y)) \leqslant \rho(B)$. Кроме того, множество $X \cup (Z \setminus Y)$ является подмножеством независимого множества Z, и, в силу **(J1)**, само независимо. Значит,

$$\rho(X \cup (Z \setminus Y)) = |X \cup (Z \setminus Y)| = |X| + |Z| - |Y|.$$

Таким образом, $|X| + |Z| - |Y| \leqslant \rho(B)$, что равносильно неравенству $(*)$. ▶

Покажем теперь, что матроид можно задать через ранговую функцию.

Теорема 3. *Пусть на подмножествах множества E определена целозначная функция ρ, удовлетворяющая условиям* **(ρ1)**, **(ρ2)**, **(ρ3)**, *а множество J состоит из всех тех подмножеств A множества E, для которых $\rho(A) = |A|$. Тогда $M = \langle E, J \rangle$ суть матроид.*

◀ Свойство **(J0)** следует непосредственно из **(ρ1)**.

Докажем **(J1)**. Пусть $\rho(A) = |A|$ и $B \subset A$. Благодаря полумодулярности функции ρ имеем

$$\rho(B \cup (A \setminus B)) + \rho(B \cap (A \setminus B)) \leqslant \rho(B) + \rho(A \setminus B).$$

Но $B \cup (A \setminus B) = A$, и $\rho(A) = |A|$, а $B \cap (A \setminus B) = \varnothing$, и $\rho(\varnothing) = 0$. Поэтому, учитывая также свойство $\rho 1$ и то, что $B \subset A$, получаем

$$|A| = \rho(A) \leqslant \rho(B) + \rho(A \setminus B) \leqslant |B| + |A \setminus B| = |B| + |A| - |B| = |A|.$$

Поскольку на концах этой цепочки соотношений стоит одно и то же число, всюду в ней на самом деле выполняются равенства, в частности, $\rho(B) = |B|$. Таким образом, $B \in J$.

Свойство **(J2)** будем доказывать от противного. Пусть $A, B \in J$, $|B| = k$, $|A| = k + 1$. Если $B \subset A$, то доказывать нечего. Поэтому можно считать, что $|A \setminus B| \geqslant 2$. Предположим, что для любого элемента $e \in A \setminus B$ неверно, что $B \cup \{e\} \in J$. Тогда $\rho(B \cup \{e\}) \neq k + 1$ и, в силу соотношений

$$k = \rho(B) \leqslant \rho(B \cup \{e\}) \leqslant |B \cup \{e\}| = k + 1$$

и целочисленности функции ρ, имеем $\rho(B \cup \{e\}) = k$. Возьмем в качестве e два различных элемента c и d и пусть $C = B \cup \{c\}$, $D = B \cup \{d\}$. Тогда $C \cup D = B \cup \{c, d\}$ и $C \cap D = B$. Поэтому

$$\rho(B \cup \{c, d\}) + \rho(B) = \rho(C \cup D) + \rho(C \cap D) \leqslant \rho(C) + \rho(D) \leqslant k + k,$$

откуда $\rho(B \cup \{c, d\}) \leqslant k$. Так как $\rho(B \cup \{c, d\}) \geqslant \rho(B) = k$, получаем

$$\rho(B \cup \{c, d\}) = k.$$

Итак, при добавлении к множеству B двух элементов из $A \setminus B$ мы получили множество с прежним значением функции ρ.

Если в множестве $A \setminus B$, кроме c и d, есть еще, например, элемент f, положим $C = B \cup \{c, d\}$, $D = B \cup \{f\}$ и, повторив предыдущие выкладки, получим, что $\rho(B \cup \{c, d, f\}) = k$.

Добавляя к множеству B последовательно элементы из $A \setminus B$, мы рано или поздно придем к множеству $B \cup A$, и при этом окажется, что $\rho(B \cup A) = k$, в то время как $\rho(B \cup A) \geqslant \rho(A) = k + 1$. Противоречие получено. ►

§ 5. Жадный алгоритм

Весьма общей является следующая задача оптимизации.

Пусть каждому элементу e непустого конечного множества E поставлено в соответствие неотрицательное число $w(e)$, называемое *весом* этого элемента. *Вес подмножества* $X \subset E$ определяется как сумма весов его элементов:

$$w(X) = \sum_{e \in X} w(e).$$

Рассматривается некоторая совокупность J подмножеств множества E. Требуется найти в J подмножество максимального веса.

Подобный вид имеют или сводятся к нему многие задачи: например, задача коммивояжера, задача о рюкзаке, задача о минимальном стягивающем дереве и другие.

Жадный алгоритм решения описанной задачи состоит в последовательном, элемент за элементом, формировании искомого множества S, причем на каждом шаге из всех элементов множества E, добавление которых к ранее выбранным возможно (то есть приводит к некоторому множеству из J), выбирается элемент наибольшего веса.

Формально алгоритм можно описать так.

1. В качестве первого (e_1) элемента выбрать элемент, удовлетворяющий условию

$$w(e_1) = \max_{\{e\} \in J} w(e).$$

Следующий шаг выполнять до тех пор, пока он приводит к расширению формируемого множества S.

2. Если $S = \{e_1, e_2, \ldots, e_{k-1}\}$, то в качестве очередного элемента множества S выбрать элемент e_k такой, что

$$w(e_k) = \max \{w(e) \mid \{e_1, e_2, \ldots, e_{k-1}, e\} \in J,\ e \notin \{e_1, e_2, \ldots, e_{k-1}\}\}.$$

Конкретная реализация жадного алгоритма зависит во многом от того, что представляет собой множество J.

Пример 1. Пусть $E = \{1, 2, 3\}$, $J = \{\{1\}, \{1, 2\}, \{2, 3\}\}$, $w(1) = 3$, $w(2) = 2$, $w(3) = 4$. Действуя по жадному алгоритму, мы последовательно получим: $e_1 = 1$, $e_2 = 2$ и множество $\{1, 2\}$ веса 5, в то время как входящее в J множество $\{2, 3\}$ имеет вес 6. Жадность не помогла! Она не всегда дальновидна!

Пример 2. В задаче коммивояжера требуется найти замкнутый маршрут наименьшей длины, проходящий через заданные города. Здесь E — множество дорог между городами, в роли веса дороги выступает ее длина. Жадная стратегия для задачи коммивояжера состоит в том, что, начав маршрут в произвольном городе, в качестве очередного города на каждом шаге выбираем такой ранее не посещенный город, к которому ведет самая короткая дорога.

Пример 3. В задаче о минимальном стягивающем дереве требуется в заданном связном взвешенном графе $G = \langle V, E\rangle$ выделить стягивающее дерево минимального веса. Здесь E — множество ребер графа, а J состоит из всех его стягивающих деревьев. Если $w'(e)$ — вес ребра e, а число M больше веса любого ребра, то положив $w(e) = M - w'(e)$, перейдем от задачи минимизации к задаче максимизации. Это стандартный прием, но ценность его скорее чисто теоретическая, поскольку еще проще в описанном алгоритме заменить всюду нахождение максимума нахождением минимума. Различные способы реализации жадной стратегии при нахождении минимального стягивающего дерева — алгоритмы Краскала и Прима — мы рассмотрели в § 8 гл. LXX.

Известно, что жадный алгоритм для задачи из примера 3 всегда дает оптимальное решение, а для задачи из примера 2 — не всегда.

В этом параграфе мы выясним, каким требованиям должна удовлетворять совокупность множеств J, чтобы жадная стратегия приводила к оптимальному решению.

Теорема 4. *Пусть $M = \langle E, J\rangle$ — матроид, а на множестве E определена функция веса $w : E \to \mathbb{R}^+$. Тогда жадный алгоритм выделяет независимое подмножество E наибольшего веса.*

◀ Пусть в результате работы жадного алгоритма сформировано множество $I = \{e_1, e_2, \ldots, e_s\}$. По смыслу алгоритма элементы этого множества проиндексированы в порядке убывания их веса:

$$w(e_1) \geqslant w(e_2) \geqslant \ldots \geqslant w(e_s).$$

Возьмем в E произвольное независимое подмножество $L = \{e'_1, e'_2, \ldots, e'_t\}$ максимального веса, считая, что

$$w(e'_1) \geqslant w(e'_2) \geqslant \ldots \geqslant w(e'_t).$$

Заметим, что множество L максимально по включению среди множеств, входящих в J (иначе его можно расширить, а вес при этом не уменьшится). Множество I максимально по включению по самому смыслу жадного алгоритма. Таким образом, и L, и I — базисы матроида. Значит, как нам уже известно, в них поровну элементов: $t = s$. Докажем по индукции, что для любого i выполняется неравенство $w(e_i) \geqslant w(e'_i)$. *База индукции* обеспечена первым шагом жадного алгоритма.

Пусть теперь для любого $k < n$ уже установлено, что $w(e_k) \geqslant w(e'_k)$. Нужно доказать, что $w(e_n) \geqslant w(e'_n)$. Предположим, что это не так: $w(e_n) < w(e'_n)$.

Сформируем множество

$$A = \{e \in E \mid w(e) \geqslant w(e'_n)\}.$$

Рассмотрим ограничение матроида $M = \langle E, J\rangle$ на множество A — матроид $M' = M|A$. Поскольку

$$w(e_1) \geqslant w(e_2) \geqslant \ldots \geqslant w(e_{n-1}) \geqslant w(e'_{n-1}) \geqslant w(e'_n),$$

множество $B = \{e_1, e_2, \ldots, e_{n-1}\}$ является подмножеством множества A. Это множество независимо (будучи подмножеством независимого множества I) и максимально по включению. Действительно, если в A имеется более широкое независимое подмножество $\{e_1, e_2, \ldots, e_{n-1}, e\}$, то $w(e) \geqslant w(e'_n) > w(e_n)$, и жадный алгоритм должен бы был на n-м шаге включать в формируемое множество вместо элемента e_n элемент e. Итак, B — базис в матроиде M'. Однако, в M' содержится и независимое множество $C = \{e'_1, e'_2, \ldots, e'_n\}$ (оно является подмножеством независимого множества L). Получилось, что в некотором независимом множестве матроида M' элементов больше, чем в его базисе. Противоречие!

Итак, для всех i справедливо неравенство $w(e_i) \geqslant w(e'_i)$. Тогда

$$w(I) = \sum_{i=1}^{s} w(e_i) \geqslant \sum_{i=1}^{s} w(e'_i) = w(L).$$

Значит, I — независимое подмножество максимального веса. ►

Доказательство теоремы показывает, что для задачи с матроидной структурой в оптимальном решении I по сравнению с произвольным независимым множеством L больше (если выразиться более аккуратно, не меньше) не только вес всего множества, но также вес i-го по весу элемента для каждого i. Интересной особенностью оптимального решения является также то, что оно целиком определяется упорядочением весов элементов множества E, но не их конкретными значениями.

Здесь же отметим, чем жадные алгоритмы привлекательны для программистов. Во-первых, эти алгоритмы обычно легки для программирования (вспомним, например алгоритм Прима). Во-вторых, они имеют, как правило, полиномиальные оценки трудоемкости. Это объясняется тем, что искомое множество формируется элемент за элементом, в отличие от алгоритмов типа перебора с возвратом, для которых характерна экспоненциальная трудоемкость.

Итак, в случае матроидной структуры подмножеств жадный алгоритм приводит к оптимальному решению. Оказывается, справедливо и обратное утверждение, возникающее при естественном предположении о замкнутости системы множеств относительно включения.

Теорема 5. *Пусть J — непустая система подмножеств множества E такая, что выполняется условие* **(J1)**. *Если для любой весовой функции $w : E \to \mathbb{R}^+$ жадный алгоритм находит подмножество E наибольшего веса, то $\langle E, J\rangle$ — матроид.*

◄ Достаточно привести пример весовой функции, для которой жадный алгоритм, примененный к задаче, в которой выполняются условия **(J0)** и **(J1)** и не выполняется условие **(J2)**, не дает оптимального решения.

Пусть подмножества A и B множества E таковы, что $|A| = k + 1$, $|B| = k$, и для любого элемента $e \in A \setminus B$ множество $B \cup \{e\}$ не входит в J. Определим

весовую функцию следующим образом:

$$w(e) = \begin{cases} k+2, & \text{если} \quad e \in B; \\ k+1, & \text{если} \quad e \in A \setminus B; \\ 0, & \text{если} \quad e \notin A \cup B. \end{cases}$$

Жадный алгоритм сначала выберет все k элементов множества B, после чего не сможет добавить к нему ни одного элемента ненулевого веса. Таким образом, будет сформировано подмножество веса $(k+2)k = k^2 + 2k$. С другой стороны, множество A имеет заведомо бóльший вес, поскольку вес каждого из $k+1$ его элементов не меньше, чем $k+1$, и

$$w(A) \geqslant (k+1)^2 > k^2 + 2k.$$

Жадный алгоритм не привел к оптимальному решению задачи. ►

§ 6. Одна задача планирования эксперимента

Рассмотрим задачу практического характера, в которой возникает структура матроида.

Пусть некоторый объект подвергается воздействию нескольких независимых факторов. В результате единичного эксперимента можно найти некоторую числовую характеристику объекта, которая является функцией значений указанных факторов. В случае линейной модели эта функция имеет вид:

$$f = c_1x_1 + c_2x_2 + \ldots + c_nx_n,$$

где f — числовая характеристика объекта, n — общее количество факторов, x_i — значения факторов, c_i — коэффициенты, которые надлежит определить в результате проведения серии экспериментов. По техническим причинам факторы могут встречаться только в определенных комбинациях. Будем считать, что таких комбинаций m, причем $m \geqslant n$.

Пример. Пусть изучается влияние содержания различных минералов в почве на повышение урожайности некоторой зерновой культуры. При этом в распоряжении экспериментаторов имеется m различных удобрений, каждое из которых представляет собой смесь указанных минералов в определенных пропорциях.

В принципе можно провести m различных экспериментов и получить m уравнений:

$$\begin{gathered} a_{11}c_1 + a_{12}c_2 + \ldots + a_{1n}c_n = f_1; \\ a_{21}c_1 + a_{22}c_2 + \ldots + a_{2n}c_n = f_2; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}c_1 + a_{m2}c_2 + \ldots + a_{mn}c_n = f_m. \end{gathered}$$

Предположим, что каждый эксперимент имеет свою цену, известную экспериментаторам, а те желают провести наиболее дешевую серию опытов для определения искомых коэффициентов c_i. Для этого им нужно в матрице $A = (a_{ij})$ выбрать n линейно независимых строк с наименьшим суммарным весом, где вес i-й строки есть стоимость i-го эксперимента. Эта задача разрешима, если ранг этой матрицы равен n; будем предполагать, что это условие выполняется.

Рассмотрим матроид строк матрицы A. Каждый базис матроида состоит из n линейно независимых векторов-строк. Независимое множество наименьшего веса как раз и есть то, что нам требуется: оно содержит строки, определяющие наиболее дешевую систему экспериментов.

В заключение заметим, что известен вариант жадного алгоритма для матричного матроида, основанный на классическом методе Гаусса приведения матрицы к треугольному виду. Трудоемкость этого алгоритма — порядка m^2n операций.

§ 7. Трансверсали

Пусть E — непустое конечное множество, $P = (S_1, S_2, \ldots, S_m)$ — некоторая последовательность его непустых подмножеств (они могут пересекаться и даже совпадать). *Трансверсалью* (или *системой различных представителей*) для совокупности множеств P называют множество $T = \{t_1, t_2, \ldots, t_m\}$ такое, что для каждого числа i элемент t_i принадлежит множеству S_i; при этом при различных i и j элементы t_i и t_j также различны.

Другими словами, трансверсаль состоит из m различных представителей m множеств. Заметим, что при этом представителю одного множества не возбраняется быть членом и других множеств.

Трансверсаль любой подпоследовательности последовательности $P = (S_1, S_2, \ldots, S_m)$ называют *частичной трансверсалью* для P. Пустое множество также будем считать частичной трансверсалью: тогда *любое подмножество частичной трансверсали есть частичная трансверсаль*.

Пример 1. Имеется несколько работников, каждый из которых может выполнять определенное (свое для каждого работника) множество работ. При этом для выполнения каждой работы требуется ровно один человек. Требуется так распределить имеющуюся рабочую силу, чтобы каждая работа выполнялась. Формализуя эту задачу, имеем: E — множество работников, множество S_i состоит из тех работников, которые могут выполнять i-ю работу. Назначения на каждый вид работ сводятся к отысканию трансверсали для последовательности множеств $P = (S_1, S_2, \ldots, S_m)$, где m — общее количество работ.

Пример 2. В некотором учреждении имеется m комиссий. Требуется из состава каждой комиссии назначить их председателей так, чтобы ни один человек не председательствовал более чем в одной комиссии. Здесь трансверсаль комиссий составят их председатели.

Пример 3. Пусть $S_1 = S_2 = \{1, 2\}$, $S_3 = S_4 = \{2, 3\}$, $S_5 = \{1, 2, 3, 4, 5, 6\}$. Легко видеть, что не существует трансверсали для $P = (S_1, S_2, S_3, S_4, S_5)$, однако, например, элементы 1, 2, 3, 6 составляют трансверсаль для последовательности $P' = (S_1, S_2, S_3, S_5)$, то есть частичную трансверсаль для P.

Необходимое и достаточное условие существования трансверсали дает следующая

Теорема 6. *Пусть E — непустое конечное множество. Последовательность его непустых подмножеств $P = (S_1, S_2, \ldots, S_m)$ имеет трансверсаль тогда и только тогда, когда объединение любых k подмножеств из этой последовательности содержит не менее k элементов, где k — произвольное натуральное число, не превосходящее m.*

◄ Сначала дадим краткую запись условия существования трансверсали из формулировки теоремы:

$$\forall A \subset \{1, 2, \ldots, m\} \quad \Big|\bigcup_{i\in A} S_i\Big| \geqslant |A|. \tag{1}$$

Необходимость данного условия очевидна. Перейдем к достаточности.

Предварительно докажем

Утверждение. *Если в некотором множестве, например, в S_1, не менее двух элементов, то из этого множества можно удалить один элемент, не нарушив при этом условия* (1).

◄ От противного: пусть $|S_1| \geqslant 2$ и, какой элемент ни удалить из S_1, условие (1) не будет выполнено. Возьмем два элемента x и y из множества S_1. Для них найдутся такие множества индексов $A' = \{1\} \cup A$ и $B' = \{1\} \cup B$, где $A, B \subset \{2, 3, \ldots, m\}$, что

$$\Big|\bigcup_{i\in A} S_i \cup (S_1 \setminus \{x\})\Big| < |A'| = |A| + 1 \text{ и } \Big|\bigcup_{i\in B} S_i \cup (S_1 \setminus \{y\})\Big| < |B'| = |B| + 1. \tag{2}$$

Положим:

$$X = \bigcup_{i\in A} S_i \cup (S_1 \setminus \{x\}), \quad Y = \bigcup_{i\in B} S_i \cup (S_1 \setminus \{y\}).$$

Соотношения (2) перепишем в виде:

$$|X| \leqslant |A|; \quad |Y| \leqslant |B|,$$

откуда

$$|X| + |Y| \leqslant |A| + |B|. \tag{3}$$

Для дальнейшего нам понадобится следующий вариант формулы включения-исключения:

$$|C| + |D| = |C \cup D| + |C \cap D|, \tag{4}$$

где C и D — произвольные множества.

С помощью условия (1) оценим снизу мощности объединения и пересечения множеств X и Y. Поскольку

$$X \cup Y = \bigcup_{i\in A\cup B} S_i \cup (S_1 \setminus \{x\}) \cup (S_1 \setminus \{y\}) = \bigcup_{i\in A\cup B} S_i \cup S_1,$$

выполняется неравенство

$$|X \cup Y| \geqslant |A \cup B| + 1. \tag{5}$$

В силу того, что

$$X \cap Y \supset \bigcup_{i\in A\cap B} S_i,$$

имеем

$$|X \cap Y| \geqslant |A \cap B|. \tag{6}$$

Сложим неравенства (5) и (6), дважды использовав тождество (4):

$$|X| + |Y| = |X \cup Y| + |X \cap Y| \geqslant |A \cup B| + |A \cap B| + 1 = |A| + |B| + 1.$$

Полученное противоречие с неравенством (3) завершает доказательство утверждения. ►

Будем применять процедуру из утверждения до тех пор, пока у нас не останутся лишь одноэлементные множества. При этом в объединении любых k из них содержится k элементов. Значит, все эти множества попарно не пересекаются, а их объединение и есть искомая трансверсаль. ►

Замечание. Искушенный читатель, наверное, сразу узнал в теореме о существовании трансверсали теорему Холла. Действительно, построим двудольный граф с долями $V_1 = \{v_1, v_2, \ldots, v_m\}$ и $V_2 = S_1 \cup S_2 \cup \ldots \cup S_m$, в котором для каждого i множество S_i есть множество вершин, смежных с вершиной v_i. Тогда трансверсаль задает совершенное паросочетание из V_1 в V_2. В матримониальной трактовке теоремы Холла множество S_i состоит из девушек, знакомых i-му юноше, а трансверсаль есть множество счастливых невест.

Идея изложенного выше доказательства, принадлежащего Р. Радо, позволяет получить более общий результат. *Об этом пойдет речь в § 9. А сейчас установим* два следствия из доказанной теоремы.

Следствие 1. *Пусть E — непустое конечное множество. Последовательность его непустых подмножеств $P = (S_1, S_2, \ldots, S_m)$ имеет частичную трансверсаль мощности t тогда и только тогда, когда объединение любых k подмножеств из этой последовательности содержит не менее $k + t - m$ элементов, где k — произвольное натуральное число, не превосходящее m, т. е.*

$$\forall A \subset \{1, 2, \ldots, m\} \quad \Big|\bigcup_{i \in A} S_i\Big| \geqslant |A| + t - m.$$

◄ Чтобы иметь возможность применить утверждение теоремы, возьмем множество D, имеющее мощность $m - t$ и не пересекающееся с E, и образуем новое семейство множеств $P' = (S_1', S_2', \ldots, S_m')$, где $S_i' = S_i \cup D$. С помощью $m - t$ элементов множества D любая частичная трансверсаль мощности t дополняется до (полной) трансверсали. Обратно: если имеется трансверсаль для P', то выбросив из нее элементы множества D, получим частичную трансверсаль мощности не меньше t, а, значит, есть и частичная трансверсаль, мощность которой равна t. Таким образом, существование частичной трансверсали мощности t для P равносильно существованию полной трансверсали для P', а последнее имеет место тогда и только тогда, когда

$$\forall A \subset \{1, 2, \ldots, m\} \quad \Big|\bigcup_{i \in A} S_i'\Big| = \Big|\bigcup_{i \in A} S_i \cup D\Big| = \Big|\bigcup_{i \in A} S_i\Big| + m - t \geqslant |A|.$$

Доказательство следствия 1 завершено. ►

Следствие 2. *Пусть E — непустое конечное множество, $P = (S_1, S_2, \ldots, S_m)$ — последовательность его непустых подмножеств. Множество $X \subset E$ содержит частичную трансверсаль мощности t для P тогда и только тогда, когда*

$$\forall A \subset \{1, 2, \ldots, m\} \quad \Big|\Big(\bigcup_{i \in A} S_i\Big) \cap X\Big| \geqslant |A| + t - m.$$

◄ Положим $S_i' = S_i \cap X$ (для каждого i) и применим к последовательности $P' = (S_1', S_2', \ldots, S_m')$ предыдущее следствие. Получим условие

$$\forall A \subset \{1, 2, \ldots, m\} \quad \Big|\bigcup_{i \in A} S_i'\Big| \geqslant |A| + t - m.$$

Но $\cup S_i' = \cup (S_i \cap X) = (\cup S_i) \cap X$. ►

§ 8. Трансверсальный матроид

Теорема 7 (Дж. Эдмондс, Д. Фалкерсон, 1965 г.). *Пусть E — непустое конечное множество, $P = (S_1, S_2, \ldots, S_m)$ — некоторая последовательность его непустых подмножеств, а J — множество всех частичных трансверсалей для P. Тогда $\langle E, J\rangle$ — матроид.*

◄ Свойства **(J0)** и **(J1)**, очевидно, имеют место. Проверим выполнение аксиомы независимости **(J2)**.

Прибегнем к наглядному представлению семейства множеств $P = (S_1, \ldots, S_m)$ с помощью двудольного графа G, который строится следующим образом. Вершины первой доли V_1 будут соответствовать множествам $S_1, \ldots, S_m$, вершины второй доли V_2 — элементам множества E, и (для каждого i) ребра, инцидентные вершине S_i, соединяют ее со всеми элементами множества S_i. Выделению системы различных представителей соответствует некоторое паросочетание (т. е. множество попарно несмежных ребер) в этом графе: если элемент t_i представляет множество S_i, то в паросочетание войдет ребро $S_i t_i$. Заметим, кстати, что в случае трансверсали имеем совершенное паросочетание из V_1 в V_2.

Пусть A и B — частичные трансверсали и $|A| = |B| + 1$. Нужно доказать, что найдется элемент $e \in A \setminus B$ такой, что $B \cup \{e\}$ — частичная трансверсаль. Паросочетания, отвечающие указанным частичным трансверсалям, обозначим соответственно через W_A и W_B. Покрасим ребра из $W_A \setminus W_B$ в красный цвет, из $W_B \setminus W_A$ — в синий, а из $W_A \cap W_B$ — в зеленый. Красных ребер будет на одно больше, чем синих. Заметим также, что зеленое ребро не смежно ни с одним покрашенным ребром.

Рассмотрим подграф G' исходного графа, образованный красными и синими ребрами. Так как два ребра одного цвета не могут быть смежны, степень каждой вершины в G' равна 1 или 2. Легко видеть, что компоненты связности G' представляют собой циклы и цепи. В каждом цикле и каждой цепи цвета ребер чередуются. Поэтому в цикле, а также цепи четной длины одинаковое количество красных и синих ребер. Поскольку красных ребер больше, чем синих, найдется цепь C нечетной длины $v_1 \dashrightarrow v_2 \to \ldots \to v_{2k}$, в которой первое и последнее ребро — красные. Ровно одна из концевых вершин цепи C лежит в V_2, пусть это вершина v_1. Эта вершина инцидентна только красному ребру и изображает элемент из $A \setminus B$. Каждая из вершин $v_3, v_5, \ldots, v_{2k-1}$ изображает элемент множества E и инцидентна как красному, так и синему ребру. Значит, $\{v_3, v_5, \ldots, v_{2k-1}\} \subset A \cap B$. Перекрасим теперь цепь C, заменив красный цвет синим, а синий красным.

Вернемся к графу G. В результате произведенной перекраски множество вершин из V_2, покрытых синими и зелеными ребрами, пополнилось вершиной v_1, то есть частичная трансверсаль B удлинилась за счет элемента из $A \setminus B$. ►

Матроид, образованный частичными трансверсалями фиксированного семейства множеств P, будем называть *трансверсальным* и обозначать $M[P]$.

Приведем пример практической задачи, в которой возникает трансверсальный матроид.

Пример. Имеется m работников; i-й работник может выполнять работы из множества работ S_i, где $i = 1, 2, \ldots, m$. Пусть общее множество работ $E = \cup S_i = \{e_1, e_2, \ldots, e_n\}$, а прибыль от выполнения работы e_i равна $w(e_i)$. Требуется так распределить работы между работниками (при этом каждый выполняет не более одной работы, а для каждой работы нужен один работник; какие-то работы могут оказаться невыполненными, а какие-то работники могут остаться без работы), чтобы общая прибыль от выполнения работ была максимальной. Математически, задача сводится к отысканию частичной трансверсали наибольшего веса для последовательности множеств $P = (S_1, S_2, \ldots, S_m)$. Другими словами, нужно найти независимое множество наибольшего веса в трансверсальном матроиде. Для этого, как нам уже известно, годится жадный алгоритм.

В заключение параграфа, используем понятие трансверсального матроида для решения одной теоретической задачи.

Выясним, *каким требованиям должны удовлетворять множество $A \subset E$ и семейство множеств P, чтобы первое можно было дополнить до трансверсали второго*, т. е. чтобы семейство P имело трансверсаль, содержащую множество A. Очевидно, необходимыми являются следующие условия:

1. P имеет хотя бы одну трансверсаль.
2. A — частичная трансверсаль для P.

Удивительно, но эти условия являются и достаточными.

◄ Доказательство проводится очень просто, если опираться на теорию матроидов. Действительно, множество A, будучи частичной трансверсалью, является независимым множеством трансверсального матроида. Любое независимое множество можно расширить до базиса. Все базисы матроида имеют одну и ту же мощность. В силу условия 1 мощность базиса равна m. Значит, базис суть трансверсаль. ►

§ 9. Независимые трансверсали

Ранее мы установили необходимое и *достаточное условие существования* трансверсали для семейства подмножеств $P = (S_1, S_2, \ldots, S_m)$ множества E. Теперь пусть на множестве E задан некоторый матроид. *Независимой трансверсалью* для P назовем трансверсаль, которая является независимым множеством в смысле указанного матроида. В частности, если матроид — дискретный, то любая трансверсаль — независимая. Следующая теорема дает критерий существования независимой трансверсали.

Теорема 8 (Р. Радо, 1942 г.). *Пусть $M = \langle E, J \rangle$ — матроид. Последовательность $P = (S_1, S_2, \ldots, S_m)$ непустых подмножеств множества E имеет независимую трансверсаль тогда и только тогда, когда объединение любых k подмножеств из этой последовательности содержит независимое множество, в котором не менее k элементов, где k — произвольное натуральное число, не превосходящее m.*

◄ Условие теоремы удобно сформулировать, используя понятие ранга множества (наибольшей мощности независимого подмножества):

$$\forall A \subset \{1, 2, \ldots, m\} \quad \rho\Big(\bigcup_{i \in A} S_i\Big) \geqslant |A|. \tag{1}$$

Необходимость. Если имеется независимая трансверсаль, то ее пересечение с множеством $\bigcup\limits_{i \in A} S_i$ имеет $|A|$ элементов, откуда $\rho\Big(\bigcup\limits_{i \in A} S_i\Big) \geqslant |A|$.

Достаточность. Предварительно докажем

Утверждение. *Если в некотором множестве (например, в S_1) не менее двух элементов, то из этого множества можно удалить один элемент, не нарушив при этом условия* (1).

◄ От противного: пусть $|S_1| \geqslant 2$ и, какой элемент ни удалить из S_1, условие (1) не будет выполнено. Возьмем два элемента x и y из множества S_1. Для них найдутся такие множества индексов $A' = \{1\} \cup A$ и $B' = \{1\} \cup B$, где $A, B \subset \{2, 3, \ldots, m\}$, что

$$\rho\Big(\bigcup_{i \in A} S_i \cup (S_1 \setminus \{x\})\Big) < |A'| = |A| + 1 \quad \text{и} \quad \rho\Big(\bigcup_{i \in B} S_i \cup (S_1 \setminus \{y\})\Big) < |B'| = |B| + 1. \tag{2}$$

Положим:

$$X = \bigcup_{i \in A} S_i \cup (S_1 \setminus \{x\}), \quad Y = \bigcup_{i \in B} S_i \cup (S_1 \setminus \{y\}).$$

Соотношения (2) перепишем в виде:

$$\rho(X) \leqslant |A|; \quad \rho(Y) \leqslant |B|,$$

откуда

$$\rho(X) + \rho(Y) \leqslant |A| + |B|. \tag{3}$$

С помощью условия (1) оценим снизу ранги объединения и пересечения множеств X и Y. Поскольку

$$X \cup Y = \bigcup_{i \in A \cup B} S_i \cup (S_1 \setminus \{x\}) \cup (S_1 \setminus \{y\}) = \bigcup_{i \in A \cup B} S_i \cup S_1,$$

выполняется неравенство

$$\rho(X \cup Y) \geqslant |A \cup B| + 1. \tag{4}$$

В силу того, что

$$X \cap Y \supset \bigcup_{i \in A \cap B} S_i,$$

имеем

$$\rho(X \cap Y) \geqslant |A \cap B|. \tag{5}$$

Используя свойство полумодулярности ранговой функции, после сложения (4) и (5) получим:

$$\rho(X) + \rho(Y) \geqslant \rho(X \cup Y) + \rho(X \cap Y) \geqslant |A \cup B| + |A \cap B| + 1 = |A| + |B| + 1. \tag{6}$$

Неравенство (6) противоречит неравенству (3). Утверждение доказано. ►

Будем применять процедуру из утверждения до тех пор, пока у нас не останется m одноэлементных множеств $\{t_1\}, \{t_2\}, \ldots, \{t_m\}$. При этом ранг их объединения $T = \{t_1, t_2, \ldots, t_m\}$ равен m. Значит, T и есть искомая независимая трансверсаль. ►

Следствие. *Пусть $M = \langle E, J\rangle$ — матроид. Последовательность $P = (S_1, S_2, \ldots, S_m)$ непустых подмножеств множества E имеет независимую частичную трансверсаль мощности t тогда и только тогда, когда объединение любых k подмножеств из этой последовательности содержит независимое подмножество мощности не менее $k + t - m$, т. е.*

$$\forall A \subset \{1, 2, \ldots, m\} \quad \rho\Big(\bigcup_{i \in A} S_i\Big) \geqslant |A| + t - m.$$

◄ Доказательство вполне аналогично доказательству следствия 1 из теоремы 6. ►

§ 10. Общие трансверсали

Критерий существования независимой трансверсали позволяет получить необходимое и достаточное условия существования общей трансверсали у двух различных систем подмножеств одного и того же множества. Имеет место

Теорема 9. *Два семейства $P = (S_1, S_2, \ldots, S_m)$ и $Q = (R_1, R_2, \ldots, R_m)$ непустых подмножеств конечного множества E обладают общей трансверсалью тогда и только тогда, когда для любых подмножеств A и B множества $\{1, 2, \ldots, m\}$ выполняется неравенство*

$$\Big|\Big(\bigcup_{i \in A} S_i\Big) \cap \Big(\bigcup_{i \in B} R_i\Big)\Big| \geqslant |A| + |B| - m.$$

◄ Рассмотрим матроид частичных трансверсалей для P. Общая трансверсаль P и Q есть независимая (в указанном матроиде) трансверсаль Q. По теореме Радо независимая трансверсаль Q существует в том и только том случае, когда объединение любых k множеств R_i содержит независимое множество из k элементов, которое в нашем случае суть частичная трансверсаль мощности k. Применяя следствие 2 из теоремы 6, имеем

$$\forall A, B \subset \{1, 2, \ldots, m\} \quad \Big|\Big(\bigcup_{i \in A} S_i\Big) \cap X\Big| \geqslant |A| + k - m,$$

где $X = \bigcup\limits_{i \in B} R_i$, $k = |B|$. ►

Покажем, как свести нахождение общей трансверсали к нахождению максимального потока в сети.

Итак, имеем множество $E = \{e_1, e_2, \ldots, e_n\}$ и два семейства его подмножеств $P = (S_1, S_2, \ldots, S_m)$ и $Q = (R_1, R_2, \ldots, R_m)$. Построим ориентированный граф, содержащий следующие вершины:

- a — источник, b — сток;

- вершины, изображающие подмножества $S_1, S_2, \ldots, S_m, R_1, R_2, \ldots, R_m$;
- по две вершины на каждый элемент множества E: $v_1', v_1'', v_2', v_2'', \ldots, v_n', v_n''$

и следующие дуги:

- aS_i и R_ib для $i = 1, 2, \ldots, m$;
- S_iv_j', если $e_j \in S_i$;
- $v_j''R_i$, если $e_j \in \mathbb{R}_i$;
- $v_i'v_i''$ для $j = 1, 2, \ldots, n$.

Положим пропускные способности всех дуг равными единице. Если существует общая трансверсаль $t_1, t_2, \ldots, t_m$ для P и Q, то в построенном графе есть m непересекающихся путей из источника в сток вида

$$a \to S_i \to v_k' \to v_k'' \to R_j \to b,$$

где элемент e_k является представителем множеств S_i и R_j. Эти m путей формируют максимальный поток (его величина m) в построенной транспортной сети. После нахождения максимального потока легко указать общую трансверсаль.

Пример. Для множеств $S_1 = \{1, 2\}$, $S_2 = \{1, 2, 3, 4\}$, $S_3 = \{2, 4\}$, $R_1 = \{2, 3\}$, $R_2 = \{1, 4\}$, $R_3 = \{1, 2, 3\}$ имеем сеть (с единичными пропускными способностями всех дуг):

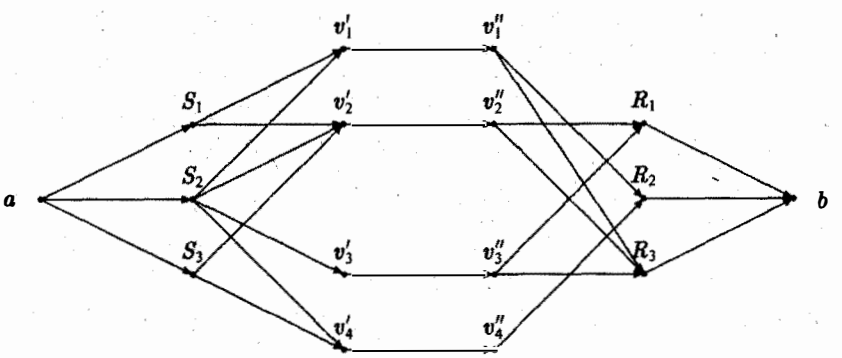


Рис. 2

После нахождения максимального потока можно увидеть общую трансверсаль $\{1, 2, 3\}$, причем 1 является представителем множеств S_1 и R_2, 2 представляет S_3 и R_1, а 3 — множества S_2 и R_3.

§ 11. Некоторые интересные матроиды

Геометрическое представление матроидов малого ранга

Пусть в матроиде нет циклов длины 1 и 2, а ранг матроида не больше 4. Будем изображать такой матроид в виде графа, вершины которого соответствуют элементам матроида, и при этом:

- если три элемента матроида образуют цикл, то изображающие их точки лежат на одной прямой или на одной окружности;

- если четыре элемента матроида образуют цикл, то соответствующие им точки лежат на одной плоскости.

Если полученному графу можно сопоставить многогранник, то, как это принято при изображении пространственных фигур, некоторые ребра (невидимые) будем рисовать прерывистыми линиями.

11.1. Матроид Фано

Матроид Фано F изображен на рис. 3. Он обладает многими замечательными свойствами. Установим некоторые из них.

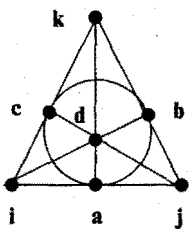


Рис. 3

1. *Матроид Фано является бинарным.*

◄ Действительно, рассмотрим линейное пространство с базисом $(\mathbf{i}, \mathbf{j}, \mathbf{k})$ над полем $GF(2)$. Полученный векторный матроид изоморфен F. В этом легко убедиться, поставив в соответствие вершинам треугольника векторы $\mathbf{i}, \mathbf{j}, \mathbf{k}$, середине каждой стороны — сумму векторов ее концов, а центру — вектор $\mathbf{i}+\mathbf{j}+\mathbf{k}$. ►

2. *Матроид Фано не является регулярным.*

◄ Предположим, что матроид F представим над некоторым полем. Пусть элементам матроида соответствуют векторы $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$, $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$, $\mathbf{d}$ (рис. 3). Разложим по базису $(\mathbf{i}, \mathbf{j}, \mathbf{k})$ остальные векторы:

$$\mathbf{a} = x_1\mathbf{i} + y_1\mathbf{j}; \quad \mathbf{b} = y_2\mathbf{j} + z_2\mathbf{k};$$
$$\mathbf{c} = x_3\mathbf{i} + z_3\mathbf{k}; \quad \mathbf{d} = x\mathbf{i} + y\mathbf{j} + z\mathbf{k}.$$

Из линейной зависимости векторов $\mathbf{i}, \mathbf{b}, \mathbf{d}$ следует равенство нулю определителя, составленного из их координат:

$$\begin{vmatrix} 1 & 0 & 0 \\ 0 & y_2 & z_2 \\ x & y & z \end{vmatrix} = 0.$$

Отсюда

$$y_2 z = y z_2. \tag{1}$$

Аналогично из линейной зависимости троек векторов $\mathbf{j}, \mathbf{c}, \mathbf{d}$; $\mathbf{k}, \mathbf{a}, \mathbf{d}$ и $\mathbf{a}, \mathbf{b}, \mathbf{c}$ вытекают соответственно равенства:

$$z_3 x = z x_3; \tag{2}$$
$$x_1 y = x y_1; \tag{3}$$
$$x_1 y_2 z_3 + y_1 z_2 x_3 = 0. \tag{4}$$

Заметим, что никакие два элемента в F не образуют зависимого множества; поэтому элементы числового поля $x_1, y_1, y_2, z_2, x_3, z_3$ отличны от нуля. А из того, что тройки векторов $\mathbf{d}, \mathbf{i}, \mathbf{j}$; $\mathbf{d}, \mathbf{i}, \mathbf{k}$ и $\mathbf{d}, \mathbf{j}, \mathbf{k}$ являются линейно независимыми, следует неравенство нулю скаляров x, y и z. Перемножив равенства (1), (2) и (3) и сократив на xyz, получим

$$x_1 y_2 z_3 = y_1 z_2 x_3.$$

Число $t = x_1y_2z_3 = y_1z_2x_3$ не равно нулю, и, в то же время, как показывает соотношение (4), $t + t = 0$. Это означает, что поле имеет характеристику 2.

Подведем итог. Если матроид Фано F представим над некоторым полем, то это поле имеет характеристику 2. Стало быть, матроид F представим не над любым полем, то есть он не является регулярным. ►

В дальнейшем матроид Фано будем рассматривать как векторный матроид с элементами $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$, $\mathbf{i}+\mathbf{j}$, $\mathbf{i}+\mathbf{k}$, $\mathbf{j}+\mathbf{k}$, $\mathbf{i}+\mathbf{j}+\mathbf{k}$ над полем $GF(2)$.

3. *Матроид Фано не является трансверсальным.*

◄ Доказательство от противного. Если матроид трансверсальный, то поскольку векторы $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ образуют независимое множество, без ограничения общности можно считать, что $\mathbf{i} \in S_1$, $\mathbf{j} \in S_2$, $\mathbf{k} \in S_3$. Вектор $\mathbf{i}+\mathbf{j}+\mathbf{k} \notin S_l$, где $l > 3$, так как в противном случае векторы $\mathbf{i}, \mathbf{j}, \mathbf{k}$, $\mathbf{i}+\mathbf{j}+\mathbf{k}$ были бы линейно независимы, что неверно. Пусть $\mathbf{i}+\mathbf{j}+\mathbf{k} \in S_1$. Посмотрим, в каких множествах S_i может находиться элемент $\mathbf{i}+\mathbf{k}$. Он не входит в S_2 (иначе векторы $\mathbf{i}$, $\mathbf{i}+\mathbf{k}$, $\mathbf{k}$ линейно независимы, что не имеет места) и в S_3 (иначе линейно независимыми окажутся векторы $\mathbf{i}+\mathbf{j}+\mathbf{k}$, $\mathbf{j}$, $\mathbf{i}+\mathbf{k}$). Но и при $l > 3$ вектор $\mathbf{i}+\mathbf{k}$ не принадлежит S_l (в противном случае можно составить частичную трансверсаль из элементов $\mathbf{i}$, $\mathbf{k}$, $\mathbf{i}+\mathbf{k}$). Остается единственная возможность: $\mathbf{i}+\mathbf{k} \in S_1$. Аналогичные рассуждения, примененные к вектору $\mathbf{i}+\mathbf{j}$, показывают, что он также входит лишь в множество S_1. Отсюда следует, что в нашем матроиде множество $\{\mathbf{i}+\mathbf{k}, \mathbf{i}+\mathbf{j}\}$ является зависимым, а это неверно. ►

4. *Матроид Фано является эйлеровым (то есть представим в виде объединения непересекающихся циклов).*

◄ Действительно, имеем циклы $\{\mathbf{i}, \mathbf{j}, \mathbf{k}, \mathbf{i}+\mathbf{j}+\mathbf{k}\}$ и $\{\mathbf{i}+\mathbf{j}, \mathbf{i}+\mathbf{k}, \mathbf{j}+\mathbf{k}\}$. ►

5. *Матроид Фано не является графическим.*

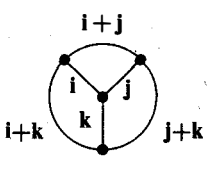


Рис. 4

◄ Пусть это не так. Отождествим элементы матроида с ребрами графа G, матроид циклов которого изоморфен F. Ребра $\mathbf{i}$, $\mathbf{j}$, $\mathbf{i}+\mathbf{j}$ образуют цикл, поэтому ребра $\mathbf{i}$ и $\mathbf{j}$ смежны. Аналогично, смежны ребра $\mathbf{i}$ и $\mathbf{k}$, $\mathbf{j}$ и $\mathbf{k}$. В то же время $\mathbf{i}$, $\mathbf{j}$ и $\mathbf{k}$ не образуют цикла. Если три ребра попарно смежны и не образуют цикла, то у них есть общая вершина. Получаем подграф графа G, изображенный на рис. 4. Из рисунка видно, что ребра $\mathbf{j}$ и $\mathbf{i}+\mathbf{k}$ не смежны, однако вместе с ребром $\mathbf{i}+\mathbf{j}+\mathbf{k}$ они должны составлять цикл. Противоречие! ►

6. *Матроид Фано не является кографическим.*

◄ Вновь рассуждая от противного, отождествим элементы матроида с ребрами графа G, матроид разрезов которого изоморфен F. Поскольку в матроиде Фано циклы состоят из трех или четырех элементов, в графе G любой разрез содержит три или четыре ребра. Значит, степень каждой вершины графа не меньше 3. По лемме о рукопожатиях сумма степеней всех вершин графа G равна удвоенному числу ребер, то есть $2 \cdot 7 = 14$. Отсюда следует, что в нашем графе не более четырех вершин. Каждое ребро графа должно входить в некоторый его разрез (так как каждый элемент матроида входит в некоторый цикл); поэтому в графе нет петель. Поскольку для любых двух элементов матроида a и b можно указать цикл, включающий элемент a и не содержащий b, для каждого ребра графа найдется разрез с этим ребром, но без любого другого (наперед заданного). Значит, в графе нет

кратных ребер. Итак, имеем простой граф, в котором не больше четырех вершин. Но тогда ребер будет не более шести, а их семь. Пришли к противоречию. ►

11.2. Матроид Вамоса

Пусть $E = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Матроид Вамоса V удобно задать, назвав все его зависимые множества: это все подмножества E, в которых не менее пяти элементов, а также $\{1, 2, 5, 6\}$, $\{1, 2, 7, 8\}$, $\{3, 4, 5, 6\}$, $\{3, 4, 7, 8\}$, $\{5, 6, 7, 8\}$. Графическое представление матроида — на рис. 5.

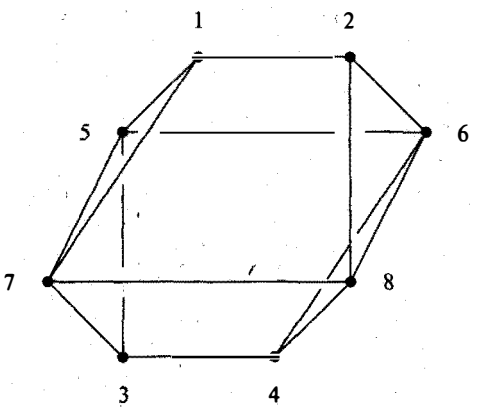


Рис. 5

Сначала убедимся в том, что перед нами действительно матроид. Фактически нуждается в проверке лишь тот факт, что если A и B независимые множества и $|B| = 3$, $|A| = 4$, то в A найдется такой элемент e, что $B \cup \{e\}$ — независимое множество. Когда $B \subset A$, это очевидно. В противном же случае множество $A \setminus B$ содержит по меньшей мере два различных элемента. Обозначим их через e_1 и e_2. Теперь осталось заметить, что из множеств $B \cup \{e_1\}$ и $B \cup \{e_2\}$ хотя бы одно независимое, так как по условию нет двух зависимых множеств из четырех элементов, отличающихся одним элементом.

Докажем, что *матроид Вамоса — не векторный*, т. е. что *он не представим ни над каким полем*. Заметим, что среди всех таких матроидов он имеет наименьший порядок. Этим он и замечателен.

◄ Предположим, что существует изоморфный V векторный матроид $M = \langle E, J \rangle$, где $E = \{x_1, x_2, \ldots, x_8\}$, и для каждого i вектор x_i соответствует элементу i матроида Вамоса.

Множество $\{x_1, x_2, x_3, x_4\}$ является базисом M. Запишем координаты каждого вектора в этом базисе: $x_i = (a_{i1}, a_{i2}, a_{i3}, a_{i4})$. Для дальнейшего нам понадобятся также векторы $y_i = (a_{i1}, a_{i2}, 0, 0)$ и $z_i = (0, 0, a_{i3}, a_{i4})$, где $i = 1, 2, \ldots, 8$. Ввиду линейной зависимости векторов x_1, x_2, x_5, x_6 получаем равенство нулю определителя, составленного из координат этих векторов:

$$\begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ a_{51} & a_{52} & a_{53} & a_{54} \\ a_{61} & a_{62} & a_{63} & a_{64} \end{vmatrix} = 0.$$

Отсюда

$$\begin{vmatrix} a_{53} & a_{54} \\ a_{63} & a_{64} \end{vmatrix} = 0,$$

то есть векторы z_5 и z_6 линейно зависимы. Заметим, что вектор z_5 ненулевой (иначе были бы линейно зависимыми векторы x_1, x_2, x_5, а у нас любые три вектора линейно независимые). Поэтому для некоторого скаляра (то есть элемента

числового поля, над которым рассматривается линейное пространство) μ имеет место равенство $z_6 = \mu z_5$. Точно так же из линейной зависимости четверок векторов $\{x_1, x_2, x_7, x_8\}$, $\{x_3, x_4, x_5, x_6\}$, $\{x_3, x_4, x_7, x_8\}$ получаем соответственно равенства $z_8 = \beta z_7$, $y_6 = \lambda y_5$, $y_8 = \alpha y_7$, где греческими буквами обозначены некоторые скаляры.

Наконец, используем линейную зависимость векторов x_5, x_6, x_7, x_8. С помощью найденных соотношений будем преобразовывать определитель, составленный из координат этих векторов (при этом вместо строк определителя для наглядности записываем поначалу соответствующие векторы):

$$\begin{vmatrix} x_5 \\ x_6 \\ x_7 \\ x_8 \end{vmatrix} = \begin{vmatrix} y_5 + z_5 \\ y_6 + z_6 \\ y_7 + z_7 \\ y_8 + z_8 \end{vmatrix} = \begin{vmatrix} y_5 + z_5 \\ \lambda y_5 + \mu z_5 \\ y_7 + z_7 \\ \alpha y_7 + \beta z_7 \end{vmatrix} = \begin{vmatrix} y_5 \\ \mu z_5 \\ y_7 \\ \beta z_7 \end{vmatrix} + \begin{vmatrix} y_5 \\ \mu z_5 \\ z_7 \\ \alpha y_7 \end{vmatrix} + \begin{vmatrix} z_5 \\ \lambda y_5 \\ y_7 \\ \beta z_7 \end{vmatrix} + \begin{vmatrix} z_5 \\ \lambda y_5 \\ z_7 \\ \alpha y_7 \end{vmatrix} =$$

$$= \mu(\beta - \alpha) \begin{vmatrix} y_5 \\ z_5 \\ y_7 \\ z_7 \end{vmatrix} - \lambda(\beta - \alpha) \begin{vmatrix} y_5 \\ z_5 \\ y_7 \\ z_7 \end{vmatrix} = (\mu - \lambda)(\beta - \alpha) \begin{vmatrix} a_{51} & a_{52} & 0 & 0 \\ 0 & 0 & a_{53} & a_{54} \\ a_{71} & a_{72} & 0 & 0 \\ 0 & 0 & a_{73} & a_{74} \end{vmatrix} =$$

$$= (\mu - \lambda)(\beta - \alpha) \begin{vmatrix} a_{51} & a_{52} \\ a_{71} & a_{72} \end{vmatrix} \cdot \begin{vmatrix} a_{53} & a_{54} \\ a_{73} & a_{74} \end{vmatrix} = 0.$$

Теперь заметим, что $\mu \neq \lambda$ (в противном случае линейно зависимыми будут векторы $x_5 = y_5 + z_5$ и $x_6 = \lambda y_5 + \mu z_5$), а $\alpha \neq \beta$ (иначе линейно зависимы векторы x_7 и x_8). Поэтому равен нулю один из определителей $\begin{vmatrix} a_{51} & a_{52} \\ a_{71} & a_{72} \end{vmatrix}$ или $\begin{vmatrix} a_{53} & a_{54} \\ a_{73} & a_{74} \end{vmatrix}$ — например, первый из них. Но тогда

$$\begin{vmatrix} x_3 \\ x_4 \\ x_5 \\ x_7 \end{vmatrix} = \begin{vmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ a_{51} & a_{52} & a_{53} & a_{54} \\ a_{71} & a_{72} & a_{73} & a_{74} \end{vmatrix} = \begin{vmatrix} a_{51} & a_{52} \\ a_{71} & a_{72} \end{vmatrix} = 0,$$

то есть векторы x_3, x_4, x_5, x_7 линейно зависимы, что противоречит условию. ►

Упражнения

1. Доказать, что с точностью до изоморфизма число матроидов порядка n не превосходит 2^{2^n}.
2. Найти ранг, все базисы и циклы матроида столбцов матрицы

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix},$$

обозначая i-й столбец матрицы через e_i.

3. Дан граф G (рис. 6).
Для а) матроида циклов $M(G)$; б) матроида разрезов $M^*(G)$ найти все циклы и базисы.

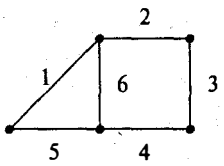


Рис. 6

4. Пусть в матроиде M, заданном на множестве $E = \{1, 2, 3\}$, есть ровно два базиса: $\{1, 2\}$ и $\{1, 3\}$. Доказать, что этот матроид планарный, построив такие графы G_1 и G_2, что матроид M изоморфен матроиду циклов $M(G_1)$ и матроиду разрезов $M^*(G_2)$.
5. Покажите, что все матроиды порядка не выше 3 графические, построив соответствующие графы. Подсчитайте количество попарно неизоморфных матроидов порядка 0, 1, 2 и 3.
6. Доказать, что матроид $U_{n-1,n}$ — графический.
7. Доказать, что матроид $U_{1,n}$ — кографический.
8. Доказать, что матроид $U_{2,4}$ не является ни графическим, ни кографическим.
9. Укажите все попарно неизоморфные матроиды порядка 4. Сколько среди них не являются графическими?
10. Доказать, что матроиды $M(K_5)$ и $M(K_{3,3})$ — не кографические.
11. Через $M_q[A]$ обозначим матроид столбцов матрицы A над полем $GF(q)$. Пусть

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

   1) Найти три столбца матрицы A, образующие цикл в $M_2[A]$ и базис в $M_3[A]$.
   2) Доказать, что $M_2[A]$ — графический матроид, а $M_3[A]$ — нет.
   3) Доказать, что матроид $M_2[A]$ представим над полем $GF(3)$, а $M_3[A]$ не представим над $GF(2)$.

12. Для каждого из следующих семейств подмножеств множества $\{1, 2, 3, 4, 5\}$ выяснить, имеет ли оно трансверсаль:
    $P_1 = (\{1\}, \{2, 3\}, \{1, 2\}, \{1, 3\}, \{1, 4, 5\})$;
    $P_2 = (\{1, 2\}, \{2, 3\}, \{4, 5\}, \{4, 5\})$;
    $P_3 = (\{1, 3\}, \{2, 3\}, \{1, 2\}, \{3\})$;
    $P_4 = (\{1, 3, 4\}, \{1, 4, 5\}, \{2, 3, 5\}, \{2, 4, 5\})$.
13. Доказать, что любой матроид ранга 1 трансверсален.
14. Доказать, что k-однородный матроид трансверсален.
15. Имеется множество юношей, каждый из которых знаком с некоторыми девушками. Две свахи знают, кто с кем знаком. Одна сваха заявляет: «Я могу одновременно женить всех юношей так, чтобы каждый из них женился на знакомой ему девушке!» Вторая сваха говорит: «А я могу устроить судьбу всех блондинок!» Этот диалог услышал любитель математики, который сказал: «В таком случае я могу сделать и то, и другое!» Прав ли он?
16. Пусть E — непустое конечное множество, $P = (S_1, S_2, \ldots, S_m)$ — некоторая последовательность его подмножеств. Частичные трансверсали P определяют трансверсальный матроид ранга r. Доказать, что этот матроид можно задать последовательностью из r множеств.
17. Доказать, что с точностью до изоморфизма число трансверсальных матроидов порядка n не превосходит 2^{n^2}.

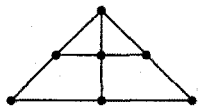


Рис. 7

18. Доказать, что матроид, изображенный на рис. 7, — не бинарный, но тернарный.

19. Доказать, что матроид из предыдущего упражнения не является трансверсальным.

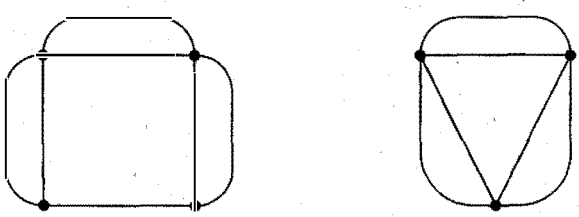
20. Пусть C — цикл. Доказать, что $\rho(C) = |C| - 1$.

21. Найти $U^*_{k,n}$.

22. Доказать, что матроид $U_{2,3}$ — регулярный.

23. Над какими полями представим матроид $U_{2,4}$?

24. На рис. 8 изображены графы. Относительно матроидов циклов этих графов выяснить, являются ли они трансверсальными.



G_1 G_2

Рис. 8

Ответы

5. 1, 2, 4, 8. **9.** Всего 17 матроидов, из них 16 графических. **15.** Прав. См. конец § 8.

16. Рассмотрим двудольный граф $G(V_1, V_2)$, в котором вершины первой доли соответствуют множествам S_i, а второй — элементам множества E. Ребро $S_i e_j$ присутствует в графе тогда и только тогда, когда $e_j \in S_i$.

Любое независимое множество трансверсального матроида можно теперь рассматривать как множество вершин второй доли, покрытое некоторым паросочетанием.

Зафиксируем некоторую максимальную частичную трансверсаль. Ей отвечает некоторое паросочетание мощности r. Пусть оно покрывает множество A вершин из V_1.

Возьмем теперь произвольное независимое множество матроида — множество B вершин из V_2, покрываемое некоторым паросочетанием. Согласно задаче 12 из § 12 гл. LXXI, существует паросочетание M, покрывающее одновременно множества A и B. Его мощность не меньше r (поскольку M покрывает A), но и не больше r (это ранг матроида) — значит, она равна r.

Таким образом, элементы множества B образуют частичную трансверсаль для системы множеств A. Стало быть, если мы сохраним в P лишь множества, вошедшие в A, то получим тот же самый матроид.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

С

Т

У

Ф

Ц

Ч

Э

ВСЯ ВЫСШАЯ МАТЕМАТИКА

В семи томах:

Том 1

- Аналитическая геометрия
- Векторная алгебра
- Линейная алгебра
- Дифференциальное исчисление

Том 2

- Интегральное исчисление
- Дифференциальное исчисление функций нескольких переменных
- Дифференциальная геометрия

Том 3

- Теория рядов
- Обыкновенные дифференциальные уравнения
- Теория устойчивости

Том 4

- Кратные и криволинейные интегралы
- Векторный анализ
- Функции комплексного переменного
- Дифференциальные уравнения с частными производными

Том 5

- Теория вероятностей
- Математическая статистика
- Теория игр

Том 6

- Вариационное исчисление
- Линейное программирование
- Вычислительная математика
- Теория сплайнов

Том 7

- Теория чисел
- Общая алгебра
- Комбинаторика
- Теория Пойа
- Теория графов
- Пересчетания
- Матроиды

Любые отзывы о настоящем издании, а также обнаруженные опечатки присылайте по адресу URSS@URSS.ru. Ваши замечания и предложения будут учтены и отражены на web-странице этой книги в нашем интернет-магазине http://URSS.ru

КОНКУРС ПО СОЗДАНИЮ НОВЫХ УЧЕБНИКОВ

ЛАУРЕАТ

МИНИСТЕРСТВА ОБРАЗОВАНИЯ РОССИИ

НАУЧНАЯ И УЧЕБНАЯ ЛИТЕРАТУРА
E-mail: URSS@URSS.ru
Каталог изданий в Интернете:
http://URSS.ru
Тел./факс: 7 (095) 135-42-16
URSS Тел./факс: 7 (095) 135-42-46

3384 ID 31314

9 785484 005215