

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КАФЕДРА ТЕОРЕТИЧЕСКОЙ КИБЕРНЕТИКИ

А. В. Косточка, Ф. И. Соловьева

ДИСКРЕТНАЯ МАТЕМАТИКА

Учебное пособие
Часть 1

Новосибирск
2001

ББК: В 183.5 я73-1
УДК: 519

Пособие является первой частью конспекта лекций по курсу "Дискретная математика". Рассматриваются основы теории булевых функций, комбинаторики (включая некоторые дискретные задачи теории вероятностей) и теории графов. Пособие предназначено для студентов физического факультета (специальность "информатика"), факультета информационных технологий НГУ, а также технического факультета ВКИ НГУ (специальность "компьютерная техника").

Переиздание подготовлено при поддержке гранта ФЦП "Интеграция" № 274.

© Новосибирский государственный университет, 2001

Предисловие

Настоящее учебное пособие является переизданием первой части конспекта лекций по курсу "Дискретная математика". В нем рассматриваются основы теории булевых функций, комбинаторики (включая некоторые дискретные задачи теории вероятностей) и теории графов.

При подготовке лекций использована в основном следующая литература:

1. Г. П. Гаврилов, А. А. Сапоженко, Задачи и упражнения по курсу дискретной математики. М.: Наука, 1992.
2. В. А. Евстигнеев, Применение теории графов в программировании. М.: Наука, 1985.
3. В. А. Емеличев, О. И. Мельников, В. И. Сарванов, Р. И. Тышкевич, Лекции по теории графов. М.: Наука, 1990.
4. В. Липский, Комбинаторика для программистов. М.: Мир, 1988.
5. В. Феллер, Введение в теорию вероятностей и ее приложения. М.: Мир, 1984. Т. 1.
6. С. В. Яблонский, Введение в дискретную математику. М.: Наука, 1979.

1 АЛГЕБРА ВЫСКАЗЫВАНИЙ И БУЛЕВЫ ФУНКЦИИ

1.1 Высказывания. Логические операции

Основными объектами исследования алгебры высказываний являются высказывания. Под *высказыванием* будем понимать такое утверждение, которое либо истинно, либо ложно (но не может быть истинным и ложным одновременно).

Примеры

1. "Вы умеете читать" – истинное высказывание.
2. "Новосибирск – столица России" – ложное высказывание.
3. "Чему равно $2 + 2$?" – не является высказыванием.

Значением истинности истинного высказывания будем считать "истина", значением истинности ложного – "ложь". Из простых высказываний можно составлять сложные с помощью логических связок.

Примеры

1. "Если три стороны одного треугольника равны трем сторонам другого треугольника, то эти треугольники равны".
2. "Если сегодня в аудитории идут занятия, то на улице идет дождь".

Цель алгебры высказываний – изучение истинности сложных высказываний, если известна истинность составляющих их простых высказываний.

Рассмотрим простейшие операции над высказываниями.

1. Если x – некоторое высказывание, то по определению его *отрицание* $\neg x$ истинно, если и только если x ложно. Выражение $\neg x$ читается "не x ".

2. Если x и y – некоторые высказывания, то по определению их *конъюнкция* $x \& y$ истинна, если и только если x и y истинны. Выражение $x \& y$ читается " x и y ".

3. Если x и y – некоторые высказывания, то по определению их *дизъюнкция* $x \vee y$ истинна, если и только если хотя бы одно из x и y истинно. Выражение $x \vee y$ читается " x или y ".

4. Логическую связь "если x , то y " моделирует *импликация* $x \rightarrow y$. По определению импликация $x \rightarrow y$ истинна, если и только если x ложно или y истинно.

Приведем определение формулы алгебры высказываний.

Рассмотрим алфавит

$\Omega = \Omega_1 \cup \Omega_2 \cup \Omega_3$, где

$\Omega_1 = \{A_0, A_1, A_2, \dots\}$ – множество простых высказываний,

Ω_2 – множество операций над высказываниями,
 $\Omega_3 = \{ (,) \}$ – множество вспомогательных символов.

Формулы алгебры высказываний определим индуктивно:

1. Простое высказывание является формулой.
2. Если $f \in \Omega_2$ – некоторая m -местная операция над высказываниями, а A_1, \dots, A_m – формулы, то $f(A_1, \dots, A_m)$ – тоже формула.

1.2 Эквивалентность. Таблицы истинности

Назовем два высказывания A и B *эквивалентными*, если при любом наборе значений истинности входящих в них логических переменных значения истинности A и B совпадают.

Естественно, желательно иметь способы определять по любым высказываниям A и B , являются ли они эквивалентными. Одним из теоретически простых способов является построение для каждого из интересующего нас высказывания его *таблицы истинности*, т. е. таблицы, где выписываются все возможные наборы значения истинности входящих в него логических переменных и соответствующие этим наборам значения истинности нашего составного высказывания. По определению два высказывания эквивалентны, если их таблицы истинности совпадают. Примеры таблиц для некоторых высказываний приведены ниже.

x	y	\bar{x}	$x \& y$	$x \vee y$	$x \rightarrow y$	$\bar{x} \& \bar{y}$	$\overline{x \vee y}$
1	1	0	1	1	1	0	0
1	0	0	0	1	0	0	0
0	1	1	0	1	1	0	0
0	0	1	0	0	1	1	1

Таблицу истинности высказывания, зависящего от n простых высказываний, можно рассматривать как таблицу значений функции, принимающей значения 0 или 1 и зависящей от n переменных, каждая из которых тоже принимает два значения. Такие функции часто называют *функциями алгебры логики*, или *булевыми функциями*.

Таким образом, каждому высказыванию A , зависящему от n простых высказываний, однозначно соответствует некоторая булева функция f от n переменных. При этом будем говорить, что формула A *реализует* функцию f . По определению эквивалентным высказываниям соответствует одна и та же функция. В дальнейшем при рассмотрении булевых функций будем писать 1 вместо "истина", 0 вместо "ложь".

Итак, булева функция от n переменных – это отображение множества всех двоичных наборов длины n во множество $\{0, 1\}$, а формула – одна из ее возможных реализаций.

Пусть P – множество функций, соответствующих множеству операций над высказываниями Ω_2 . *Суперпозицией над множеством P* называется всякая булева функция, которую можно реализовать формулой над множеством Ω_2 .

Обозначим через \mathcal{P}_2 множество всех булевых функций. Иногда в дальнейшем знак $\&$ будем опускать, полагая $x\&y = xy$.

Если зафиксировать n переменных, то различные таблицы истинности, отвечающие различным булевым функциям, отличаются друг от друга только значениями в правом столбце. Следовательно справедлива

Теорема 1.1. *Количество всех булевых функций, зависящих от n переменных, равно 2^{2^n} .*

Пусть задана таблица истинности некоторой булевой функции. Как по ней найти формулу, реализующую эту булеву функцию? Ответ на этот вопрос дается в следующем разделе.

1.3 Совершенные нормальные формы

Элементарной конъюнкцией, соответствующей набору переменных $\sigma_1, \dots, \sigma_n$, называется конъюнкция, в которую каждая из переменных x_1, \dots, x_n входит один раз, с отрицанием или без:

$$x_1^{\sigma_1} x_2^{\sigma_2} \dots x_n^{\sigma_n},$$

где

$$x_i^{\sigma_i} = \begin{cases} x_i, & \text{если } \sigma_i = 1, \\ \bar{x}_i, & \text{если } \sigma_i = 0, \quad i = 1, \dots, n. \end{cases}$$

Пример

Набору 001 отвечает элементарная конъюнкция $\bar{x}\bar{y}\&z$ длины три.

Элементарная конъюнкция равна 1 тогда и только тогда, когда значения переменных, входящих без отрицания, равны 1, а значения переменных, входящих с отрицаниями, равны 0. Это обстоятельство подсказывает путь построения функции из заданной таблицы истинности.

Теорема 1.2. *Всякая булева функция, не тождественно равная 0, может быть выражена через дизъюнкцию элементарных конъюнкций, соответствующих тем наборам значений переменных, при которых значение функции равно 1.*

ДОКАЗАТЕЛЬСТВО. Рассмотрим таблицу истинности булевой функции $f(x_1, \dots, x_n)$, $f \neq 0$, и отметим в ней все строки $\sigma_1, \dots, \sigma_n$

такие, что $f(\sigma_1, \dots, \sigma_n) = 1$. Образум для каждой из этих строк элементарную конъюнкцию

$$x_1^{\sigma_1} x_2^{\sigma_2} \dots x_n^{\sigma_n},$$

затем соединим все полученные элементарные конъюнкции посредством дизъюнкций:

$$g(x_1, \dots, x_n) = \bigvee_{\substack{(\sigma_1, \dots, \sigma_n) \\ f(\sigma_1, \dots, \sigma_n) = 1}} x_1^{\sigma_1} x_2^{\sigma_2} \dots x_n^{\sigma_n}.$$

Покажем, что $g = f$. По определению дизъюнкции g принимает значение 1 тогда и только тогда, когда истинен хотя бы один дизъюнктивный член, т. е. хотя бы одна элементарная конъюнкция $x_1^{\sigma_1} x_2^{\sigma_2} \dots x_n^{\sigma_n}$ равняется 1. Но $x_1^{\sigma_1} x_2^{\sigma_2} \dots x_n^{\sigma_n} = 1$, если $(\sigma_1, \dots, \sigma_n)$ такова, что $f(\sigma_1, \dots, \sigma_n) = 1$. Следовательно, множество всех "единиц" функции g (т. е. совокупность всех наборов значений переменных, при которых функция g принимает значение 1) содержится в множестве всех "единиц" булевой функции f .

Обратно: пусть $f(\sigma_1, \dots, \sigma_n) = 1$. Тогда найдется элементарная конъюнкция $x_1^{\sigma_1} x_2^{\sigma_2} \dots x_n^{\sigma_n}$ такая, что она входит в запись формулы g . Следовательно, $g = f$. ∇ (Везде далее в тексте знак ∇ читается "окончание доказательства".)

С учетом того, что функция $x \& \bar{x}$ является тождественно ложной, получили, что каждую булеву функцию можно выразить в виде формулы через отрицание, конъюнкцию и дизъюнкцию, причем отрицания стоят только над переменными.

Элементарной дизъюнкцией, соответствующей набору переменных $\sigma_1, \dots, \sigma_n$, называется дизъюнкция, в которую каждая из переменных x_1, \dots, x_n входит один раз, с отрицанием или без отрицания:

$$x_1^{\bar{\sigma}_1} \vee x_2^{\bar{\sigma}_2} \vee \dots \vee x_n^{\bar{\sigma}_n},$$

где

$$x_i^{\bar{\sigma}_i} = \begin{cases} x_i, & \text{если } \sigma_i = 0, \\ \bar{x}_i, & \text{если } \sigma_i = 1, \end{cases} \quad i = 1, \dots, n.$$

Элементарная дизъюнкция равна 0 тогда и только тогда, когда значения переменных, входящих без отрицания, равны 0, а значения переменных, входящих с отрицаниями, равны 1.

Пример

Элементарная дизъюнкция $x \vee y \vee \bar{z}$ равна 0 тогда и только тогда, когда $x = 0, y = 0, z = 1$.

Аналогично теореме 1.2 доказывается

Теорема 1.3. *Всякая булева функция, не тождественно равная 1, может быть выражена через конъюнкцию элементарных дизъюнкций, соответствующих тем наборам значений переменных, при которых значение функции равно 0.*

Будем говорить, что булева функция $f(x_1, \dots, x_n)$ записана в *совершенной дизъюнктивной нормальной форме* (с. д. н. ф.), если она представлена в виде дизъюнкции попарно различных элементарных конъюнкций, каждая из которых зависит от всех переменных x_1, \dots, x_n .

Аналогично, булева функция $f(x_1, \dots, x_n)$ записана в *совершенной конъюнктивной нормальной форме* (с. к. н. ф.), если она представлена в виде конъюнкции попарно различных элементарных дизъюнкций, каждая из которых зависит от всех переменных x_1, \dots, x_n .

В этих терминах результаты теорем 1.2 и 1.3 сводятся в один.

Теорема 1.4. *Всякая булева функция, не являющаяся константой, эквивалентна:*

- 1) некоторой булевой функции, записанной в с. д. н. ф.;
- 2) некоторой булевой функции, записанной в с. к. н. ф.

1.4 Двойственность, монотонность, линейность. Замкнутые классы

Булева функция

$$f^*(x_1, \dots, x_n) = \bar{f}(\bar{x}_1, \dots, \bar{x}_n)$$

называется *двойственной* к булевой функции $f(x_1, \dots, x_n)$. Если $f = f^*$, то f называется *самодвойственной*. Множество всех самодвойственных булевых функций обозначим через \mathcal{S} .

Примеры

$$x^* = \bar{x} = x;$$

$$(x \vee y)^* = \bar{x} \bar{y} = \bar{x} \& \bar{y} = x \& y.$$

Следующая теорема позволяет находить формулу, реализующую двойственную булеву функцию Φ^* , если известна формула, реализующая исходную булеву функцию Φ .

Теорема 1.5. *Если*

$$\Phi(x_1, \dots, x_n) = f(f_1(x_{11}, \dots, x_{1p_1}), \dots, f_m(x_{m1}, \dots, x_{mp_m})),$$

то

$$\Phi^*(x_1, \dots, x_n) = f^*(f_1^*(x_{11}, \dots, x_{1p_1}), \dots, f_m^*(x_{m1}, \dots, x_{mp_m})).$$

ДОКАЗАТЕЛЬСТВО.

$$\begin{aligned}
\Phi^*(x_1, \dots, x_n) &= \overline{\Phi}(\overline{x}_1, \dots, \overline{x}_n) = \\
&= \overline{f}(f_1(\overline{x}_{11}, \dots, \overline{x}_{1p_1}), \dots, f_m(\overline{x}_{m1}, \dots, \overline{x}_{mp_m})) = \\
&= \overline{f}(\overline{f}_1(\overline{x}_{11}, \dots, \overline{x}_{1p_1}), \dots, \overline{f}_m(\overline{x}_{m1}, \dots, \overline{x}_{mp_m})) = \\
&= f^*(\overline{f}_1(\overline{x}_{11}, \dots, \overline{x}_{1p_1}), \dots, \overline{f}_m(\overline{x}_{m1}, \dots, \overline{x}_{mp_m})) = \\
&= f^*(f_1^*(x_{11}, \dots, x_{1p_1}), \dots, f_m^*(x_{m1}, \dots, x_{mp_m})). \quad \nabla
\end{aligned}$$

Отсюда вытекает

Принцип двойственности. Если некоторая формула $A(f_1, \dots, f_m)$ реализует функцию $\Phi(x_1, \dots, x_n)$, то формула $A(f_1^*, \dots, f_m^*)$, полученная заменой f_i на f_i^* , $i = 1, \dots, m$, реализует функцию $\Phi^*(x_1, \dots, x_n)$, двойственную к $\Phi(x_1, \dots, x_n)$.

Для формул над множеством $\{0, 1, \overline{x}, x_1 \& x_2, x_1 \vee x_2\}$ принцип двойственности состоит в следующем: для получения формулы A^* , двойственной к формуле A , необходимо везде в формуле A сделать замены: 0 на 1, 1 на 0, & на \vee , \vee на &.

Пример

Для формулы $x_1 \& \overline{x}_2$ получаем $x_1 \vee \overline{x}_2$.

Замыканием множества R булевых функций называется совокупность всех булевых функций, полученных суперпозициями функций из R . Замыкание множества R обозначим через $[R]$. Класс функций назовем замкнутым, если $R = [R]$.

Нетрудно убедиться, что класс всех самодвойственных функций \mathcal{S} замкнут.

Пусть $a = (a_1, \dots, a_n)$, $b = (b_1, \dots, b_n) \in E^n$ (множеству всех двоичных наборов длины n). Будем говорить, что набор a предшествует набору b , и писать $a \preceq b$, если для любого $i = 1, \dots, n$ выполняется $a_i \leq b_i$.

Функцию $f(x_1, \dots, x_n)$ будем называть *монотонной*, если для любых наборов a, b значений переменных из неравенства $a \preceq b$ вытекает неравенство $f(a) \leq f(b)$.

Обозначим множество всех монотонных булевых функций через \mathcal{M} .

Примеры

$xy, x \vee y \in \mathcal{M}$.

Теорема 1.6. Класс \mathcal{M} замкнут.

ДОКАЗАТЕЛЬСТВО. Докажем, что суперпозиция монотонных функций является монотонной функцией, т. е.

$$f(x_1, \dots, x_n) = f_0(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)),$$

где $f_0, f_1, \dots, f_m \in M$.

Пусть $a, b \in E^n$ и справедливо $a \preceq b$. Пусть $c_i = f_i(a)$, $d_i = f_i(b)$, $i = 1, \dots, m$, и $c = (c_1, \dots, c_m)$, $d = (d_1, \dots, d_m)$.

Тогда, в силу монотонности функций f_1, \dots, f_m , имеем $c_1 \leq d_1, \dots, c_m \leq d_m$, т.е. $c \preceq d$. В силу монотонности f_0 справедливо $f_0(c) \leq f_0(d)$. Но т. к. $f(a) = f_0(c)$, а $f(b) = f_0(d)$, то $f(a) \leq f(b)$, где $a \preceq b$. Тем самым замкнутость M установлена. ∇

Булева функция называется *линейной*, если

$$f(x_1, \dots, x_n) = a_0 \oplus a_1 x_1 \oplus \dots \oplus a_n x_n,$$

где $a_i \in \{0, 1\}$, $i = 0, 1, \dots, n$.

Обозначим класс линейных функций через \mathcal{L} . Из определения следует, что \mathcal{L} замкнут.

Через \mathcal{T}_0 (\mathcal{T}_1) обозначим множество всех таких булевых функций $f(x_1, \dots, x_n)$, которые *сохраняют константу 0* (1):

$$f(0, 0, \dots, 0) = 0 \quad (f(1, 1, \dots, 1) = 1).$$

Нетрудно убедиться, что $\mathcal{T}_0 = [\mathcal{T}_0]$ и $\mathcal{T}_1 = [\mathcal{T}_1]$.

1.5 Критерий полноты

Система булевых функций называется *полной*, если любая булева функция может быть записана в виде формулы через функции этой системы.

Пример

Система функций $\{\bar{x}, x \& y, x \vee y\}$ полна.

Для доказательства критерия полноты (теоремы Поста) потребуются четыре леммы.

Лемма 1.7. (О несамодвойственной функции.) *Из несамодвойственной функции путем подстановки функций x, \bar{x} можно получить константу (несамодвойственную функцию одной переменной).*

ДОКАЗАТЕЛЬСТВО. Пусть $f(x_1, \dots, x_n) \notin \mathcal{S}$, тогда существует набор (a_1, \dots, a_n) такой, что

$$f(a_1, \dots, a_n) = f(\bar{a}_1, \dots, \bar{a}_n).$$

Положим $\varphi_i(x) = x^{a_i}$ для $i = 1, \dots, n$ и

$$\varphi(x) = f(\varphi_1(x), \varphi_2(x), \dots, \varphi_n(x)).$$

Тогда

$$\begin{aligned} \varphi(0) &= f(\varphi_1(0), \varphi_2(0), \dots, \varphi_n(0)) = \\ &= f(0^{a_1}, \dots, 0^{a_n}) = f(\bar{a}_1, \dots, \bar{a}_n) = \\ &= f(a_1, \dots, a_n) = f(1^{a_1}, \dots, 1^{a_n}) = \\ &= f(\varphi_1(1), \varphi_2(1), \dots, \varphi_n(1)) = \varphi(1). \end{aligned}$$

Таким образом, $\varphi(0) = \varphi(1)$, т. е. $\varphi(x)$ константа. ∇

Лемма 1.8. (О немонотонной функции.) Из немонотонной функции путем подстановки функций $0, 1, x$ можно получить функцию \bar{x} .

ДОКАЗАТЕЛЬСТВО. Пусть $f(x_1, \dots, x_n) \notin \mathcal{M}$. Тогда существуют наборы (a_1, \dots, a_n) и (b_1, \dots, b_n) такие, что $a \preceq b$, но $f(a) > f(b)$.

Заменим в $f(x_1, \dots, x_n)$ константой 0 все переменные x_i , для которых $a_i = b_i = 0$, константой 1 все переменные x_j , для которых $a_j = b_j = 1$, и переменной x все остальные переменные. Получим функцию $g(x)$ такую, что $g(0) > g(1)$, т. е. $g(x) = \bar{x}$. ∇

Из полноты системы функций $\{\bar{x}, xy\}$ и из того, что $\bar{x} = x \oplus 1$, следует полнота системы $\{1, x \oplus y, xy\}$. Следовательно, любая булева функция может быть записана в виде формулы через функции этой системы. Раскрывая скобки и преобразуя, получим полином по mod 2, называемый *полиномом Жегалкина*:

$$a \oplus \sum_{(i_1, \dots, i_s)} a_{i_1, \dots, i_s} x_{i_1} \cdot \dots \cdot x_{i_s},$$

где $a, a_{i_1, \dots, i_s} \in \{0, 1\}$.

Лемма 1.9. (О нелинейной функции.) Из нелинейной функции путем подстановки функций $0, x$ можно получить нелинейную функцию от двух переменных.

ДОКАЗАТЕЛЬСТВО. Рассмотрим полином Жегалкина для нелинейной функции f

$$f(x_1, \dots, x_n) = a \oplus \sum_{(i_1, \dots, i_s)} a_{i_1, \dots, i_s} x_{i_1} \cdot \dots \cdot x_{i_s}.$$

В силу нелинейности f в нем есть нелинейные слагаемые. Рассмотрим нелинейное слагаемое наименьшей степени: пусть, например, оно имеет вид $x_1 \dots x_r$, $r \geq 2$. Заменим в $f(x_1, \dots, x_n)$ переменную x_1 на x , переменные x_2, \dots, x_r на y , остальные – константой 0. Тогда

$$g(x, y) = f(x, y, \dots, y, 0, \dots, 0) \notin \mathcal{L}. \quad \nabla$$

Лемма 1.10. *Из нелинейной функции от двух переменных путем подстановки функций x, \bar{x} можно получить одну из функций $xy, xy \oplus 1$.*

ДОКАЗАТЕЛЬСТВО. Поскольку $g(x, y) \notin \mathcal{L}$, имеем $g(x, y) = xy \oplus ax \oplus by \oplus c$, где $a, b, c \in \{0, 1\}$. Полагая $q(x, y) = g(x \oplus b, y \oplus a)$, получаем

$$q(x, y) = (x \oplus b)(y \oplus a) \oplus a(x \oplus b) \oplus b(y \oplus a) \oplus c = xy \oplus ab \oplus c \in \{xy, xy \oplus 1\}. \quad \nabla$$

Теорема 1.11. (Теорема Поста.) Для того чтобы система функций B была полной, необходимо и достаточно, чтобы она целиком не содержалась ни в одном из пяти замкнутых классов $\mathcal{S}, \mathcal{M}, \mathcal{L}, \mathcal{T}_0, \mathcal{T}_1$.

ДОКАЗАТЕЛЬСТВО. Необходимость. Пусть B полна в \mathcal{P}_2 , т. е. $[B] = \mathcal{P}_2$. Если бы B целиком содержалась в одном из замкнутых классов $\mathcal{S}, \mathcal{M}, \mathcal{L}, \mathcal{T}_0$ или \mathcal{T}_1 (обозначим его через R), то $[B] = R$ и, следовательно, $[R] = \mathcal{P}_2$. Но каждый из классов $\mathcal{S}, \mathcal{M}, \mathcal{L}, \mathcal{T}_0$ и \mathcal{T}_1 отличен от \mathcal{P}_2 .

Достаточность. Пусть система функций B целиком не содержится ни в одном из классов $\mathcal{S}, \mathcal{M}, \mathcal{L}, \mathcal{T}_0, \mathcal{T}_1$. Тогда в B можно выбрать такие функции $f_S, f_M, f_L, f_{T_0}, f_{T_1}$, что $f_S \notin \mathcal{S}, f_M \notin \mathcal{M}, f_L \notin \mathcal{L}, f_{T_0} \notin \mathcal{T}_0, f_{T_1} \notin \mathcal{T}_1$ (среди этих функций могут быть одинаковые).

Положим $B' = \{f_S, f_M, f_L, f_{T_0}, f_{T_1}\}$. Покажем, что $[B'] = \mathcal{P}_2$ (отсюда немедленно следует $[B] = \mathcal{P}_2$, поскольку $B' \subseteq B$).

1. Сначала получим константы и функцию \bar{x} . Так как $f_{T_1} \notin \mathcal{T}_1, f_{T_0} \notin \mathcal{T}_0$, то $f_{T_1}(1, \dots, 1) = 0, f_{T_0}(0, \dots, 0) = 1$. Положим

$$\varphi_1(x) = f_{T_1}(x, \dots, x), \varphi_0(x) = f_{T_0}(x, \dots, x).$$

Тогда $\varphi_1(x)$ есть одна из функций 0 или \bar{x} , $\varphi_0(x)$ – одна из функций 1 или \bar{x} .

1а. Пусть $\varphi_1(x) \equiv 0, \varphi_0(x) \equiv 1$. Тогда по лемме 1.8 из $\varphi_1(x), \varphi_0(x)$ и немонотонной функции f_M получаем функцию \bar{x} .

1б. Пусть хотя бы одна из функций $\varphi_1(x), \varphi_0(x)$ есть \bar{x} . Тогда согласно лемме 1.7 получим одну константу суперпозицией функций \bar{x} и f_S , вторую константу получим как отрицание первой.

2. Используя константы 0 и 1, функцию \bar{x} и нелинейную функцию f_L , на основе лемм 1.9 и 1.10 строим одну из функций xy или $xy \oplus 1$.

Таким образом, формулами над B' реализованы функции \bar{x} и xy (так как $xy = \overline{xy \oplus 1}$), которые образуют полную в \mathcal{P}_2 систему функций. Отсюда $[B'] = \mathcal{P}_2$ и, следовательно, $[B] = \mathcal{P}_2$. ∇

1.6 Применение алгебры высказываний в теории множеств

Будем рассматривать всевозможные подмножества некоторого фиксированного множества U .

Пусть $A(a_1, \dots, a_n)$ – некоторая формула алгебры высказываний от переменных a_1, \dots, a_n , в записи которой встречаются только $\&, \vee, \neg$. Обозначим через $A^*(x)$ высказывание, полученное из A подстановками выражений $x \in X_1, \dots, x \in X_n$ вместо переменных a_1, \dots, a_n соответственно. Обозначим через Z_A множество, полученное из A вследствие следующих процедур замен: переменные a_1, \dots, a_n заменим соответственно на множества X_1, \dots, X_n ; логические операции заменим на теоретико-множественные: $\&$ на пересечение \cap , \vee на объединение \cup , \neg на дополнение $-$.

Пример

$A = a\&b\vee\bar{c}$. Тогда

$$A^*(x) = x \in X_1 \& x \in X_2 \vee x \in \overline{X_3},$$

$$Z_A = X_1 \cap X_2 \cup \overline{X_3}.$$

Теорема 1.12. *Высказывание $A^*(x)$ истинно для элемента $x \in U$ и множеств X_1, \dots, X_n тогда и только тогда, когда $x \in Z_A$.*

ДОКАЗАТЕЛЬСТВО. Рассмотрим формулу A и назовем длиной A число вхождений символов $\&, \vee, \neg$ в A .

Доказательство будем вести индукцией по длине формулы A .

1. Длина формулы A равна 0, т. е. $A = a$, где a – элементарное высказывание. Тогда $A^*(x) = x \in X$ и $Z_A = X$. Теорема утверждает, что

$$x \in X \iff x \in X.$$

2. Пусть для всех формул с длиной меньше или равной n теорема справедлива и длина формулы A равна $n + 1$. Тогда формула A может иметь один из следующих видов:

$$A = B\&C, \quad A = B\vee C, \quad A = \bar{B},$$

где B и C – формулы длины меньшей или равной n . По индукционному предположению для B и C имеем

$$B^*(x) \iff x \in Z_B,$$

$$C^*(x) \iff x \in Z_C.$$

Пусть для A имеем вариант

$$A^*(x) = B^*(x) \& C^*(x),$$

а также $Z_A = Z_B \cap Z_C$. Тогда

$$A^*(x) = \text{И} \iff B^*(x) \& C^*(x) = \text{И} \iff x \in Z_B \& x \in Z_C \iff$$

$$\iff x \in Z_B \cap x \in Z_C \iff x \in Z_A.$$

Аналогично рассматриваются случаи, когда

$$A^*(x) = B^*(x) \vee C^*(x),$$

$$A^*(x) = \overline{B^*(x)}. \quad \nabla$$

Эта теорема позволяет по теоремам логики высказываний получать теоремы теории множеств, например:

1) $A = \overline{a \vee \bar{a}} \equiv 0$, тогда $Z_A = \overline{X \vee \bar{X}} = \emptyset$ для любого подмножества X множества U ;

2) $a \& (b \vee c) = (a \& b) \vee (a \& c)$, тогда в теории множеств имеем $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$.

1.7 Понятие о предикатах

В повседневной жизни мы часто используем *предикаты*.

Примеры

1. Предикаты используются в контрольных утверждениях языков программирования, например выражение "if $x \leq y$ then $z \rightarrow t$ " содержит предикат \leq .

2. Предложение *Некто написал роман "Мать"* есть предикат, так как о нем можно судить, истинно оно или ложно, подставив вместо "некто" имя конкретного человека.

3. Рассмотрим уравнение $x + 2y = 23$. Если $(x, y) = (3, 10)$, то предикат $x + 2y = 23$ превращается в истинное высказывание.

Некоторым предикатам математики отвели специальные обозначения, например предикатам $=, >, \leq$.

Пусть

$$A^n = A \times \dots \times A = \{(a_1, \dots, a_n) : a_i \in A, i = 1, \dots, n\} -$$

n -я декартова степень множества A .

Предикат $P(x_1, \dots, x_n)$ - это функция, отображающая множество A^n во множество $\{И,Л\}$ (или во множество $\{1, 0\}$), где A - произвольное множество.

Чтобы задать предикат, надо *указать множество* A^n - область определения предиката. Множество $B, B \subseteq A^n$, на котором предикат $P(x_1, \dots, x_n)$ принимает значение И, называется *областью истинности* предиката. Если предикат $P(x_1, \dots, x_n)$ принимает значение $P(c_1, \dots, c_n) = И$ для любого $(c_1, \dots, c_n) \in A$, то говорят, что предикат P *истинен* на A^n ; если существует такой набор $P(c_1, \dots, c_n)$, что $P(c_1, \dots, c_n) = И$, то говорят, что P *выполним* на A^n . То есть предикат $P(c_1, \dots, c_n)$ понимают как высказывание "упорядоченный набор (c_1, \dots, c_n) принадлежит B ".

Таким образом, предикат $P(x_1, \dots, x_n)$ является *отношением* на множестве A^n .

При $n = 1$ предикат P называется *одноместным* или свойством (или его рассматривают как отношение объекта с самим собой). При $n > 1$ предикат P называют отношением (бинарным, тернарным и т. д.).

Примеры

1. Предикат $>$ является бинарным отношением.
2. Предикат \neg - одноместный предикат на множестве $\{0, 1\}$.
3. Функции алгебры высказываний $\&$, \vee являются двуместными предикатами, определенными на множестве $\{0, 1\}^2$.

Любую n - местную функцию можно сделать $(n + 1)$ - местным предикатом.

Пример

Функции $f(x, y) = x + y$ отвечает предикат $S(x, y, z)$, равный 1, если $x + y = z$ с соответствующей областью определения: это либо N^3 , либо R^3 , либо D^3 и т. д. В N^3 имеем

$$S(2, 3, 5) = И, S(2, 3, 7) = Л.$$

Чтобы превратить предикат в высказывание, надо *связать* его переменные, т. е. придать им конкретные значения или "навесить" на переменные кванторы.

Если $P(x_1, \dots, x_n)$ - предикат от переменных x_1, \dots, x_n , то

$$\forall x_1 P(x_1, \dots, x_n)$$

читается как "для любого x верно $P(x_1, \dots, x_n)$ ", например предикат $\forall y S(x, y, y)$ читается "для любого y справедливо отношение $x + y = y$ ". Этот предикат принимает значение И тогда и только тогда, когда $x = 0$.

На переменные можно "навешивать" квантор существования \exists . Выражение

$$\exists x P(x)$$

читается как "существует x такой, что $P(x)$ истинно на области определения предиката $P(x)$ ".

Пример

$\exists y S(y, y, x)$ читается как "найдется y такое, что истинно $S(y, y, x)$ " (т. е. $y + y = x$) – предикат принимает значение И на N^3 тогда и только тогда, когда x четно.

Если область определения предиката конечна, то иногда удобно заменить навешивание кванторов высказываниями, в которых переменным приданы конкретные значения.

Пример

Пусть $A = \{1, 2, 3\}$ и на A задан одноместный предикат $P(x)$, тогда $\forall x P(x)$ эквивалентно $P(1) \& P(2) \& P(3)$;

$\exists x P(x)$ эквивалентно $P(1) \vee P(2) \vee P(3)$.

При использовании нескольких кванторов существен их порядок.

Из предикатов, используя логические связки, кванторы \exists , \forall и скобки, можно строить сложные предикаты (с учетом области определения).

1.8 Синтез схем (π -схемы, контактные схемы, схемы из функциональных элементов)

Речь пойдет о моделях, вычисляющих булевы функции. Интерес к построению этих моделей, изучению их свойств и функционированию диктуется практическими вычислительными задачами. Для многих задач важно не просто составить программу или построить устройство, но еще и добиться экономичности и надежности этих объектов. Например, необходимо решить задачу экономного построения отдельных блоков ЭВМ. При этом возникают такие естественные меры сложности, как число элементов в схеме, число букв в формуле, число контактов в контактной схеме, число конъюнкций в д. н. ф., глубина схемы (максимальная длина цепочки, по которой сигнал проходит от входа до выхода схемы) и т. д.

Важно также при этом удачно выбрать язык описания алгоритмов и схем. Имеющиеся языки программирования удобны при разработке алгоритмов, но для доказательства существования или несуществования

экономных алгоритмов они малопригодны. Поэтому желательно иметь дело с простейшими *моделями* алгоритмов, позволяющими анализировать алгоритмы.

В качестве таких моделей можно указать булевы формулы, д. н. ф., с которыми мы уже познакомились, а также контактные схемы, π -схемы, схемы из функциональных элементов и т. д.

Одни модели удобнее при исследовании объема вычислительного устройства, например число элементов в сумматоре ЭВМ. Другие модели лучше приспособлены для изучения сложности программных вычислений (времени работы программы или требуемой его рабочей памяти).

Модель вычислений, или *управляющая система*, состоит из схемы и вычисляемой ею функции. *Схема* – это объект, построенный по определенным правилам и служащий для вычисления функции. Будем рассматривать схемы, вычисляющие булевы функции (далее б. ф.), поскольку эти функции сочетают предельную простоту с универсальностью. Достаточно заметить, что любая программа современной ЭВМ фактически вычисляет совокупность б. ф.

- 1. С формулами, реализующими б. ф. в некотором базисе, мы уже познакомились. Мы узнали, что существует очень много различных базисов, познакомились с критерием полноты систем функций, научились выражать одни базисы через другие.

- 2. Вторая модель вычислений – это реализация б. ф. с помощью д. н. ф., т. е. частный случай реализации б. ф. в базисе $\{\&, \vee, \neg\}$. Этот базис очень удобен в исследованиях и изучениях б. ф., так как с помощью принципа двойственности позволяет в формуле "спустить" отрицания до переменных, произведя эквивалентные преобразования. Язык формул является весьма естественным для аналитического задания б. ф.

Как для любой б. ф. построить формулу, ее реализующую? Ответ на этот вопрос дает теорема 1.2 о представлении любой б. ф., не равной тождественно 0, с помощью с. д. н. ф. Б. ф., тождественно равную 0, можно представить формулой $x \& \bar{x} \equiv 0$. Если же стремиться построить экономную формулу, то этот вопрос становится *очень сложным*. Данному вопросу посвящено множество статей, монографий.

- 3. Следующая модель вычисления или управляющая система, которую мы рассмотрим, – это наиболее "древний" класс управляющих систем, введенный К.Шенноном в 1938 г.

Контактная схема – это устройство из контактов и проводов, связывающих *полюсы* схемы (вход и выход).

Рабочему состоянию контакта ставим в соответствие 1, нерабочему – 0, наличию тока – 1, отсутствию тока – 0.

Контакты различают замыкающие и размыкающие: контакт *замы-*

кающий, если в рабочем состоянии (кнопка нажата), он замыкает цепь. Замыкающему контакту естественным образом отвечает булева функция $\varphi(x) = x$.

Контакт *размыкающий*, если он замыкает цепь в нерабочем состоянии. Размыкающему контакту отвечает булева функция $\varphi(x) = \bar{x}$.

Последовательно соединенные контакты реализуют конъюнкцию: $x_1 \& x_2$, параллельно соединенные контакты реализуют дизъюнкцию: $x_1 \vee x_2$.

Если произвольная цепь C без самопересечений, соединяющая вход и выход схемы (полюсы схемы), содержит контакты $x_{i_1}^{\sigma_1}, \dots, x_{i_k}^{\sigma_k}$ и только их, то этой цепи сопоставляется конъюнкция $K_c = x_{i_1}^{\sigma_1} \dots x_{i_k}^{\sigma_k}$. Контактная схема S реализует по определению б. ф.

$$\bigvee_c K_c,$$

где \vee берется по всем цепям *без самопересечений*, соединяющим полюсы контактной схемы.

Функция, реализуемая контактной схемой, является функцией *проводимости схемы*. Функция равна 1 тогда и только тогда, когда есть проводящая цепь между полюсами схемы.

• 4. Самостоятельный интерес представляет подкласс контактных схем – параллельно-последовательные контактные схемы (π -схемы). Приведем их индуктивное определение:

- а) один контакт (a, b) есть π -схема с полюсами a и b ;
- б) если $S_1(a_1, b_1)$ и $S_2(a_2, b_2)$ – π -схемы, то схема $S(a, b)$, полученная отождествлением (склеиванием) полюсов a_1 с a_2 и b_1 с b_2 , есть π -схема (параллельное соединение π -схем S_1 и S_2) с полюсами $a = a_1 = a_2$, $b = b_1 = b_2$;
- в) схема $S(a, b)$, полученная склеиванием полюса a_2 с b_1 , есть π -схема (последовательное соединение π -схем) с полюсами a_1 и b_2 ;
- г) других π -схем нет.

π -Схеме естественным образом отвечает д. н. ф. Отметим, что π -схемы изоморфны формулам д. н. ф., так как функция, реализуемая π -схемой и соответствующая ей д. н. ф., совпадают. Однако π -схемы весьма *наглядны*, что часто позволяет эффективно исследовать именно их, а не д. н. ф. Существуют разные алгоритмы минимизации π -схем, контактных схем.

Как правило, контактные схемы содержат меньше контактов, чем эквивалентные им π -схемы, поэтому бывает удобнее иногда рассматривать реализацию б. ф. именно контактной схемой.

• 5. Дадим определение схемы, состоящей из функциональных элементов (с. ф. э.). Эти схемы более экономны, чем описанные выше, поскольку выход любого элемента может быть использован многократно.

Для определения (с. ф. э.) нам потребуется определение графа, а также ориентированного графа.

Пусть V – произвольное множество, U – множество некоторых его пар элементов. Совокупность $G = (V, U)$ называется графом с множеством вершин V и множеством ребер U . Граф ориентированный, если каждая пара $(x, y) \in U$ упорядочена.

Пусть G – произвольный конечный ориентированный граф без ориентированных циклов, в каждую вершину которого входит не более двух дуг.

Вершины, в которые не входят дуги, называются входами (полюсами), остальные вершины внутренние, некоторые вершины пометим как выходные.

Каждому полюсу припишем букву алфавита $\{x_1, \dots, x_n\}$, каждой внутренней вершине с одной входящей дугой – \neg , вершине с двумя входящими дугами – $\&$ или \vee . Булева операция, приписанная вершине a , вместе с этой вершиной называется *функциональным элементом*: если \neg , то инвертор; если $\&$, то конъюнктор; если \vee , то дизъюнктор.

Ориентированный граф такого специального вида с помеченными описанным образом вершинами называется *схемой из функциональных элементов*.

Каждой вершине схемы можно приписать булеву функцию, которую она реализует. Каждому полюсу x_i приписываем функцию x_i . Пусть некоторой вершине a схемы предшествуют вершины b и c , которым приписаны функции $f_b(x_1, \dots, x_n)$ и $f_c(x_1, \dots, x_n)$. Если a помечена в схеме $\&$ (\vee), то ей приписываем функцию $f_b \& f_c$ ($f_b \vee f_c$). Если в a входит только дуга из b , то приписываем $\neg f_b$. Про эту функцию будем говорить, что она *вычисляется (реализуется) схемой S в вершине a* .

Важнейшие ресурсы при программировании – это время и память ЭВМ, и часто на практике остро встает вопрос о вычислительных ресурсах, т. е. возникает задача оптимизации программ. Оптимизировать ее можно по времени, по памяти и т. д.

При схемных вычислениях сложность характеризуется числом (и, возможно, качеством) элементов.

Пусть $L_{\Phi}(F)$ – число вхождений символов переменных и констант в формулу F .

Формула (схема), имеющая минимальную сложность среди всех эквивалентных ей формул (схем), называется *минимальной*.

Сложностью б. ф. f в классе формул (схем) (обозначим $L_{\Phi(f)}$) называется сложность минимальной формулы (схемы), реализующей f . Положим

$$L_{\Phi(n)} = \max_{f \in \mathcal{P}_2} L_{\Phi(f)}.$$

Функция $L_{\Phi(n)}$ называется функцией Шеннона. Она равна сложности самой сложной функции от n переменных.

Аналогично определяется сложность функции и функция Шеннона для других классов схем.

Оценкам сложности б. ф. и построению экономных схем, реализующих б. ф., посвящен большой раздел дискретной математики – синтез схем.

Обычно существует тривиальный метод нахождения самой экономной (минимальной) схемы, реализующей данную функцию. Этот метод связан с перебором всех схем определенной сложности, но он малоэффективен, так как для его осуществления требуется много шагов.

В 1949 г. Клодом Шенноном было предложено *найти метод синтеза схем, позволяющий для любой функции от n переменных строить формулу (схему), для которой $L_{\Phi(F)}$ была бы близка к $L_{\Phi(n)}$* , например, $L_{\Phi(F)} \leq C L_{\Phi(n)}$, где C – некоторая константа.

2 ЭЛЕМЕНТЫ КОМБИНАТОРИКИ

2.1 Подсчет числа отображений конечных множеств в конечные множества с различными элементами

Введем несколько обозначений.

Для любого натурального n через $n!$ (читается *n -факториал*) обозначается произведение $1 \cdot 2 \cdot 3 \cdot \dots \cdot n$. По определению полагается $0! = 1$.

Для любого действительного x и для любого натурального k *убывающим факториалом* $[x]_k$ называется произведение

$$x(x-1)(x-2) \cdots (x-k+1).$$

При натуральном x это произведение называется также *числом размещений из x элементов по k элементов* и обозначается A_x^k .

Для действительного x и натурального k положим

$$\binom{x}{k} = \frac{[x]_k}{k!}, \quad \binom{k}{0} = 1.$$

При натуральном x это называется *числом сочетаний из x элементов по k элементов* и обозначается также C_x^k .

Ряд комбинаторных задач о числе перестановок, размещений, сочетаний и т. п. можно интерпретировать как задачи о числе различного вида отображений конечных множеств в конечные множества.

В дальнейшем $X = \{x_1, \dots, x_m\}, Y = \{y_1, \dots, y_n\}$. Если пишем \tilde{X} (соответственно \tilde{Y}), это значит, что элементы X (соответственно Y) неразличимы.

Утверждение 2.1. *Число всех отображений $f : X \rightarrow Y$ равно n^m .*

ДОКАЗАТЕЛЬСТВО. Рассмотрим построение f как поэтапный процесс. На первом шаге выбираем $f(x_1)$, на втором – $f(x_2)$ и т. д. На каждом из m шагов имеется n возможностей. Таким образом, общее количество разных последовательностей выборов равно n^m . Но разным последовательностям выборов соответствуют разные функции. ∇

Примеры

1. Удобно представлять отображение $f : X \rightarrow Y$ как раскладывание m помеченных шаров в n различных ящиков.

2. Пусть требуется подсчитать число m -мерных векторов, каждая координата которых может принимать любое значение из $Y = \{y_1, \dots, y_n\}$. Очевидно, эта задача эквивалентна предыдущей.

3. Пусть производится m опытов (называемых *упорядоченными выборками с возвращениями*), состоящих в том, что из *генеральной совокупности* Y наудачу выбирается какой-нибудь элемент y_i , результат опыта фиксируется, а затем элемент возвращается в генеральную совокупность. Понятно, что, поставив последовательности $\{y_{i_1}, \dots, y_{i_m}\}$ исходов этих опытов в соответствие вектор $\{y_{i_1}, \dots, y_{i_m}\}$, получим взаимно однозначное соответствие между множеством различных последовательностей исходов наших опытов и множеством m -мерных векторов с координатами из Y . Таким образом, число упорядоченных выборок с возвращениями подсчитывается по той же схеме.

Утверждение 2.2. *Число всех инъективных (т.е. таких, при которых образы разных элементов различны) отображений $f : X \rightarrow Y$ равно $[n]_m$.*

ДОКАЗАТЕЛЬСТВО. Как и при доказательстве утверждения 2.1, для выбора $f(x_1)$ имеется n возможностей. Но после этого для выбора $f(x_2)$ в $Y \setminus \{f(x_1)\}$ имеется уже не n , а $n - 1$ возможностей, для выбора $f(x_3)$ имеется $n - 2$ возможностей, и т. д. Следовательно, общее число различных инъективных отображений $f : X \rightarrow Y$ равно $n(n - 1) \cdots (n - m + 1) = [n]_m$. ∇

Примеры

1. Инъективное отображение $f : X \rightarrow Y$ удобно представлять как раскладывание m помеченных шаров в n различных ящиков таким образом, чтобы в каждом ящике было не более одного шара.

2. Пусть производятся опыты (называемые *упорядоченными выборками без возвращения объема m*), состоящие в том, что из генеральной совокупности Y наудачу выбирается какой-нибудь элемент y_i , из оставшегося множества $Y \setminus \{y_i\}$ наудачу выбирается другой элемент, и т. д. (всего m раз). Нетрудно усмотреть соответствие множества исходов этих опытов с раскладыванием m шаров в n разных ящиков.

Следствие 2.3. Число всех биективных отображений $f : X \rightarrow Y$ равно $n!$ при $m = n$ и равно 0 при $m \neq n$.

Пример

Число перестановок чисел $1, \dots, n$ равно $n!$.

Утверждение 2.4. Число m -элементных подмножеств n -элементного множества Y равно $\binom{n}{m}$.

ДОКАЗАТЕЛЬСТВО. Поставим в соответствие каждому инъективному отображению $f : X \rightarrow Y$ множество $f(X)$. Тогда каждому отображению будет соответствовать одно m -элементное подмножество Z множества Y и по следствию 2.3 каждое такое Z соответствует $m!$ различным отображениям. Следовательно, искомое число равно $[n]_m/m! = \binom{n}{m}$. ∇

Для любых натуральных $n \geq m \geq 1$ имеем $\binom{n}{m} = \frac{n!}{m!(n-m)!} = \binom{n}{n-m}$.

Утверждение 2.5. А. Число сюръективных отображений $f : \tilde{X} \rightarrow Y$ (\tilde{X} означает, что элементы X неразличимы) равно $\binom{m-1}{n-1}$;

Б. Число всех отображений $f : \tilde{X} \rightarrow Y$ равно $\binom{n+m-1}{n-1}$; $|X| = m$, $|Y| = n$.

ДОКАЗАТЕЛЬСТВО. Поставим в соответствие каждому сюръективному отображению $f : \tilde{X} \rightarrow Y$ набор из $n - 1$ перегородок в промежутках между m элементами X , расположенными на одной прямой, по следующим правилам. Если $|f^{-1}(y_i)| = a_i$, то i -я перегородка размещается между элементами с номерами $a_1 + \dots + a_i$ и $a_1 + \dots + a_i + 1$. При этом соответствию каждому отображению f сопоставлена одна расстановка перегородок, и наоборот, каждая расстановка сопоставлена какому-то f . Наконец, если f_1 и f_2 различные отображения \tilde{X} на Y , то для некоторого i числа $|f_1^{-1}(y_i)|$ и $|f_2^{-1}(y_i)|$ должны различаться. Но тогда отображениям f_1 и f_2 соответствуют различные расстановки перегородок. Следовательно, число таких расстановок равно числу сюръективных

отображений $f : \tilde{X} \rightarrow Y$. Поскольку имеется $m - 1$ мест, куда можно ставить $n - 1$ перегородок и в каждое место можно ставить лишь одну перегородку, это число равно $\binom{m-1}{n-1}$.

Для доказательства части Б нашего утверждения заметим, что аналогично случаю А имеется взаимно однозначное соответствие между множеством всех отображений $f : \tilde{X} \rightarrow Y$ и множеством таких расстановок $n - 1$ перегородок в $m - 1$ промежутков, что в любой промежуток разрешается ставить любое количество перегородок. Число таких расстановок можно подсчитать следующим образом. Имеется $m + n - 1$ мест для элементов X и перегородок. Ставим на любые $n - 1$ из них перегородки, а на оставшиеся места – элементы X . Число способов сделать это равно $\binom{n+m-1}{n-1}$. ∇

Примеры

1. Число способов раскладывания m одинаковых шаров в n различных ящиков равно $\binom{n+m-1}{n-1}$.
2. Допустим, мы бросаем m одинаковых игральных костей. Тогда можно различить $\binom{m+5}{5}$ разных исходов бросания.
3. Число векторов (y_1, \dots, y_n) в R^n с целочисленными неотрицательными координатами, удовлетворяющими уравнению $y_1 + \dots + y_n = m$, равно $\binom{n+m-1}{n-1}$.
4. Число способов раскладывания m одинаковых шаров в n различных ящиков так, чтобы не было пустых ящиков, равно $\binom{m-1}{n-1}$.

2.2 Разбиения конечных множеств и числа Стирлинга второго рода

Число разбиений m -элементного множества на k непустых подмножеств обозначим через $S(m, k)$ и будем называть его *числом Стирлинга второго рода*.

- Утверждение 2.6.** А. Число сюръективных отображений $f : X \rightarrow \tilde{Y}$ (элементы Y неразличимы) равно $S(m, n)$.
 Б. Число сюръективных отображений $f : X \rightarrow Y$ равно $n!S(m, n)$.
 В. Число всех отображений $f : X \rightarrow \tilde{Y}$ равно $\sum_{k=1}^n S(m, k)$.

ДОКАЗАТЕЛЬСТВО. Каждое отображение f множества X на множество Y порождает разбиение

$$X = f^{-1}(y_1) \cup f^{-1}(y_2) \cup \dots \cup f^{-1}(y_n).$$

Если два отображения f_1 и f_2 порождают одно и то же разбиение, значит существует такая перестановка (i_1, \dots, i_n) чисел $1, \dots, n$, что

$$f_2^{-1}(y_{i_i}) = f_1^{-1}(y_i) \quad i = 1, \dots, n.$$

Это как раз и означает, что если элементы Y неразличимы, то f_1 и f_2 совпадают. Тем самым А доказано.

Любое сюръективное отображение $f : X \rightarrow Y$ можно построить в два этапа: сначала разбить X на n непустых частей X_1, \dots, X_n (имея в виду, что элементы из одной части будут отображаться в один и тот же элемент множества Y), а затем для каждого такого разбиения (X_1, \dots, X_n) выбрать в качестве $f(X_1), \dots, f(X_n)$ различные элементы Y . Согласно А имеется $S(m, n)$ разных исходов первого этапа. Для любого исхода первого этапа имеется $n!$ разных исходов второго этапа. Итого имеется $n!S(m, n)$ возможностей.

Утверждение В следует из А, поскольку при неразличимых элементах Y отображения X на разные подмножества Y , состоящие из одинакового количества элементов, одинаковы. ∇

Утверждение 2.7. А. $S(m, m) = 1$ при $m \geq 0$.

Б. $S(m, 0) = 0$ при $m > 0$.

В. $S(m, k) = S(m - 1, k - 1) + kS(m - 1, k)$ при $0 < k < m$.

ДОКАЗАТЕЛЬСТВО. Утверждения А и Б очевидны. Для доказательства В заметим, что множество R всех разбиений множества $X = \{x_1, \dots, x_m\}$ на n частей распадается на множества $R_1 = \{\pi \in R \mid \text{одноэлементное множество } \{x_m\} \text{ является элементом разбиения}\}$ и $R_2 = R \setminus R_1$.

Очевидно, $|R_1| = S(m - 1, k - 1)$. Поставим в соответствие каждому разбиению $\pi \in R_2$ разбиение π' множества $X \setminus \{x_m\}$, полученное из π удалением элемента x_m из той части, которой он принадлежал. Поскольку каждое разбиение π' множества $X \setminus \{x_m\}$ будет поставлено в соответствие ровно k разбиениям множества X (образованным из π' путем добавления x_m к какой-нибудь из k частей), то $|R_2| = kS(m - 1, k)$. ∇

Доказанные равенства позволяют вычислять значения $S(m, k)$ по *треугольнику Стирлинга*:

$m \setminus k$	0	1	2	3	4	5	6	7
1	0	1						
2	0	1	1					
3	0	1	3	1				
4	0	1	7	6	1			
5	0	1	15	25	10	1		
6	0	1	31	90	65	15	1	
7	0	1	63	301	350	140	21	1

Утверждение 2.8. Для любого $k \geq 2$

$$S(m, k) = \sum_{i=k-1}^{m-1} \binom{m-1}{i} S(i, k-1).$$

ДОКАЗАТЕЛЬСТВО. Пусть (X_1, \dots, X_k) – произвольное разбиение X на k непустых подмножеств, $x_m \in X_k$. Имеется $\binom{m-1}{r-1}$ возможностей выбрать X_k с $|X_k| = r$ и $x_m \in X_k$. После этого останется $S(m-r, k-1)$ возможностей разбить оставшееся множество на $k-1$ непустых подмножеств. Следовательно,

$$S(m, k) = \sum_{r=1}^{m-k+1} \binom{m-1}{r-1} S(m-r, k-1) = \sum_{i=k-1}^{m-1} \binom{m-1}{i} S(i, k-1). \quad \nabla$$

Числом Белла B_n называется число всех разбиений n -элементного множества на непустые подмножества. Ясно, что $B_n = \sum_{i=1}^n S(n, i)$.

Упражнение

Доказать, что $B_{n+1} = \sum_{i=0}^n \binom{n}{i} B_i$. (Полагаем $B_0 = 1$.)

Теорема 2.9. Для каждого $m \geq 0$

$$x^m = \sum_{k=1}^m S(m, k)[x]_k.$$

ДОКАЗАТЕЛЬСТВО. Пусть n – натуральное число. По утверждению 2.1 число отображений $f : X \rightarrow Y$, где $|X| = m$, $|Y| = n$, равно n^m . Подсчитаем это число другим способом. Для каждого $A \subseteq Y$, $A \neq \emptyset$, пусть \mathcal{X}_A – множество отображений $f : X \rightarrow Y$ с $f(X) = A$. Если $|A| = k$, то $|\mathcal{X}_A| = k!S(m, k)$. Следовательно, по утверждению 2.6 Б

$$n^m = \sum_{k=1}^m \binom{n}{k} S(m, k) k! = \sum_{k=1}^m S(m, k) [n]_k.$$

Таким образом, значения многочленов x^m и $\sum_{k=1}^m S(m, k)[x]_k$ совпадают при $x = 1, 2, 3, \dots$. Значит, это один и тот же многочлен. ∇

2.3 Разбиения чисел на слагаемые. Диаграммы Ферре

Рассмотрим теперь отображения \tilde{X} в \tilde{Y} . В этом случае для того, чтобы отображения f_1 и f_2 различались, необходимо, чтобы различались

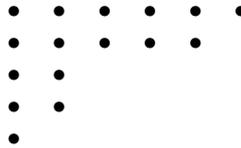
наборы чисел $\{|f_1^{-1}(y_1)|, |f_1^{-1}(y_2)|, \dots, |f_1^{-1}(y_n)|\}$ и $\{|f_2^{-1}(y_1)|, |f_2^{-1}(y_2)|, \dots, |f_2^{-1}(y_n)|\}$ (без учета порядка этих чисел). Таким образом, задача нахождения числа $\tilde{\mathcal{C}}(m, n)$ отображений \tilde{X} в \tilde{Y} эквивалентна нахождению числа разложений натурального числа m в сумму n неотрицательных целых слагаемых (порядок слагаемых не учитывается).

Обозначим через $P(m, k)$ число разбиений m на k натуральных слагаемых, а через $P(m)$ – число разбиений m на натуральные слагаемые. Понятно, что

$$P(m) = \sum_{k=1}^m P(m, k) \quad \forall m > 0,$$

$$\tilde{\mathcal{C}}(m, n) = \sum_{k=1}^n P(m, k).$$

Изучать некоторые свойства $P(m, k)$ помогают *диаграммы Ферре*. Диаграмма Ферре для разложения $m = a_1 + a_2 + \dots + a_k$ (для единообразия считаем, что $a_1 \geq a_2 \geq \dots \geq a_k$) состоит из k строк, где строка i содержит a_i точек, расположенных в столбцах $1, \dots, a_i$. В примере изображена диаграмма Ферре для разложения $16 = 6 + 5 + 2 + 2 + 1$.



Нетрудно убедиться, что каждая диаграмма соответствует в точности одному разложению числа в сумму натуральных слагаемых.

Утверждение 2.10. *А. Число разложений числа m в сумму ровно k слагаемых равно числу представлений m в виде суммы натуральных слагаемых, наибольшее из которых равно k .*

Б. Число представлений m в виде суммы попарно различных (натуральных) слагаемых равно числу представлений m в виде суммы нечетных слагаемых.

ДОКАЗАТЕЛЬСТВО. Докажем А. Поставим в соответствие каждой диаграмме (Ферре) D для разбиения m на k слагаемых двойственную ей диаграмму, полученную "транспонированием" D . Очевидно, "транспонированная" диаграмма отвечает некоторому разложению $m = a_1 + a_2 + \dots + a_s$ с $a_1 = k$. Легко убедиться, что указанное соответствие

взаимно однозначно отображает множество диаграмм с k строками на множество диаграмм с k столбцами. Тем самым А доказано.

Докажем Б. Пусть \mathcal{Q} – множество разложений m в сумму различных слагаемых, а \mathcal{P} – множество разложений m в сумму нечетных слагаемых. Построим отображение $F : \mathcal{Q} \rightarrow \mathcal{P}$ по следующим правилам. Пусть $m = a_1 + a_2 + \dots + a_k$ и $a_1 > a_2 > \dots > a_k$. Каждое из a_i представим в виде $a_i = 2^{c_i} b_i$, где b_i нечетно. Такое представление однозначно. Поставим в соответствие разложению $m = a_1 + a_2 + \dots + a_k$ разложение

$$m = \underbrace{b_1 + b_1 + \dots + b_1}_{2^{c_1} \text{ раз}} + \underbrace{b_2 + b_2 + \dots + b_2}_{2^{c_2} \text{ раз}} + \dots + \underbrace{b_k + b_k + \dots + b_k}_{2^{c_k} \text{ раз}}.$$

Это соответствие обозначим через F .

Теперь построим отображение $G : \mathcal{P} \rightarrow \mathcal{Q}$ по следующим правилам. Пусть дано разложение

$$m = \underbrace{b_1 + b_1 + \dots + b_1}_{d_1 \text{ раз}} + \underbrace{b_2 + b_2 + \dots + b_2}_{d_2 \text{ раз}} + \dots + \underbrace{b_s + b_s + \dots + b_s}_{d_s \text{ раз}} \quad (1)$$

числа m на нечетные слагаемые (из них s различных). Каждое из d_i -х однозначно представимо в виде суммы степеней двойки:

$$d_i = 2^{e_{i,1}} + 2^{e_{i,2}} + \dots + 2^{e_{i,t(i)}}, \text{ где } e_{i,1} > e_{i,2} > \dots > e_{i,t(i)}. \quad (2)$$

Тогда разложение

$$m = \sum_{i=1}^s (2^{e_{i,1}} b_i + 2^{e_{i,2}} b_i + \dots + 2^{e_{i,t(i)}} b_i) \quad (3)$$

представляет m в виде суммы различных слагаемых. Действительно, при одном и том же i слагаемые различны, поскольку различны $e_{i,j}$, а при разных i различны наибольшие нечетные делители чисел. Пусть отображение G сопоставляет каждому разложению вида (1) разложение вида (3).

Из определений следует, что если на некоторое разложение вида (1) подействовать отображением G , а затем на полученное разложение числа m в сумму различных слагаемых подействовать отображением F , то снова получится исходное разложение. В силу однозначности представления (2) из двух несовпадающих разложений числа m на различные слагаемые после действия на них отображения F нельзя получить одно и то же разложение вида (1).

Значит, F и G – взаимно однозначные отображения и $|\mathcal{P}| = |\mathcal{Q}|$. ∇

Утверждение 2.11. Справедливо равенство $P(m, n) = P(m-n, 1) + P(m-n, 2) + \dots + P(m-n, n)$.

ДОКАЗАТЕЛЬСТВО. Пусть $\mathcal{R}(m, n)$ – множество разложений числа m в сумму n натуральных слагаемых, $\mathcal{R}(m, n, k)$ – множество тех разложений из $\mathcal{R}(m, n)$, в которых ровно k слагаемых равны 1. Поставим в соответствие каждому разложению $m-n = a_1 + a_2 + \dots + a_k$ из $\mathcal{R}(m-n, k)$ разложение

$$m = (a_1 + 1) + (a_2 + 1) + \dots + (a_k + 1) + \underbrace{1 + 1 + \dots + 1}_{n-k \text{ раз}}$$

из $\mathcal{R}(m, n, n-k)$. Ясно, что это соответствие взаимно однозначно отображает $\mathcal{R}(m-n, k)$ на $\mathcal{R}(m, n, n-k)$. ∇

Часть изложенных выше результатов суммируется в таблице (напомним, что $|X| = m$, $|Y| = n$).

Отобр.	Произвольные отображения	Инъективные отображения	Сюръект. отобр.	Биект. отобр.
$X \rightarrow Y$	n^m	$[n]_m$	$n!S(m, n)$	$n!$
$\tilde{X} \rightarrow Y$	$\binom{n+m-1}{m}$	$\binom{n}{m}$	$\binom{m-1}{n-1}$	1
$X \rightarrow \tilde{Y}$	$\sum_{k=1}^n S(m, k)$	0, если $m > n$ 1, если $m \leq n$	$S(m, n)$	1
$\tilde{X} \rightarrow \tilde{Y}$	$\sum_{k=1}^n P(m, k)$	0, если $m > n$ 1, если $m \leq n$	$P(m, n)$	1

2.4 Возвратные последовательности

Как мы видели в предыдущих параграфах, в ряде случаев удается вывести рекуррентные соотношения для вычисления членов различных последовательностей. К сожалению, не всегда из таких соотношений удается получить малотрудоемкие явные формулы. Разберем один случай, когда это можно сделать.

Последовательность $\{a_n\}_{n=0}^{\infty}$ назовем *возвратной*, если для некоторого натурального k найдутся такие p_1, \dots, p_k ($p_k \neq 0$), что

$$a_{n+k} + p_1 a_{n+k-1} + \dots + p_k a_n = 0, \quad \forall n \geq 0. \quad (4)$$

Пример

Фибоначчи сформулировал следующую задачу. Некто получил пару новорожденных кроликов 1 января. Кролики месяц растут, а затем каждый месяц дают приплод – одну пару. В свою очередь, каждая новая пара месяц растет, а затем каждый месяц дает приплод. Требуется узнать, сколько кроликов будет к концу года. Обозначив через F_n число пар кроликов к концу n -го месяца, имеем

$$F_0 = 1, F_1 = 1, F_n = F_{n-1} + F_{n-2}, \quad \forall n \geq 2. \quad (5)$$

Требуется найти F_{12} . Последовательность $\{F_n\}_{n=0}^{\infty}$ является возвратной, так как удовлетворяет уравнениям

$$F_{n+2} - F_{n+1} - F_n = 0, \quad \forall n \geq 0.$$

К соотношениям вида (5) приводят совершенно разные задачи.

Утверждение 2.12. *Множество \mathcal{U} последовательностей $\{a_n\}_{n=0}^{\infty}$, удовлетворяющих (4), является линейным пространством размерности k .*

ДОКАЗАТЕЛЬСТВО. Множество всех бесконечных числовых последовательностей с операциями сложения (покомпонентно) и умножения на число (покомпонентно) является линейным пространством. Чтобы показать, что последовательности $\{a_n\}_{n=0}^{\infty}$, удовлетворяющие (4), образуют его линейное подпространство, достаточно убедиться в замкнутости множества таких последовательностей относительно операций сложения и умножения на число. Если $\{a_n\}_{n=0}^{\infty}$ и $\{b_n\}_{n=0}^{\infty}$ удовлетворяют (4), α и β – любые действительные числа, а n – произвольное неотрицательное целое, то

$$\begin{aligned} & (\alpha a_{n+k} + \beta b_{n+k}) + p_1(\alpha a_{n+k-1} + \beta b_{n+k-1}) + \dots + p_k(\alpha a_n + \beta b_n) = \\ & = \alpha(a_{n+k} + p_1 a_{n+k-1} + \dots + p_k a_n) + \beta(b_{n+k} + p_1 b_{n+k-1} + \dots + p_k b_n) = 0. \end{aligned}$$

Следовательно, \mathcal{U} – линейное пространство.

Если последовательность $\{a_n\}_{n=0}^{\infty}$ удовлетворяет (4) и заданы числа a_0, \dots, a_{k-1} , то все остальные a_i определяются из (4) однозначно. Значит, размерность \mathcal{U} не превосходит k . С другой стороны, для $j = 0, 1, \dots, k-1$ последовательность \mathcal{A}_j пусть строится так: $a_j = 1$, $a_i = 0$ для $i \in \{0, 1, \dots, k-1\} \setminus \{j\}$; остальные a_{n+k} для $n \geq 0$ определяются из (4). Тогда последовательности \mathcal{A}_j ($j = 0, 1, \dots, k-1$) линейно независимы в совокупности. ∇

Многочлен

$$P(x) = x^k + p_1 x^{k-1} + \dots + p_k \quad (6)$$

называется *характеристическим многочленом для последовательности* $\{a_n\}_{n=0}^{\infty}$. Характеристическим многочленом для последовательности $\{F_n\}_{n=0}^{\infty}$ будет $x^2 - x - 1$.

Утверждение 2.13. Пусть λ – корень многочлена (6) кратности s ($s \geq 1$). Тогда для любого t , $1 \leq t \leq s$, последовательность $\{b_n(t)\}_{n=0}^{\infty}$, где $b_n = n^{t-1}\lambda^n$, удовлетворяет (4).

ДОКАЗАТЕЛЬСТВО.

Случай 1. $t = 1$. Тогда $b_n = \lambda^n$ ($n = 0, 1, \dots$) и

$$\begin{aligned} b_{n+k} + p_1 b_{n+k-1} + \dots + p_k b_n &= \lambda^{n+k} + p_1 \lambda^{n+k-1} + \dots + p_k \lambda^n = \\ &= \lambda^n (\lambda^k + p_1 \lambda^{k-1} + \dots + p_k) = 0. \end{aligned}$$

Случай 2. $t > 1$. Заметим, что $\lambda \neq 0$, поскольку $p_k \neq 0$. Определим $\varphi(f(x)) = xf'(x)$ и $\varphi_m(f(x)) = \underbrace{\varphi(\dots \varphi(f(x) \dots))}_{m \text{ раз}}$. Легко проверить, что $\varphi(f(x) + g(x)) = \varphi(f(x)) + \varphi(g(x))$, и что $\varphi(ax^r) = arx^r$. Так как λ – корень кратности не менее t многочлена $P_n(x) = x^n P(x)$, то λ является и корнем многочлена

$$\begin{aligned} \varphi_{t-1}(P_n(x)) &= \varphi_{t-1}(x^{n+k} + p_1 x^{n+k-1} + \dots + p_k x^n) = \\ &= \varphi_{t-1}(x^{n+k}) + \varphi_{t-1}(p_1 x^{n+k-1}) + \dots + \varphi_{t-1}(p_k x^n) = (n+k)^{t-1} x^{n+k} + \\ &+ (n+k-1)^{t-1} p_1 x^{n+k-1} + \dots + (n+1)^{t-1} p_{k-1} x^{n+1} + n^{t-1} p_k x^n. \end{aligned}$$

Поскольку $\lambda \neq 0$, получаем

$$(n+k)^{t-1} \lambda^k + (n+k-1)^{t-1} p_1 \lambda^{k-1} + \dots + (n+1)^{t-1} p_{k-1} \lambda + n^{t-1} p_k = 0.$$

Но последнее равенство как раз и требовалось доказать. ∇

Таким образом, если $\lambda_1, \dots, \lambda_m$ – корни многочлена (6) и λ_i – корень кратности s_i ($1 \leq i \leq m$, $s_1 + \dots + s_m = k$), то любая последовательность $\{a_n\}_{n=0}^{\infty}$ вида

$$\begin{aligned} a_n &= (\alpha_{1,1} + \alpha_{1,2}n + \dots + \alpha_{1,s_1} n^{s_1-1}) \lambda_1^n + \dots \\ &\dots + (\alpha_{m,1} + \alpha_{m,2}n + \dots + \alpha_{m,s_m} n^{s_m-1}) \lambda_m^n \quad (n = 0, 1, 2, \dots), \end{aligned}$$

где $\alpha_{i,j}$ – произвольные константы, удовлетворяет (4).

Можно показать, что все построенные выше k последовательностей будут линейно независимы. В общем случае доказательство громоздко. Сейчас мы разберем два случая, используя следующий простой факт.

Упражнение

Если $\lambda_1, \dots, \lambda_k$ различны, то определитель Вандермонда $W = W(\lambda_1, \dots, \lambda_k)$ не равен нулю.

$$W = \begin{vmatrix} 1 & \lambda_1 & \lambda_1^2 & \dots & \lambda_1^{k-1} \\ 1 & \lambda_2 & \lambda_2^2 & \dots & \lambda_2^{k-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \lambda_k & \lambda_k^2 & \dots & \lambda_k^{k-1} \end{vmatrix}$$

Случай 1. Все корни (6) имеют кратность 1. Для доказательства того, что последовательности $\{\lambda_i^n\}_{n=0}^\infty$ ($i = 1, \dots, k$) линейно независимы, достаточно убедиться, что линейно независимы векторы $(1, \lambda_i, \lambda_i^2, \dots, \lambda_i^{k-1})$ ($i = 1, 2, \dots, k$), т. е. векторы, составленные из их первых k координат. Последнее эквивалентно утверждению упражнения.

Случай 2. Корень λ имеет кратность k . Тогда достаточно показать, что $D_k \neq 0$, где

$$D_k = \begin{vmatrix} 1 & \lambda & \lambda^2 & \dots & \lambda^{k-1} \\ 0 & \lambda & 2\lambda^2 & \dots & (k-1)\lambda^{k-1} \\ 0 & \lambda & 2^2\lambda^2 & \dots & (k-1)^2\lambda^{k-1} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \lambda & 2^{k-1}\lambda^2 & \dots & (k-1)^{k-1}\lambda^{k-1} \end{vmatrix}.$$

Но

$$D_k = \lambda^{k(k-1)/2} \begin{vmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & 2 & 3 & \dots & k-1 \\ 0 & 1 & 2^2 & 3^2 & \dots & (k-1)^2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 1 & 2^{k-1} & 3^{k-1} & \dots & (k-1)^{k-1} \end{vmatrix}.$$

Пример

Характеристическим многочленом для последовательности $\{F_n\}_{n=0}^\infty$ является $P(x) = x^2 - x - 1$. Корнями $P(x)$ являются $\lambda_1 = \frac{1+\sqrt{5}}{2}$ и $\lambda_2 = \frac{1-\sqrt{5}}{2}$. Следовательно, для некоторых α_1 и α_2 имеем

$$F_n = \alpha_1 \lambda_1^n + \alpha_2 \lambda_2^n, \quad \forall n.$$

Найдем α_1 и α_2 , зная, что $F_0 = F_1 = 1$:

$$\alpha_1 + \alpha_2 = 1 \quad \text{и} \quad \alpha_1 \lambda_1 + \alpha_2 \lambda_2 = 1.$$

Отсюда $\alpha_1 = \frac{1+\sqrt{5}}{2\sqrt{5}}$, $\alpha_2 = -\frac{1-\sqrt{5}}{2\sqrt{5}}$ и

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

2.5 Числа Каталана

Числа Каталана $\{c_n\}_{n=0}^{\infty}$ определяются по следующим правилам: $c_0 = 1$ и для любого $n > 0$

$$c_n := c_0 c_{n-1} + c_1 c_{n-2} + \dots + c_{n-1} c_0. \quad (7)$$

Начало последовательности: 1, 1, 2, 5, 14, 42, 132, 429, ...

Пример 1

Плоское корневое дерево – это дерево с выделенной вершиной (называемой *корнем*), где непосредственные потомки каждой вершины упорядочены каким-нибудь образом. Каждому плоскому корневному дереву T с корнем r можно сопоставить пару деревьев (T_1, T_2) , полученную после удаления из T ребра (r, s) , соединяющего r со старшим потомком s . При этом считаем, что T_1 содержит r , а $T_2 - s$. По построению суммарное число вершин в T_1 и T_2 равно числу вершин в T . С другой стороны, из каждой пары (T_1, T_2) плоских корневых деревьев добавление ребра, соединяющего их корни, и выбор корня T_1 в качестве корня дает новое плоское корневое дерево. Следовательно, для числа t_n плоских корневых деревьев с количеством ребер n справедливы соотношения $t_0 = 1$ и для любого $n > 0$

$$t_n := t_0 t_{n-1} + t_1 t_{n-2} + \dots + t_{n-1} t_0.$$

Другими словами, t_n есть n -е число Каталана.

Пример 2

Пусть плоское корневое дерево T расположено на плоскости так, что потомки каждой вершины лежат выше ее и расположены по убыванию их старшинства (в выбранном порядке) слева направо. Тогда обходу этого дерева вдоль ребер, начиная с корня так, что дерево остается всегда справа, соответствует последовательность из чисел 1 и (-1) по следующим правилам: если мы переходим от какой-либо вершины к ее потомку, то добавляем к последовательности 1, а если к предку, то добавляем -1 .

В полученной последовательности будет n единиц и n минус-единиц, причем для любого $1 \leq i \leq 2n$ сумма первых i членов последовательности неотрицательна. С другой стороны, по каждой последовательности с такими свойствами можно однозначно построить плоское корневое дерево. Следовательно, число p_n последовательностей из n единиц и n минус-единиц таких, что для любого $1 \leq i \leq 2n$ сумма первых i членов последовательности неотрицательна, тоже равна c_n .

Для нахождения явной формулы c_n представим p_n в виде $p_n = w_n - v_n$, где w_n – число всех последовательностей из n единиц и n

минус-единиц, а v_n – число таких последовательностей из n единиц и n минус-единиц, что

$$\exists i : a_1 + \dots + a_i \leq -1. \quad (8)$$

Очевидно, $w_n = \binom{2n}{n}$.

Чтобы подсчитать v_n , сопоставим каждой последовательности $A = \{a_j\}_{j=1}^{2n}$ из множества \mathcal{V}_n последовательностей из n единиц и n минус-единиц, удовлетворяющих (8), последовательность $F(A)$ по следующим правилам. Пусть $i(A)$ – наименьшее натуральное i , для которого $a_1 + \dots + a_i = -1$. Тогда $F(A)$ получается из A переменной знаков всех первых $i(A)$ членов последовательности. По построению, $F(A)$ имеет $n + 1$ единиц и $n - 1$ минус-единиц.

Покажем, что так определенное F взаимно-однозначно отображает \mathcal{V}_n на множество \mathcal{Z}_n всех последовательностей из $n + 1$ единиц и $n - 1$ минус-единиц. Действительно, пусть $B = \{b_j\}_{j=1}^{2n} \in \mathcal{Z}_n$, а $k(B)$ – наименьшее натуральное k , для которого $b_1 + \dots + b_k = 1$. Обозначим через $G(B)$ последовательность, которая получается из B переменной знаков всех первых $k(B)$ членов. Нетрудно видеть, что $G(B) \in \mathcal{V}_n$, $i(G(B)) = k(B)$ и $F(G(B)) = B$. Следовательно, $|\mathcal{V}_n| = |\mathcal{Z}_n| = \binom{2n}{n-1}$.

Таким образом,

$$c_n = p_n = \binom{2n}{n} - \binom{2n}{n-1} = \frac{1}{n+1} \binom{2n}{n}.$$

Пример 3

Дано произведение $a_1 a_2 \dots a_{n+1}$ из $n + 1$ сомножителей. Пусть $\mathcal{R}(n)$ – множество таких расстановок n пар скобок между этими сомножителями, что внутри каждой пары скобок ровно два сомножителя. Чему равно $r_n := |\mathcal{R}(n)|$?

Если $n = 0$, т. е. имеется лишь один множитель, то скобок не надо совсем. Значит, единственный способ расстановки скобок – не ставить их, и $r_0 = 1$.

Если имеется два сомножителя $a_1 a_2$, то снова один способ расстановки скобок: $(a_1 a_2)$ и $r_1 = 1$.

Если имеются три сомножителя $a_1 a_2 a_3$, то имеем два способа расстановки скобок: $((a_1 a_2) a_3)$ и $(a_1 (a_2 a_3))$, откуда $r_2 = 2$.

При $n \geq 1$ всегда имеется "внешняя" пара скобок: самая левая открывающая с самой правой закрывающей. Назовем "второй" пару скобок, в которой открывающая является самой левой, не считая "внешней". Пусть $\mathcal{R}(n, k)$ – множество таких расстановок $R \in \mathcal{R}(n)$, в которых закрывающая "вторую" пару скобка стоит после a_k . Тогда при $k \leq n$

$$|\mathcal{R}(n, k)| = r_{k-1} r_{n-k},$$

а условие $k = n + 1$ означает, что "вторая" открывающая скобка в R стоит после a_1 и R имеет вид $(a_1(a_2 \dots a_{n+1}))$. Расстановок такого вида, по определению, r_{n-k} . Следовательно,

$$\begin{aligned} r_n &= \sum_{k=2}^{n+1} |\mathcal{R}(n, k)| = r_{n-1} + \sum_{k=2}^n r_{k-1} r_{n-k} = \\ &= r_{n-1} r_0 + \sum_{j=1}^{n-1} r_j r_{n-j-1} = \sum_{j=0}^{n-1} r_j r_{n-j-1}. \end{aligned}$$

Значит, r_n удовлетворяет рекуррентному соотношению (7) и совпадает с c_n для любого n .

2.6 Производящие функции

С каждой последовательностью $\{a_n\}_{n=0}^{\infty}$ можно связать формальный степенной ряд $A(t) = a_0 + a_1 t + a_2 t^2 + a_3 t^3 + \dots$, называемый *производящей функцией для последовательности* $\{a_n\}_{n=0}^{\infty}$. Если $|a_n|$ растет не слишком быстро, то в некоторой окрестности нуля этот ряд абсолютно сходится и $A(t)$ можно отождествить с получающейся аналитической функцией.

Примеры

1. $a_n = \binom{k}{n}$. Тогда $A(t) = 1 + kt + \binom{k}{2} t^2 + \dots + \binom{k}{k} t^k = (1+t)^k$.
2. $a_n = 1$. Тогда $A(t) = 1 + t + t^2 + t^3 + \dots = 1/(1-t)$.
3. $a_n = \frac{1}{n!}$. Тогда $A(t) = 1 + \frac{t}{1!} + \frac{t^2}{2!} + \dots = e^t$.
4. $a_n = F_n$. Тогда

$$\begin{aligned} A(t) &= \sum_{n=0}^{\infty} F_n t^n = 1 + t + \sum_{n=2}^{\infty} (F_{n-2} + F_{n-1}) t^n = \\ &= 1 + t + t^2 \sum_{n=0}^{\infty} F_n t^n + t \sum_{n=1}^{\infty} F_n t^n = 1 + t^2 A(t) + t A(t). \end{aligned}$$

Из уравнения $A(t) = 1 + t^2 A(t) + t A(t)$ получаем $A(t) = \frac{1}{1-t-t^2}$.

Зная производящую функцию $A(t)$, можно найти любое a_n , используя разложение Тейлора. Имеем $a_n = \frac{A^{(n)}(0)}{n!}$.

Примеры

1. $A(t) = 1/(1-2t)$. Тогда $A^{(n)}(t) = (-1)(-2) \dots (-n)(-2)^n (1-2t)^{-1-n}$. Значит, $A(0) = 1$, $\frac{A'(0)}{1!} = 2$, $\frac{A''(0)}{2!} = 2^2, \dots, \frac{A^{(n)}(0)}{n!} = 2^n$.

2. $A(t) = (1+t)^{-m}$, где число $-m$ не является натуральным. Тогда $A^{(n)}(t) = (-m)(-m-1)\dots(-m-n+1)(1+t)^{-m-n}$. Значит, $a_n = \frac{A^{(n)}(0)}{n!} = \frac{[-m]_n}{n!} = \binom{-m}{n} = (-1)^n \binom{m+n-1}{n}$.

Формальные ряды можно складывать и умножать: если $A(t) = \sum_{n=0}^{\infty} a_n t^n$, $B(t) = \sum_{n=0}^{\infty} b_n t^n$, то

$$A(t)B(t) = \sum_{n=0}^{\infty} d_n t^n, \text{ где } d_k = a_0 b_k + a_1 b_{k-1} + \dots + a_k b_0. \quad (9)$$

Это свойство можно использовать при выводе ряда тождеств.

Пример

Распишем очевидное равенство $(1+t)^k(1+t)^{-m} = (1+t)^{k-m}$ через ряды:

$$\left(\sum_{n=0}^{\infty} \binom{k}{n} t^n \right) \left(\sum_{n=0}^{\infty} (-1)^n \binom{m+n-1}{n} t^n \right) = \sum_{n=0}^{\infty} \binom{k-m}{n} t^n.$$

Сравнивая коэффициенты при t^n , получаем справа $\binom{k-m}{n}$, а слева

$$\sum_{i=0}^n \binom{k-m}{i} (-1)^{n-i} \binom{m+n-1-i}{n-i}.$$

Следовательно,

$$\binom{k-m}{n} = \sum_{i=0}^n \binom{k-m}{i} (-1)^{n-i} \binom{m+n-1-i}{n-i}.$$

Используя определение (7) чисел Каталана, найдем производящую функцию $C(t)$ этой последовательности и тем самым выведем их явную формулу еще одним способом. Имеем

$$\begin{aligned} C(t) &= \sum_{n=0}^{\infty} c_n t^n = 1 + \sum_{n=1}^{\infty} (c_0 c_{n-1} + \dots + c_{n-1} c_0) t^n = \\ &= 1 + t \sum_{n=0}^{\infty} (c_0 c_n + \dots + c_n c_0) t^n = 1 + t(C(t))^2. \end{aligned}$$

Разрешив квадратное уравнение относительно $C(t)$, получим

$$C(t) = \frac{1 \pm \sqrt{1-4t}}{2t}.$$

Поскольку $C(0) = 1$, в формуле годится только знак "минус".

Подсчитаем n -ю производную от $\sqrt{1-4t}$:

$$\frac{d^n}{dt^n} \sqrt{1-4t} = \binom{1/2}{n} n! (1-4t)^{1/2-n} (-4)^n = 2^n (-1) (2n-3)!! (1-4t)^{1/2-n}.$$

Следовательно,

$$1 - \sqrt{1-4t} = \sum_{n=1}^{\infty} \frac{2^n (2n-3)!!}{n!} t^n$$

и

$$C(t) = \sum_{n=0}^{\infty} \frac{2^n (2n-1)!!}{(n+1)!} t^n.$$

Заметим, что

$$\frac{2^n (2n-1)!!}{(n+1)!} = \frac{(2n)!}{n!(n+1)!} = \frac{1}{n+1} \binom{2n}{n}.$$

2.7 Некоторые вероятностные задачи с конечным пространством элементарных событий

Изложенные ниже факты приобретают ценность и наглядный смысл в связи с действительными или мысленными опытами. Результаты опытов будем называть *событиями*.

Пространство элементарных событий (Ω, \mathbf{P}) – это конечное множество $\Omega = \{E_1, \dots, E_n\}$ (элементы которого называются элементарными событиями), где каждому E_i сопоставлено число $\mathbf{P}\{E_i\}$, называемое вероятностью элементарного события E_i . Эти числа должны быть неотрицательны и таковы, что

$$\mathbf{P}\{E_1\} + \mathbf{P}\{E_2\} + \dots + \mathbf{P}\{E_n\} = 1.$$

Каждый раз, когда строится воображаемое пространство, которое должно моделировать реальную ситуацию, надо, во-первых, выбрать $\{E_1, \dots, E_n\}$, а затем определить $\mathbf{P}\{E_i\}$, $i = 1, \dots, n$.

Примеры

1. Пусть опыт состоит в бросании двух различных игральных костей. Обычно рассматривают $\Omega = \{E_{ij} \mid i = 1, 2; j = 1, \dots, 6\}$, где

элементарное событие E_{ij} состоит в том, что на первой кости выпало i очков, а на второй – j очков. При этом, как правило, полагают $\mathbf{P}\{E_{ij}\} = 1/36$. В некоторых задачах, однако, удобно выбрать $\Omega = \{E_2, \dots, E_{12}\}$, где событие E_i состоит в том, что сумма очков на костях равна i . Из соображений здравого смысла полагают $\mathbf{P}\{E_i\} = \min\{i - 1, 13 - i\}/36$.

2. Рассмотрим механическую систему, состоящую из r неразличимых частиц. В статистической механике обычно разбивают фазовое пространство на большое число n малых областей и полагают, что каждая из частиц находится в какой-то одной из этих ячеек. В результате состояние всей системы описывается как случайное размещение r частиц в n ячейках. Если все n^r размещений равновероятны, то физики говорят о статистике Максвелла – Больцмана. Однако поведение реальных частиц не удается аппроксимировать этой моделью. В статистической механике показано, что для фотонов и атомных ядер годится статистика Бозе – Эйнштейна, где каждому из $\binom{n+r-1}{r}$ размещений r неразличимых частиц по n ячейкам приписана вероятность $\binom{n+r-1}{r}^{-1}$. К электронам, нейтронам и протонам применима статистика Ферми – Дирака, которая запрещает находиться в любой ячейке более чем одной частице и приписывает вероятность $\binom{n}{r}^{-1}$ каждому из размещений частиц, удовлетворяющих этому условию.

В ряде комбинаторных задач из соображений симметрии полагают вероятности всех элементарных событий равными между собой. В этом случае говорят о классическом определении вероятности.

Любое подмножество множества Ω будем называть *событием*. Вероятность $\mathbf{P}\{A\}$ любого события A есть сумма вероятностей элементарных событий, из которых состоит A :

$$\mathbf{P}\{A\} = \sum_{E_i \in A} \mathbf{P}\{E_i\}.$$

Пример

Предположим, что Вы играете в спортлото "5 из 36", и вероятность любого из $\binom{36}{5}$ исходов одна и та же. Тогда вероятность того, что в Вашем билете угадано пять номеров, равна $\binom{36}{5}^{-1} \approx 0,000026526$, четыре номера – $5 \cdot 31 \cdot \binom{36}{5}^{-1} \approx 0,0004111$, три номера – $\binom{5}{3} \cdot \binom{31}{2} \cdot \binom{36}{5}^{-1} \approx 0,0123$.

Теорема 2.14. Для любых событий A_1 и A_2 вероятность $\mathbf{P}\{A_1 \cup A_2\}$ того, что имеет место как минимум одно из этих событий, равна $\mathbf{P}\{A_1\} + \mathbf{P}\{A_2\} - \mathbf{P}\{A_1 \cap A_2\}$.

ДОКАЗАТЕЛЬСТВО.

$$\begin{aligned}
 \mathbf{P}\{A_1 \cup A_2\} &= \sum_{E_i \in A_1 \cup A_2} \mathbf{P}\{E_i\} = \sum_{E_i \in A_1} \mathbf{P}\{E_i\} + \sum_{E_i \in A_2 \setminus A_1} \mathbf{P}\{E_i\} = \\
 &= \sum_{E_i \in A_1} \mathbf{P}\{E_i\} + \sum_{E_i \in A_2} \mathbf{P}\{E_i\} - \sum_{E_i \in A_1 \cap A_2} \mathbf{P}\{E_i\} = \\
 &= \mathbf{P}\{A_1\} + \mathbf{P}\{A_2\} - \mathbf{P}\{A_1 \cap A_2\}. \nabla
 \end{aligned}$$

События A_1 и A_2 называются *взаимно исключающими*, если $A_1 \cap A_2 = \emptyset$.

Непосредственно из определений вероятности событий и взаимно исключающих событий следует

Утверждение 2.15. *Если A_1, \dots, A_k – попарно взаимно исключающие события, то $\mathbf{P}\{A_1 \cup \dots \cup A_k\} = \mathbf{P}\{A_1\} + \dots + \mathbf{P}\{A_k\}$.*

Пусть H – событие с $\mathbf{P}\{H\} > 0$. Для любого события A положим

$$\mathbf{P}\{A | H\} = \frac{\mathbf{P}\{A \cap H\}}{\mathbf{P}\{H\}}. \quad (10)$$

Таким образом определенная величина будет называться *условной вероятностью события A при условии H* .

Пример

Рассмотрим семьи с двумя детьми. Обозначим буквами m и d соответственно мальчика и девочку и на первом месте будем указывать старшего ребенка. Имеем 4 возможности: mm , md , dm , dd . Припишем каждому из этих элементарных событий вероятность $1/4$. Пусть событие H_1 состоит в том, что в семье есть мальчик, событие H_2 – в том, что старший ребенок в семье – мальчик, а событие A – в том, что оба ребенка в семье – мальчики. Тогда

$$\mathbf{P}\{A | H_1\} = \mathbf{P}\{A \cap H_1\} / \mathbf{P}\{H_1\} = (1/4) / (3/4) = 1/3,$$

$$\mathbf{P}\{A | H_2\} = \mathbf{P}\{A \cap H_2\} / \mathbf{P}\{H_2\} = (1/4) / (1/2) = 1/2.$$

Пример

Пусть Ω – множество всех упорядоченных пар карт колоды из 52 листов, и вероятность выбрать любую упорядоченную пару одинакова и равна $1/(51 \cdot 52)$. Обозначим через A событие, состоящее в том, что обе карты из пары являются тузами, через H_1 – что первая из выбранных

карт является тузом, через H_2 – что первая из выбранных карт является тузом треф. Сравним $\mathbf{P}\{A | H_1\}$ и $\mathbf{P}\{A | H_2\}$:

$$\mathbf{P}\{H_1\} = \frac{4 \cdot 51}{52 \cdot 51} = 1/13, \quad \mathbf{P}\{H_2\} = 1/52,$$

$$\mathbf{P}\{A \cap H_1\} = \mathbf{P}\{A\} = \frac{12}{52 \cdot 51}, \quad \mathbf{P}\{A \cap H_2\} = \frac{3}{52 \cdot 51},$$

откуда

$$\mathbf{P}\{A | H_1\} = \frac{12 \cdot 13}{52 \cdot 51} = 1/17, \quad \mathbf{P}\{A | H_2\} = 3/51 = 1/17.$$

Пример

Пусть теперь Ω – множество всех неупорядоченных пар карт колоды из 52 листов, и вероятность вытянуть любую пару одинакова и равна $\binom{52}{2}^{-1}$. Обозначим через A событие, состоящее в том, что обе карты из пары являются тузами, через H_1 – что хотя бы одна из выбранных карт является тузом, через H_2 – что одна из выбранных карт является тузом треф. В отличие от предыдущего примера получим, что $\mathbf{P}\{A | H_1\} < \mathbf{P}\{A | H_2\}$:

$$\mathbf{P}\{H_1\} = \left[\binom{52}{2} - \binom{48}{2} \right] \binom{52}{2}^{-1}, \quad \mathbf{P}\{H_2\} = 51 \binom{52}{2}^{-1},$$

$$\mathbf{P}\{A \cap H_1\} = \mathbf{P}\{A\} = 6 \binom{52}{2}^{-1}, \quad \mathbf{P}\{A \cap H_2\} = 3 \binom{52}{2}^{-1},$$

откуда

$$\mathbf{P}\{A | H_1\} = 6 \left[\binom{52}{2} - \binom{48}{2} \right]^{-1} = 1/33, \quad \mathbf{P}\{A | H_2\} = 3/51 = 1/17.$$

Формулу (10) иногда используют в виде

$$\mathbf{P}\{A \cap H\} = \mathbf{P}\{A | H\} \mathbf{P}\{H\}. \quad (11)$$

Теорема 2.16. (формула полной вероятности) Пусть H_1, \dots, H_k – взаимно исключающие события, объединение которых есть Ω , и вероятность каждого из H_i положительна. Тогда для любого $A \subset \Omega$

$$\mathbf{P}\{A\} = \sum_{i=1}^k \mathbf{P}\{A | H_i\} \cdot \mathbf{P}\{H_i\}.$$

ДОКАЗАТЕЛЬСТВО. По условию

$$A = (A \cap H_1) \cup (A \cap H_2) \cup \dots \cup (A \cap H_k).$$

Согласно утверждению 2.15

$$\mathbf{P}\{A\} = \mathbf{P}\{A \cap H_1\} + \mathbf{P}\{A \cap H_2\} + \dots + \mathbf{P}\{A \cap H_k\}.$$

В силу (11) последняя сумма равна $\sum_{i=1}^k \mathbf{P}\{A \mid H_i\} \cdot \mathbf{P}\{H_i\}$. ∇

Пример

Предположим, что в урне имеется M шаров, из которых n счастливых. Выбираем наугад какой-то шар, а затем, не возвращая его, – второй. Какова вероятность, что второй шар счастливый? Обозначим через H_1 событие, что первый шар счастливый, через H_2 – событие, что первый шар несчастливый, через A – событие, что второй шар счастливый. Тогда $\mathbf{P}\{H_1\} = n/M$, $\mathbf{P}\{H_2\} = 1 - n/M$, $\mathbf{P}\{A \mid H_1\} = (n - 1)/(M - 1)$, $\mathbf{P}\{A \mid H_2\} = n/(M - 1)$, и по теореме 2.16

$$\mathbf{P}\{A\} = \frac{n}{M} \frac{n-1}{M-1} + \frac{M-n}{M} \frac{n}{M-1} = \frac{n}{M}. \quad \nabla$$

Пример

Предположим, что вы k раз играете в игру, где i -й раз вероятность вашего выигрыша равна p_i . Какова вероятность P_k того, что вы выиграете хотя бы один раз из k ? Покажем индукцией по k , что она равна $1 - (1 - p_1) \cdot (1 - p_2) \cdot \dots \cdot (1 - p_k)$. Для $k = 1$ это тривиально. Пусть формула доказана для всех $k' < k$. Обозначим через $H_1(i)$ событие, что вы выиграли хотя бы раз из первых i розыгрышей, а через $H_2(i)$ событие, что этого не произошло. Тогда по теореме 2.16

$$P_k = \mathbf{P}\{H_1(k)\} = \mathbf{P}\{H_1(k) \mid H_1(k-1)\} \cdot \mathbf{P}\{H_1(k-1)\} + \mathbf{P}\{H_1(k) \mid H_2(k-1)\} \cdot \mathbf{P}\{H_2(k-1)\} = 1 \cdot \mathbf{P}\{H_1(k-1)\} + p_k \cdot \mathbf{P}\{H_2(k-1)\}.$$

По индукционному предположению, $\mathbf{P}\{H_1(k-1)\} = 1 - (1 - p_1) \cdot (1 - p_2) \cdot \dots \cdot (1 - p_{k-1})$. Значит,

$$P_k = 1 - (1 - p_1) \cdot (1 - p_2) \cdot \dots \cdot (1 - p_{k-1}) + p_k (1 - p_1) \cdot (1 - p_2) \cdot \dots \cdot (1 - p_{k-1}) = 1 - (1 - p_1) \cdot (1 - p_2) \cdot \dots \cdot (1 - p_k).$$

Это утверждение можно трактовать и так: если вероятность успеха Вашего соперника в i -м розыгрыше равна $q_i = 1 - p_i$, то вероятность того, что он выиграет все k раз, равна $q_1 \cdot \dots \cdot q_k$.

Пусть $\mathbf{P}\{A\} > 0$, $\mathbf{P}\{B\} > 0$. Согласно (11), $\mathbf{P}\{A | B\} \cdot \mathbf{P}\{B\} = \mathbf{P}\{A \cap B\} = \mathbf{P}\{B | A\} \cdot \mathbf{P}\{A\}$, откуда следует *формула Байеса*

$$\mathbf{P}\{A | B\} = \frac{\mathbf{P}\{B | A\} \cdot \mathbf{P}\{A\}}{\mathbf{P}\{B\}}.$$

Теорема 2.17. (Теорема Байеса.) Пусть H_1, \dots, H_k – взаимно исключающие события, объединение которых есть Ω , и вероятности событий H_1, \dots, H_k, A положительны. Тогда

$$\mathbf{P}\{H_i | A\} = \frac{\mathbf{P}\{A | H_i\} \cdot \mathbf{P}\{H_i\}}{\mathbf{P}\{A | H_1\} \cdot \mathbf{P}\{H_1\} + \dots + \mathbf{P}\{A | H_k\} \cdot \mathbf{P}\{H_k\}}.$$

ДОКАЗАТЕЛЬСТВО. По формуле Байеса $\mathbf{P}\{H_i | A\} = \mathbf{P}\{A | H_i\} \cdot \mathbf{P}\{H_i\} / \mathbf{P}\{A\}$. Подставив в это равенство вместо $\mathbf{P}\{A\}$ его выражение из теоремы 2.16, получим требуемое. ∇

Пример

В урне имеются две монеты: первая – симметричная с вероятностью выпадения герба $1/2$, вторая – кривая с вероятностью выпадения герба $1/3$. Выбираем наугад монету и подбрасываем: выпал герб. Какова вероятность того, что выбрана симметричная монета?

Имеем четыре элементарных исхода: M_1G, M_1C, M_2G, M_2C , где M_i – событие, что достали i -ю монету, G – что выпал герб, а C – что выпала цифра. Нам требуется узнать $\mathbf{P}\{M_1 | G\}$. По теореме Байеса

$$\begin{aligned} \mathbf{P}\{M_1 | G\} &= \frac{\mathbf{P}\{G | M_1\} \cdot \mathbf{P}\{M_1\}}{\mathbf{P}\{G | M_1\} \cdot \mathbf{P}\{M_1\} + \mathbf{P}\{G | M_2\} \cdot \mathbf{P}\{M_2\}} = \\ &= \frac{0,5 \cdot 0,5}{0,5 \cdot 0,5 + (1/3) \cdot 0,5} = 3/5. \end{aligned}$$

События A и B называются *независимыми*, если

$$\mathbf{P}\{A \cap B\} = \mathbf{P}\{A\} \cdot \mathbf{P}\{B\}.$$

Упражнение. Доказать, что если события A и B независимы, то события A и $\bar{B} = \Omega \setminus B$ тоже независимы.

События A_1, \dots, A_m называются *независимыми в совокупности*, если для любого k , $2 \leq k \leq m$ и для любых A_{i_1}, \dots, A_{i_k} справедливо равенство

$$\mathbf{P}\{A_{i_1} \cap \dots \cap A_{i_k}\} = \mathbf{P}\{A_{i_1}\} \cdot \dots \cdot \mathbf{P}\{A_{i_k}\}.$$

2.8 Случайные величины. Схема Бернулли

Функция, определенная на пространстве элементарных событий, называется *случайной величиной*. Если f – случайная величина, то функция $h_f(x) = \mathbf{P}\{f = x\}$ называется *распределением (вероятностей) случайной величины f* .

Пример

Вы играете в "поле чудес", ваша очередь хода, вы знаете, какое слово загадано и все-таки вы крутите колесо. Тогда сумма ваших очков после хода есть случайная величина, зависящая от того, где остановится колесо.

Случайная величина, которая принимает лишь значения 0 и 1, называется *бернуллиевской*.

Пусть f – случайная величина (принимая значения x_1, \dots, x_t с вероятностями $h_f(x_1), \dots, h_f(x_t)$). *Математическим ожиданием $\mathbf{M}(f)$ случайной величины f* называется сумма

$$\mathbf{M}(f) = \sum_{E_j \in \Omega} f(E_j) \cdot \mathbf{P}\{E_j\} = \sum_{i=1}^t x_i h_f(x_i).$$

Пример

Для бернуллиевской случайной величины f , принимающей значение 1 с вероятностью p , имеем $\mathbf{M}(f) = 0 \cdot (1 - p) + 1 \cdot p = p$.

Непосредственно из определений получаем, что для любых случайных величин f и g и любой константы c

- 1) $\mathbf{M}(f + g) = \mathbf{M}(f) + \mathbf{M}(g)$;
- 2) $\mathbf{M}(c \cdot f) = c \cdot \mathbf{M}(f)$;
- 3) если $f \geq g$, то $\mathbf{M}(f) \geq \mathbf{M}(g)$;
- 4) $|\mathbf{M}(f)| \leq \mathbf{M}(|f|)$.

(Докажите эти свойства в качестве упражнения.)

Пример

Для суммы $S_n = f_1 + \dots + f_n$ бернуллиевских случайных величин, каждая из которых принимает значение 1 с вероятностью p , по свойству 1 имеем $\mathbf{M}(S_n) = \mathbf{M}(f_1) + \dots + \mathbf{M}(f_n) = pn$.

Дисперсией $\mathbf{D}(f)$ случайной величины f называется величина

$$\begin{aligned} \mathbf{D}(f) &= \mathbf{M}((f - \mathbf{M}(f))^2) = \mathbf{M}(f^2 - 2f \cdot \mathbf{M}(f) + (\mathbf{M}(f))^2) = \\ &= \mathbf{M}(f^2) - 2\mathbf{M}(f) \cdot \mathbf{M}(f) + (\mathbf{M}(f))^2 \cdot \mathbf{M}(1) = \mathbf{M}(f^2) - (\mathbf{M}(f))^2. \end{aligned}$$

Непосредственно из определения получаем, что для любой случайной величины f и любых констант c и d

$$\mathbf{D}(d + c \cdot f) = c^2 \cdot \mathbf{D}(f).$$

Пример

Для бернуллиевской случайной величины f , принимающей значение 1 с вероятностью p , имеем $\mathbf{D}(f) = \mathbf{M}((f-p)^2) = p(1-p)^2 + (1-p)(-p)^2 = p(1-p)$.

Случайные величины f_1, \dots, f_m называются *независимыми в совокупности*, если для любого $k, 2 \leq k \leq m$ и для любых x_{i_1}, \dots, x_{i_k} справедливо равенство

$$\mathbf{P}\{f_{i_1} = x_{i_1}, \dots, f_{i_k} = x_{i_k}\} = \mathbf{P}\{f_{i_1} = x_{i_1}\} \cdot \dots \cdot \mathbf{P}\{f_{i_k} = x_{i_k}\}.$$

Свойства независимых случайных величин

1. Пусть f, g – независимые случайные величины, c, d – произвольные константы. Тогда $f - c, g - d$ – тоже независимые случайные величины.

ДОКАЗАТЕЛЬСТВО. Для произвольных действительных x и y имеем

$$\begin{aligned} \mathbf{P}\{f - c = x, g - d = y\} &= \mathbf{P}\{f = x + c, g = y + d\} = \\ &= \mathbf{P}\{f = x + c\} \cdot \mathbf{P}\{g = y + d\} = \mathbf{P}\{f - c = x\} \cdot \mathbf{P}\{g - d = y\}. \quad \nabla \end{aligned}$$

2. Пусть f, g – независимые случайные величины. Тогда $\mathbf{M}(fg) = \mathbf{M}(f) \cdot \mathbf{M}(g)$.

ДОКАЗАТЕЛЬСТВО. Пусть f принимает значения a_1, \dots, a_s , а g принимает значения b_1, \dots, b_t . Тогда

$$\begin{aligned} \mathbf{M}(fg) &= \sum_{i=1}^s \sum_{j=1}^t a_i b_j \cdot \mathbf{P}\{f = a_i, g = b_j\} = \\ &= \sum_{i=1}^s \sum_{j=1}^t a_i \cdot \mathbf{P}\{f = a_i\} \cdot b_j \cdot \mathbf{P}\{g = b_j\} = \\ &= \left(\sum_{i=1}^s a_i \cdot \mathbf{P}\{f = a_i\} \right) \sum_{j=1}^t b_j \cdot \mathbf{P}\{g = b_j\} = \mathbf{M}(f) \cdot \mathbf{M}(g). \quad \nabla \end{aligned}$$

3. Пусть f, g – независимые случайные величины. Тогда $\mathbf{D}(f + g) = \mathbf{D}(f) + \mathbf{D}(g)$.

ДОКАЗАТЕЛЬСТВО. По свойству 1 случайные величины $f - \mathbf{M}(f)$ и $g - \mathbf{M}(g)$ также являются независимыми. Следовательно, с учетом свойства 2 имеем

$$\mathbf{D}(f + g) = \mathbf{M}((f + g - \mathbf{M}(f) - \mathbf{M}(g))^2) =$$

$$\begin{aligned}
&= \mathbf{M}((f - \mathbf{M}(f))^2) + \mathbf{M}(2(f - \mathbf{M}(f))(g - \mathbf{M}(g))) + \mathbf{M}((g - \mathbf{M}(g))^2) = \\
&= \mathbf{D}(f) + 2\mathbf{M}(f - \mathbf{M}(f))\mathbf{M}(g - \mathbf{M}(g)) + \mathbf{D}(g) = \\
&= \mathbf{D}(f) + 2(\mathbf{M}(f) - \mathbf{M}(f))(\mathbf{M}(g) - \mathbf{M}(g)) + \mathbf{D}(g). \quad \nabla
\end{aligned}$$

Пример

Для суммы $S_n = f_1 + \dots + f_n$ независимых бернуллиевских случайных величин, каждая из которых принимает значение 1 с вероятностью p , по свойству 3 имеем

$$\mathbf{D}(S_n) = \mathbf{D}(f_1) + \dots + \mathbf{D}(f_n) = np(1 - p).$$

Неравенства Чебышева. Пусть g – неотрицательная случайная величина, а f – произвольная случайная величина. Тогда для любого $\epsilon > 0$

- (а) $\mathbf{P}\{g \geq \epsilon\} \leq \mathbf{M}(g)/\epsilon$;
- (б) $\mathbf{P}\{|f| \geq \epsilon\} \leq \mathbf{M}(|f|)/\epsilon$;
- (в) $\mathbf{P}\{|f| \geq \epsilon\} = \mathbf{P}\{f^2 \geq \epsilon^2\} \leq \mathbf{M}(f^2)/\epsilon^2$;
- (г) $\mathbf{P}\{|f - \mathbf{M}(f)| \geq \epsilon\} \leq \mathbf{D}(f)/\epsilon^2$.

ДОКАЗАТЕЛЬСТВО. Докажем неравенство (а). Пусть функция g принимает значения x_1, \dots, x_s . Тогда

$$\begin{aligned}
\mathbf{M}(g) &= \sum_{x_i \geq \epsilon} x_i h_g(x_i) + \sum_{0 \leq x_i < \epsilon} x_i h_g(x_i) \geq \\
&\geq \epsilon \sum_{x_i \geq \epsilon} h_g(x_i) = \epsilon \mathbf{P}\{g \geq \epsilon\}.
\end{aligned}$$

Каждое из оставшихся неравенств является непосредственным следствием предыдущего. ∇

Используя неравенство Чебышева, докажем закон больших чисел в следующей весьма слабой форме.

Теорема 2.18. Для любых положительных ϵ и δ при достаточно большом n для суммы $S_n = f_1 + \dots + f_n$ независимых бернуллиевских случайных величин, каждая из которых принимает значение 1 с вероятностью p ,

$$\mathbf{P}\left\{\left|\frac{S_n}{n} - p\right| \geq \epsilon\right\} < \delta.$$

ДОКАЗАТЕЛЬСТВО. Для случайной величины $f = S_n/n$ имеем $\mathbf{M}(f) = \mathbf{M}(S_n)/n = p$. В силу неравенства Чебышева

$$\mathbf{P}\{|f - \mathbf{M}(f)| \geq \epsilon\} \leq \frac{\mathbf{D}(f)}{\epsilon^2} = \frac{\mathbf{D}(S_n)}{n^2 \epsilon^2} = \frac{p(1 - p)}{n \epsilon^2}.$$

Последняя дробь при $n > \epsilon^{-2}\delta^{-1}$ меньше, чем δ . ∇

Рассмотрим случайные блуждания частицы по целочисленным точкам отрезка $[0, k]$. Если в момент времени i частица находится в точке j , $1 \leq j \leq k-1$, то в момент $i+1$ частица с вероятностью p оказывается в точке $j+1$ и с вероятностью $1-p$ оказывается в точке $j-1$. Как только частица оказывается в точке 0 или k , процесс прекращается.

Обозначим через $A_n(j, k)$ вероятность того, что частица, находящаяся в момент 0 в точке j , не более чем к n -му моменту времени окажется в точке 0. Аналогично, обозначим через $B_n(j, k)$ вероятность того, что частица, находящаяся в момент 0 в точке j , не более чем к n -му моменту времени окажется в точке k . Наконец, через $C_n(j, k)$ обозначим вероятность того, что частица, находящаяся в момент 0 в точке j , к n -му моменту времени окажется в отрезке $[1, k-1]$ (т. е. не достигнет ни 0, ни k). Для любых натуральных n и k и любых целых $0 \leq j \leq k$ справедливы следующие соотношения:

$$A_n(j, k) + B_n(j, k) + C_n(j, k) = 1, \quad (12)$$

$$A_n(0, k) = B_n(k, k) = 1, \quad (13)$$

$$A_n(k, k) = B_n(0, k) = C_n(0, k) = C_n(k, k) = 0, \quad (14)$$

$$A_{n+1}(j, k) \geq A_n(j, k), B_{n+1}(j, k) \geq B_n(j, k), C_{n+1}(j, k) \leq C_n(j, k). \quad (15)$$

Согласно (12) и (15) каждая из последовательностей $\{A_n(j, k)\}_{n=0}^{\infty}$, $\{B_n(j, k)\}_{n=0}^{\infty}$, $\{C_n(j, k)\}_{n=0}^{\infty}$ является ограниченной и монотонной. Следовательно, существуют пределы $A(j, k) = \lim_{n \rightarrow \infty} A_n(j, k)$, $B(j, k) = \lim_{n \rightarrow \infty} B_n(j, k)$ и $C(j, k) = \lim_{n \rightarrow \infty} C_n(j, k)$.

По формуле полной вероятности

$$A_{n+1}(j, k) = pA_n(j+1, k) + (1-p)A_n(j-1, k).$$

Переходя к пределу по n в обеих частях, получаем

$$A(j, k) = pA(j+1, k) + (1-p)A(j-1, k). \quad (16)$$

Аналогично (16) выводятся равенства

$$B(j, k) = pB(j+1, k) + (1-p)B(j-1, k) \text{ и}$$

$$C(j, k) = pC(j+1, k) + (1-p)C(j-1, k).$$

Таким образом, при фиксированном k каждая из последовательностей $\{A(j, k)\}_{j=0}^k$, $\{B(j, k)\}_{j=0}^k$, $\{C(j, k)\}_{j=0}^k$ удовлетворяет одному и тому же возвратному соотношению с характеристическим уравнением

$$px^2 - x + 1 - p = 0. \quad (17)$$

Корнями (17) являются $x_1 = 1$ и $x_2 = (1 - p)/p$. Переходя к пределу по n в (13) и (14), получаем

$$A(0, k) = B(k, k) = 1, \quad A(k, k) = B(0, k) = C(0, k) = C(k, k) = 0. \quad (18)$$

Случай 1. $p \neq 1/2$. Тогда имеем $C(j, k) = \alpha + \beta(\frac{1-p}{p})^j$, где α и β определяются из уравнений

$$\alpha + \beta = 0, \quad \alpha + \beta\left(\frac{1-p}{p}\right)^k = 0.$$

Единственным решением этой системы являются $\alpha = \beta = 0$, откуда $C(j, k) = 0$.

Аналогично, $B(j, k) = \alpha + \beta(\frac{1-p}{p})^j$, где α и β определяются из уравнений

$$\alpha + \beta = 0, \quad \alpha + \beta\left(\frac{1-p}{p}\right)^k = 1.$$

Решая систему, получаем

$$B(j, k) = \frac{1 - \left(\frac{1}{p} - 1\right)^j}{1 - \left(\frac{1}{p} - 1\right)^k}.$$

Переходя к пределу по n в (15), получаем $A(j, k) = 1 - B(j, k) - C(j, k) = 1 - B(j, k)$.

Случай 2. $p = 1/2$. Тогда $C(j, k) = \alpha + \beta j$, и снова $C(j, k) = 0$.

Аналогично, $B(j, k) = \alpha + \beta j$, где

$$\alpha = 0, \quad \alpha + \beta k = 1.$$

Получаем $B(j, k) = j/k$, $A(j, k) = (k - j)/k$.

2.9 Формула включений и исключений

Теорема 2.19. (Формула включений и исключений.) Пусть A_1, \dots, A_k – конечные множества, $K = \{1, \dots, k\}$. Тогда

$$|A_1 \cup \dots \cup A_k| = \sum_{j=1}^k (-1)^{j-1} \sum_{\{I \subset K: |I|=j\}} \left| \bigcap_{i \in I} A_i \right|. \quad (19)$$

ДОКАЗАТЕЛЬСТВО. Каждый элемент $x \in A_1 \cup \dots \cup A_k$ дает единицу в $|A_1 \cup \dots \cup A_k|$. Покажем, что такой же вклад x вносит и в сумму

в правой части (19). Пусть для определенности $x \in A_1 \cap \dots \cap A_r$, $x \notin A_i$ ($r < i \leq k$). По определению $x \in \bigcap_{i \in I} A_i$, если и только если $I \subset \{1, \dots, r\}$. Число j -элементных множеств $I \subset \{1, \dots, r\}$ равно $\binom{r}{j}$. Значит, x вносит в правую часть (19) вклад, равный

$$\sum_{j=1}^k (-1)^{j-1} \binom{r}{j} = \sum_{j=1}^r (-1)^{j-1} \binom{r}{j} = 1 - \sum_{j=0}^r (-1)^j \binom{r}{j} = 1 - (1-1)^r = 1. \nabla$$

Замечание. Предположим, что S – конечное множество и $A_1 \cup \dots \cup A_k \subseteq S$. Если положить $\bigcap_{i \in \emptyset} A_i = S$, то (19) можно переписать в виде

$$|S \setminus (A_1 \cup \dots \cup A_k)| = \sum_{j=0}^k (-1)^j \sum_{\{I \subset K: |I|=j\}} \left| \bigcap_{i \in I} A_i \right|. \quad (20)$$

Следующая теорема обобщает теоремы 2.19 и 2.14.

Теорема 2.20. (Формула решета.) Пусть A_1, \dots, A_k – произвольные события вероятностного пространства (Ω, \mathbf{P}) . Для каждого $I \subset \{1, \dots, k\}$ обозначим $A_I = \bigcap_{i \in I} A_i$. Тогда

$$\mathbf{P}\{A_1 \cup \dots \cup A_k\} = \sum_{j=1}^k (-1)^{j-1} \sum_{|I|=j}^{j-1} \mathbf{P}\{A_I\}. \quad (21)$$

ДОКАЗАТЕЛЬСТВО. По определению

$$\mathbf{P}\{A_1 \cup \dots \cup A_k\} = \sum_{E_j \in A_1 \cup \dots \cup A_k} \mathbf{P}\{E_j\}, \quad \mathbf{P}\{A_I\} = \sum_{E_j \in \bigcap_{i \in I} A_i} \mathbf{P}\{E_j\}.$$

Покажем, что после такой замены в правой части (21) коэффициент при $\mathbf{P}\{E_j\}$ будет равен единице, если $E_j \in A_1 \cup \dots \cup A_k$, и нулю в противном случае. Если $E_j \notin A_1 \cup \dots \cup A_k$, то $E_j \notin \bigcap_{i \in I} A_i$ при любом I . Следовательно, $\mathbf{P}\{E_j\}$ не будет входить ни в одну из сумм вида $\mathbf{P}\{A_I\}$. Пусть теперь $E_j \in A_1 \cup \dots \cup A_k$. Можно считать, что $E_j \in A_1 \cap \dots \cap A_r$, $E_j \notin A_{r+1} \cup \dots \cup A_k$. Тогда $\mathbf{P}\{E_j\}$ будет входить в сумму $\mathbf{P}\{A_I\}$, если и только если $I \subset \{1, \dots, r\}$. Значит, коэффициент при $\mathbf{P}\{E_j\}$ в правой части (21) равен

$$\sum_{t=1}^k (-1)^{t-1} \binom{r}{t} = \sum_{t=1}^r (-1)^{t-1} \binom{r}{t} = 1 - \sum_{t=0}^r (-1)^t \binom{r}{t} = 1 - (1-1)^r = 1. \nabla$$

Приведем несколько применений формул (19)–(21).

Теорема 2.21. *Если $|X| = m$, $|Y| = n$, то число $Z(m, n)$ всех сюръективных отображений $f : X \rightarrow Y$ равно $\sum_{j=0}^n (-1)^j \binom{n}{j} (n-j)^m$.*

ДОКАЗАТЕЛЬСТВО. Пусть $Y = \{y_1, \dots, y_n\}$. Обозначим через A_I множество таких функций $f : X \rightarrow Y$, что $y_i \notin f(X)$. Тогда f не сюръективное отображение, если и только если $f \in A_1 \cup \dots \cup A_n$. Поскольку всего имеется n^m отображений $f : X \rightarrow Y$, по (20) имеем

$$Z(m, n) = \sum_{j=0}^n (-1)^j \sum_{|I|=j} |A_I|,$$

где A_\emptyset – множество всех отображений $f : X \rightarrow Y$.

По определению $f \in A_I$, если и только если $f(X) \subset Y \setminus \{y_i \mid i \in I\}$. Следовательно, $|A_I| = (n - |I|)^m$. Значит,

$$Z(m, n) = \sum_{j=0}^n (-1)^j \binom{n}{j} (n-j)^m. \quad \nabla$$

Из теоремы 2.21 и утверждения 2.6 получаем

Теорема 2.22. $S(m, k) = \frac{1}{k!} \sum_{j=0}^{k-1} (-1)^j \binom{k}{j} (k-j)^m$.

Пусть S_n – множество всех перестановок чисел $1, \dots, n$. Назовем $\pi \in S_n$ *беспорядком*, если $\pi(k) \neq k$ при любых $1 \leq k \leq n$. Обозначим через D_n множество всех беспорядков на $\{1, \dots, n\}$.

Теорема 2.23. *Число $|D_n|$ всех беспорядков на $\{1, \dots, n\}$ равно*

$$n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \dots + (-1)^n \frac{1}{n!}\right) \sim \frac{n!}{e}.$$

ДОКАЗАТЕЛЬСТВО. Пусть $A_i = \{\pi \in S_n \mid \pi(i) = i\}$ ($i = 1, \dots, n$). Тогда для любого $I \subset \{1, \dots, n\}$

$$A_I = \{\pi \in S_n \mid \pi(i) = i \quad \forall i \in I\}.$$

Значит, $|A_I| = (n - |I|)!$. Число j -элементных подмножеств I множества $\{1, \dots, n\}$ равно $\binom{n}{j}$. Поскольку $D_n = S_n \setminus (A_1 \cup \dots \cup A_n)$ в силу (20), имеем

$$|D_n| = \sum_{j=0}^n (-1)^j \binom{n}{j} (n-j)! = \sum_{j=0}^n (-1)^j \frac{n!}{j!}. \quad \nabla$$

3 АЗБУКА ТЕОРИИ ГРАФОВ

3.1 Основные понятия. Способы задания графов

Граф G состоит из конечного множества V *вершин* и некоторого множества E неупорядоченных пар вершин, называемых *ребрами*.

Обычно на рисунках вершины графа изображают точками или кружками, а ребра – линиями. В *мультиграфах*, частным случаем которых являются графы, E может содержать по несколько копий одной и той же неупорядоченной пары вершин. В *псевдографах* допускаются также *петли*, т. е. пары вида (v, v) .

Для графа G через $V(G)$ и $E(G)$ обозначим множества вершин и ребер G соответственно. Если $(u, v) \in E(G)$, то говорят, что вершины u и v *смежны*. Ребро (u, v) и вершина v *инцидентны*. Если два ребра инцидентны одной и той же вершине, то они тоже называются *смежными*.

Степенью $\deg_G(v)$ вершины v в псевдографе G называют сумму числа всех ребер, инцидентных v , и числа петель, инцидентных v (таким образом, каждая петля подсчитана дважды). Вершина степени 0 называется *изолированной*, вершина степени 1 – *висячей*.

Утверждение 3.1. *Сумма степеней вершин любого псевдографа равна удвоенному числу его ребер.*

ДОКАЗАТЕЛЬСТВО. Каждое ребро вносит в указанную сумму вклад 2. ∇

Говорят, что графы $G_1 = (V_1, E_1)$ и $G_2 = (V_2, E_2)$ *изоморфны*, если существует такое взаимно однозначное отображение $f : V_1 \xrightarrow{\text{на}} V_2$, что для любых $u, v \in V_1$

$$(u, v) \in E_1 \Leftrightarrow (f(u), f(v)) \in E_2.$$

Нередко графы будут рассматриваться с точностью до изоморфизма.

Граф $G_1 = (V_1, E_1)$ называется *подграфом* графа $G_2 = (V_2, E_2)$, если $V_1 \subseteq V_2, E_1 \subseteq E_2$. Граф $G_1 = (V_1, E_1)$ называется *порожденным подграфом* графа $G_2 = (V_2, E_2)$, если $E_1 = \{(u, v) \in E_2 \mid \{u, v\} \subseteq V_1\}$. При этом говорят, что подграф G_1 *порожден* множеством вершин V_1 .

Маршрут в псевдографе G – это такая последовательность $v_0, e_1, v_1, e_2, \dots, e_n, v_n$ вершин и ребер G , что каждое ребро в этой последовательности инцидентно соседним ему вершинам. При этом говорят, что маршрут ведет из v_0 в v_n . Если $v_0 = v_n$, то маршрут называется *замкнутым*. Маршрут, все вершины которого различны, называется

путем. Замкнутый маршрут, все вершины которого различны, называется *циклом*. *Длина маршрута* – это число его ребер. *Расстоянием* $\rho_G(u, v)$ в графе G между вершинами u и v называется длина кратчайшего пути, соединяющего их.

Говорят, что граф G *связен*, если для любых его вершин u и v найдется путь, ведущий из u в v . Максимальный по включению связный подграф графа G называют *компонентой связности* G .

Полный граф K_n – это граф с n вершинами, любые две из которых соединены ребром. Множество вершин *полного двудольного графа* $K_{m,n}$ состоит из двух подмножеств V_1 и V_2 , $|V_1| = m$, $|V_2| = n$, а $E(K_{m,n}) = \{(u, v) \mid u \in V_1, v \in V_2\}$.

Имеется ряд способов, чтобы задать граф:

- 1) рисунок;
- 2) матрица инциденций;
- 3) матрица смежности;
- 4) список ребер;
- 5) списки инцидентностей.

3.2 Деревья, характеристики деревьев

Связный граф без циклов называется *деревом*. *Лес* – это граф без циклов. Таким образом, лес – это граф, каждая компонента связности которого – дерево, а дерево – это связный лес.

Теорема 3.2. Пусть $G = (V, E)$ – граф с n вершинами. Тогда следующие условия эквивалентны:

- (а) G – дерево;
- (б) любые две вершины в G соединены ровно одним путем;
- (в) G связен и имеет $n - 1$ ребро;
- (г) G имеет $n - 1$ ребро и не имеет циклов;
- (д) G не имеет циклов и добавление к G любого ребра приводит к графу ровно с одним циклом;
- (е) G – связный граф, не совпадающий с K_n при $n \geq 3$, и добавление к G любого ребра приводит к графу с ровно одним циклом.

ДОКАЗАТЕЛЬСТВО. (а) \Rightarrow (б). Так как G связен, любые две его вершины соединены хотя бы одним путем. Предположим, что есть два разных пути (v_0, v_1, \dots, v_t) и (u_0, u_1, \dots, u_s) , соединяющие вершины $x = v_0 = u_0$ и $y = v_t = u_s$. Пусть i – наименьшее натуральное число, для которого $u_i \neq v_i$, а $j = \min\{k > i \mid u_k \in \{v_0, v_1, \dots, v_t\}\}$. Можно считать, что $u_j = v_r$. Тогда в G есть цикл $(v_{i-1}, v_i, \dots, v_r = u_j, u_{j-1}, \dots, u_{i-1})$. Значит, G – не дерево.

(б) \Rightarrow (в). Поскольку любые две вершины соединены путем, граф G связен. Покажем индукцией по числу вершин, что $|E| + 1 = |V|$.

Если $|V| = 1$ или $|V| = 2$, то утверждение очевидно. Пусть $|V| > 2$ и $e = (v, u)$ – некоторое ребро в G . Рассмотрим $H = G \setminus \{e\}$. Согласно (б) в H нет пути из u в v . Пусть V_1 – множество вершин, которые в G соединены с u путями, не проходящими через v , а V_2 – множество вершин, которые в G соединены с v путями, не проходящими через u . Тогда подграф G_1 графа G , порожденный множеством V_1 , связен, поскольку каждую его вершину какой-то путь, использующий лишь вершины из V_1 , соединяет с u . Аналогично, подграф G_2 графа G , порожденный множеством V_2 , связен. По индукционному предположению, $e_1 = |V_1| - 1$, $e_2 = |V_2| - 1$, где e_i – число ребер в G_i ($i = 1, 2$). Следовательно,

$$|E| = e_1 + e_2 + 1 = (|V_1| - 1) + (|V_2| - 1) + 1 = |V| - 1.$$

(в) \Rightarrow (г). Предположим, что в $G = (V, E)$ есть цикл C с k вершинами. Для каждой вершины $v \in V \setminus C$ найдется кратчайший путь от v до C (возможно, их несколько). Поставим каждой такой вершине в соответствие первое ребро этого пути. Поскольку любое ребро будет поставлено в соответствие не более чем одной вершине, число таких ребер не менее $n - k$. Отсюда $|E| \geq k + (n - k)$, что противоречит (в).

(г) \Rightarrow (а). Так как G не имеет циклов, то G – лес. Если G имеет k компонент связности (деревьев), то (поскольку (а) \Rightarrow (в)) в G ровно $n - k$ ребер. По условию $|E| = n - 1$. Значит, $k = 1$.

(б) \Rightarrow (д). Так как любые две вершины соединены ровно одним путем, добавив любое ребро, получим ровно один цикл.

(д) \Rightarrow (е). Если бы G не был связным, то добавление ребра, соединяющего разные компоненты связности, давало бы граф без циклов.

(е) \Rightarrow (а). Предположим, что в G есть цикл. Этот цикл должен быть 3-циклом, иначе добавление диагонали привело бы к наличию как минимум трех циклов. Пусть это цикл (x, y, z) . Так как $G \neq K_3$ и связен, то найдется вершина v , смежная с x, y или z . Можно считать, что v смежна с x . Тогда добавление ребра (v, y) приводит к графу с более чем одним циклом. ∇

Следствие 3.3. *В любом дереве $T = (V, E)$ с $|V| \geq 2$ имеется не менее двух висячих вершин.*

3.3 Кодирование деревьев

Задавать деревья можно по-разному. В гл. 2 описывался способ задания плоских корневых деревьев. Одним из экономных способов записи деревьев является *код Прюфера*.

Пусть T – некоторое дерево, вершины которого занумерованы числами $1, 2, \dots, n$. Тогда код Прюфера для T строится по следующим правилам.

Удаляем висячую вершину с наименьшим номером и записываем номер ее соседа. В оставшемся дереве снова удаляем висячую вершину с наименьшим номером и выписываем номер ее соседа рядом с уже записанным. Повторяем эту процедуру $n - 1$ раз. Полученная последовательность из $n - 1$ чисел называется кодом Прюфера для T .

Теорема 3.4. *Для любой последовательности (a_1, \dots, a_{n-1}) натуральных чисел такой, что*

$$1 \leq a_i \leq n \ (i = 1, 2, \dots, n - 2), a_{n-1} = n, \quad (22)$$

существует единственное дерево на множестве вершин $\{1, 2, \dots, n\}$, код Прюфера которого совпадает с данной последовательностью.

ДОКАЗАТЕЛЬСТВО. Заметим сначала, что в силу следствия 3.3 последним числом в коде Прюфера должно быть n .

Единственность. Пусть T – дерево и (a_1, \dots, a_{n-1}) – его код Прюфера. Обозначим через b_i ($i = 1, 2, \dots, n - 1$) номер вершины, которую мы удаляли на шаге i . Очевидно, $b_i \notin \{b_1, \dots, b_{i-1}, a_i\}$. Кроме того, $b_i \notin \{a_{i+1}, \dots, a_n\}$, поскольку при $j > i$ вершина a_j принадлежит дереву $T \setminus \{b_1, \dots, b_i\}$. И наоборот, если $k \notin \{b_1, \dots, b_{i-1}, a_i, a_{i+1}, \dots, a_{n-1}\}$, то k является висячей вершиной в $T \setminus \{b_1, \dots, b_{i-1}\}$ (иначе на каком-нибудь шаге $q > i$ она оказалась бы соседней с висячей вершиной b_q и совпала бы с a_q). Значит,

$$b_i = \min\{k \mid k \notin \{b_1, \dots, b_{i-1}, a_i, a_{i+1}, \dots, a_{n-1}\}\}. \quad (23)$$

Таким образом, последовательность (a_1, \dots, a_{n-1}) однозначно (по правилу (23)) определяет последовательность $\{b_1, \dots, b_{n-1}\}$. Поскольку (b_i, a_i) – ребро в T для любого $i \in \{1, \dots, n - 1\}$, последовательность (a_1, \dots, a_{n-1}) однозначно определяет T .

Существование. Пусть последовательность (a_1, \dots, a_{n-1}) удовлетворяет (22). По правилу (23) построим соответствующую ей последовательность $\{b_1, \dots, b_{n-1}\}$ и проведем ребра (b_i, a_i) для всех $i \in \{1, \dots, n - 1\}$. Получим некоторый граф G . Обозначим

$$G_i = G \setminus \{b_1, \dots, b_{i-1}\}, \quad i = 1, \dots, n - 1.$$

Покажем, что

- (а) G – дерево,
- (б) код Прюфера для G есть (a_1, \dots, a_{n-1}) .

Для доказательства (а) достаточно убедиться, что b_i – висючая вершина в G_i для любого i , а для (б) – что номер любой висючей вершины в G_i не меньше, чем b_i .

Поскольку согласно (23) $a_i \notin \{b_1, \dots, b_{i-1}\}$, имеем $a_i \in V(G_i)$. Следовательно, b_i смежна с некоторой вершиной из G_i . Предположим, что b_i смежна в G_i с какой-то вершиной $x \neq a_i$. Тогда ребро, соединяющее b_i с этой вершиной, должно иметь вид (a_j, b_j) , где $j > i$, так как $b_j \in V(G_i)$. Поскольку все b_k различны, имеем $b_j \neq b_i$. Значит, $b_i = a_j$ и $j > i$, что противоречит (23). Следовательно, наше предположение неверно, и вершина b_i смежна в G_i лишь с a_i . Итак, все G_i являются деревьями.

Предположим теперь, что в G_i есть висючая вершина k и $k < b_i$. Поскольку при построении последовательности $\{b_1, \dots, b_{n-1}\}$ по правилам (23) мы не положили $b_i = k$, то это значит, что или $k \in \{b_1, \dots, b_{i-1}\}$, или $k \in \{a_i, a_{i+1}, \dots, a_{n-1}\}$. Первое невозможно, так как $\{b_1, \dots, b_{i-1}\} \cap V(G_i) = \emptyset$. Значит, $k = a_j$ для некоторого $j > i$. Как отмечалось, b_j – висючая вершина в G_j , смежная с a_j . Но $a_j = k$ – висючая вершина в G_i , а следовательно, и в G_j . Таким образом, G_j имеет только две вершины: a_j и b_j , т.е. $j = n - 1$ и $a_j = n$. Но $n \geq b_i > k$. ∇

Теорема 3.5. (Теорема Кэли.) Число n -вершинных деревьев с помеченными вершинами равно n^{n-2} .

3.4 Эйлеровы обходы

Эйлеров обход (цикл) в псевдографе G – это такой замкнутый маршрут M в G , что каждое ребро входит в M ровно один раз. В известной в свое время задаче о кенигсбергских мостах требовалось указать эйлеров цикл в одном из мультиграфов. Задачи о рисовании фигур без отрыва карандаша от бумаги тоже сводятся к изучению эйлеровых обходов.

Назовем псевдограф *эйлеровым*, если в нем есть эйлеров цикл. Ясно, что эйлеров псевдограф связан.

Теорема 3.6. Для связного псевдографа $G = (V, E)$ следующие утверждения эквивалентны:

- (а) G – эйлеров псевдограф;
- (б) каждая вершина псевдографа G имеет четную степень;
- (в) множество ребер псевдографа G можно разбить на простые циклы.

ДОКАЗАТЕЛЬСТВО. (а) \Rightarrow (б). Пусть M – эйлеров цикл в G , v – произвольная вершина в G . При каждом прохождении M через v используются два ребра, инцидентных v .

(б) \Rightarrow (в). Индукцией по числу ребер в G . Пусть G – наименьший по числу ребер псевдограф, для которого наше утверждение не доказано. Если в G нет ребер, то утверждение тривиально. Если G связный и нетривиальный, то степень каждой вершины не меньше двух и по следствию 3.3 в G есть цикл C . Удалив ребра C из G , снова получим псевдограф (обозначим его G'), степени всех вершин которого четны. По индукционному предположению ребра каждой компоненты связности псевдографа G' можно разбить на циклы.

(в) \Rightarrow (а). Индукцией по числу ребер в G . Пусть G – наименьший по числу ребер псевдограф, для которого наше утверждение не доказано, и пусть C_1 – один из циклов, на которые разбито $E(G)$. Рассмотрим G' , полученный из G удалением ребер цикла C_1 . По индукционному предположению, в каждой компоненте связности H_i псевдографа G' есть эйлеров цикл M_i . Из них и цикла C_1 легко строится эйлеров цикл для G . ∇

Следствие 3.7. Пусть G – связный псевдограф, $x, y \in V(G)$. В G существует маршрут, связывающий x с y , который содержит каждое ребро G ровно по одному разу, если и только если степени всех вершин, кроме x и y , четны, а степени x и y нечетны.

3.5 Двудольные графы

Мультиграф $G = (V, E)$ называется *двудольным*, если множество его вершин можно так разбить на две части (доли) V_1 и V_2 , что один из концов любого ребра принадлежит V_1 , а другой – V_2 .

Примеры

1. Любой лес – двудольный граф.
2. Циклы четной длины являются двудольными графами, а циклы нечетной длины – не являются таковыми.

Теорема 3.8. Граф G является двудольным, если и только если в G нет циклов нечетной длины.

ДОКАЗАТЕЛЬСТВО. \Rightarrow). Если в G есть цикл нечетной длины, то, как отмечалось в примере 2, G недвудолен.

\Leftarrow). Достаточно доказать утверждение теоремы для связных графов. Выберем произвольную вершину $v \in V(G)$. Пусть X_i ($i = 0, 1, 2, \dots$) – множество вершин графа G , находящихся на расстоянии i от v . Имеем $X_0 = \{v\}$, $X_1 = \{x \in V(G) \mid (x, v) \in E(G)\}$. Предположим, что для

некоторого i найдутся $x, y \in X_i$ с $(x, y) \in E(G)$. Пусть (x_0, x_1, \dots, x_i) и (y_0, y_1, \dots, y_i) , где $x_0 = y_0 = v, x_i = x, y_i = y$ являются кратчайшими путями от v до x и y , а $x_j = y_j$ – последняя общая вершина на этих путях. Тогда цикл $(x_j, x_{j+1}, \dots, x_i, y_i, y_{i-1}, \dots, y_j)$ имеет нечетную длину. Из полученного противоречия следует, что каждое ребро в G соединяет X_i с X_{i+1} для некоторого $i \geq 0$. Положим $V_1 = X_0 \cup X_2 \cup X_4 \cup \dots$, $V_2 = X_1 \cup X_3 \cup X_5 \cup \dots$. ∇

Паросочетанием в мультиграфе называется любой набор попарно несмежных ребер. Паросочетание, покрывающее все вершины мультиграфа, называется *совершенным паросочетанием*. Такое паросочетание содержит $|V(G)|/2$ ребер.

Для каждого мультиграфа G через $\pi(G)$ обозначим мощность наибольшего паросочетания в G , а через $\tau(G)$ – мощность наименьшего множества ребер, покрывающего все ребра G .

Очевидно, $\pi(G) \leq \tau(G)$ для любого мультиграфа G . Для цикла C_5 длины 5 имеем $\pi(C_5) = 2, \tau(C_5) = 3$. Для полного графа K_n на n вершинах имеем $\pi(K_n) = \lfloor n/2 \rfloor, \tau(K_n) = n - 1$.

Теорема 3.9. (Теорема Кёнига.) *Для любого двудольного мультиграфа G*

$$\pi(G) = \tau(G).$$

ДОКАЗАТЕЛЬСТВО. Пусть $G = (V, E)$ – наименьший по числу ребер двудольный мультиграф, для которого

$$\pi(G) < \tau(G). \quad (24)$$

Тогда в G найдется вершина, смежная с двумя или более другими вершинами. Можно считать, что долями G являются V_1 и V_2 , $x \in V_1$, $e_1 = (x, y_1) \in E, e_2 = (x, y_2) \in E, y_1 \neq y_2, G_1 = G \setminus \{e_1\}, G_2 = G \setminus \{e_2\}$. Ввиду минимальности G имеем $\pi(G_1) = \tau(G_1), \pi(G_2) = \tau(G_2)$. Учитывая (24) и то, что $\tau(G_i) \leq \tau(G)$ ($i = 1, 2$), получаем

$$\pi(G_i) = \tau(G_i) = \pi(G), \quad i = 1, 2.$$

Пусть S_i – множество вершин, покрывающее все ребра G_i , и $|S_i| = \pi(G)$ ($i = 1, 2$). Тогда

$$x, y_i \notin S_i, y_{3-i} \in S_i, \quad i = 1, 2. \quad (25)$$

Обозначим $R = S_1 \cap S_2, r = |R|, t = \pi(G)$. Далее, обозначим через H подграф мультиграфа G , порожденный множеством вершин $(S_1 \setminus R) \cup$

$\cup (S_2 \setminus R) \cup \{x\}$. Пусть долями двудольного мультиграфа H являются A и B , причем $|A| \leq |B|$. Имеем

$$|A| \leq \lfloor ((S_1 \setminus R) \cup (S_2 \setminus R) \cup \{x\})/2 \rfloor = \lfloor (2(t-r) + 1)/2 \rfloor = t-r.$$

Покажем, что $A \cup R$ покрывает все ребра G . Действительно, рассмотрим произвольное ребро $e \in E$. Если хотя бы один конец e принадлежит R , то $A \cup R$ покрывает e . Убедимся, что когда оба конца e не принадлежат R , тогда $e \in E(H)$. Отсюда сразу следовало бы, что A покрывает e . В силу (25) ребра (x, y_1) и (x, y_2) принадлежат $E(H)$. Если $e \notin \{(x, y_1), (x, y_2)\}$, то $S_1 \setminus R$ и $S_2 \setminus R$ должны быть инцидентны e , и, следовательно, e соединяет $S_1 \setminus R$ с $S_2 \setminus R$. Снова оба конца e принадлежат $V(H)$.

Таким образом,

$$\tau(G) \leq |A \cup R| \leq (t-r) + r = t = \pi(G). \quad \nabla$$

Для любого мультиграфа $G = (V, E)$ и любого $W \subseteq V$ через $N_G(W)$ обозначим множество $\{v \in V \setminus W \mid \exists w \in W : (w, v) \in E\}$.

Следствие 3.10. (Теорема Кёнига – Оре.) *Пусть $G = (V, E)$ – двудольный мультиграф с долями V_1 и V_2 . В G существует паросочетание, покрывающее V_1 , если и только если*

$$|N_G(A)| \geq |A| \quad \forall A \subseteq V_1. \quad (26)$$

ДОКАЗАТЕЛЬСТВО. \Rightarrow). Если $|N_G(A)| < |A|$ для некоторого $A \subseteq V_1$, то не существует паросочетания, покрывающего A .

\Leftarrow). Предположим, что $\pi(G) < |V_1|$. Тогда по теореме 3.9 $\tau(G) < |V_1|$. Пусть S – множество вершин, покрывающее все ребра G , с $|S| = s < |V_1|$. Обозначим $A_1 = V_1 \setminus S$, $A_2 = V_2 \setminus S$. Тогда

$$|A_1| + |A_2| = |V_1| + |V_2| - s \geq |V_2| + 1.$$

Другими словами, $|A_1| \geq |V_2 \setminus A_2| + 1$. Так как S покрывает все ребра G , имеем $N_G(A_1) \subseteq V_2 \setminus A_2$. Следовательно,

$$|N_G(A_1)| \leq |V_2 \setminus A_2| \leq |A_1| - 1. \quad \nabla$$

Системой различных представителей для семейства множеств $\{A_i\}_{i=1}^k$ называется такой набор $\{a_1, \dots, a_k\}$ элементов множества $\bigcup_{i=1}^k A_i$, что $a_i \in A_i$ для каждого $i \in \{1, \dots, k\}$ и все a_i различны.

Теорема 3.11. (Теорема Холла.) Пусть $\{A_i\}_{i=1}^k$ – семейство подмножеств множества $\{v_1, \dots, v_n\}$. Система различных представителей для $\{A_i\}_{i=1}^k$ существует, если и только если для любого подмножества I множества $\{1, \dots, k\}$

$$\left| \bigcup_{i \in I} A_i \right| \geq |I|. \quad (27)$$

ДОКАЗАТЕЛЬСТВО. Построим двудольный граф $G = (V, E)$ по следующим правилам: долями V будут множества $V_1 = \{A_1, \dots, A_k\}$ и $V_2 = \{v_1, \dots, v_n\}$, а пара (A_i, v_j) будет ребром, если и только если $v_j \in A_i$. Тогда наличие паросочетания в G , покрывающего $V_1 = \{A_1, \dots, A_k\}$, соответствует наличию системы различных представителей для $\{A_i\}_{i=1}^k$. По следствию 3.10 наличие такого паросочетания в G эквивалентно выполнению (26). Но выполнение (26) для построенного нами графа эквивалентно выполнению (27) для $\{A_i\}_{i=1}^k$. ∇

В ряде практических и теоретических задач требуется покрыть множество ребер какого-нибудь графа наименьшим числом паросочетаний. Поскольку два смежных ребра нельзя покрыть одним и тем же паросочетанием, то для покрытия ребер любого графа требуется не меньше паросочетаний, чем максимальная степень его вершин.

Теорема 3.12. (Теорема Кёнига.) Пусть $G = (V, E)$ – двудольный мультиграф с максимальной степенью вершин, равной k . Тогда множество E можно разбить на k паросочетаний.

ДОКАЗАТЕЛЬСТВО. Пусть $V = V_1 \cup V_2$ – некоторое разбиение V на две доли: $|V_1| = n_1$, $|V_2| = n_2$, $n_1 \geq n_2$. Добавим $n_1 - n_2$ новых вершин к V_2 , а затем будем добавлять к полученному мультиграфу на $2n_1$ вершинах ребра, пока не получим k -однородный двудольный мультиграф с $2n_1$ вершинами. Обозначим этот мультиграф через H .

Для любого $A \subseteq V_1$ имеем $|N_H(A)| \geq |A|$, поскольку из A выходят $k|A|$ ребер, а каждая вершина из $N_H(A)$ инцидентна не более чем k таким ребрам. Значит, по следствию 3.10 существует паросочетание π_1 , покрывающее V_1 . Поскольку $|V(H)| = 2|V_1|$, паросочетание π_1 покрывает все вершины H , и $H_1 = H \setminus \pi_1$ является $(k-1)$ -однородным мультиграфом. Снова, по следствию 3.10, существует паросочетание π_2 , покрывающее V_1 . Построим $H_2 = H_1 \setminus \pi_2$ и т. д. Через k шагов будут построены k паросочетаний, в совокупности покрывающих $E(H)$. Удалив из этих паросочетаний ребра, не принадлежащие $E(G)$, получим требуемое разбиение множества ребер G . ∇

3.6 Принцип Дирихле

Стандартным способом доказательства существования объектов, обладающих теми или иными свойствами, в дискретной математике является конструирование таких объектов. Но иногда наилучшим оказывается использование мощностных соображений.

Принцип Дирихле состоит в следующем: если $k + 1$ предметов раскладываются в k ящиков, то хотя бы один ящик содержит более одного предмета.

В качестве применения этой идеи рассмотрим две задачи о турнирах.

Турнир T состоит из множества игроков V и множества E результатов турнира. Множество E состоит из $\binom{|V|}{2}$ упорядоченных пар элементов множества V , и для любой пары $\{u, v\} \subset V$ в точности одна из пар $(u, v), (v, u)$ принадлежит E . (Содержательный смысл пары (u, v) : игрок u выиграл у игрока v .)

Часто элементы множества игроков изображают точками или кружками на плоскости, а элементы E – дугами, соединяющими эти точки. Поскольку для любой пары $\{u, v\} \subset V$ имеется ровно две возможности выбора дуги, соединяющей эти вершины, то всего на множестве из n различных игроков можно построить $2^{\binom{n}{2}}$ различных турниров.

Гамильтоновым путем в турнире $T = (V, E)$ с $V = \{v_1, \dots, v_n\}$ называется такая перестановка $\Gamma = (v_{i_1}, \dots, v_{i_n})$ игроков турнира, что $(v_{i_j}, v_{i_{j+1}}) \in E$ для каждого $j \in \{1, \dots, n-1\}$. Число различных гамильтоновых путей, которые можно построить на множестве из n игроков, равно $n!$.

Г. Селе (1943 г.) доказал, что в любом турнире с количеством игроков n число гамильтоновых путей меньше, чем $n!2^{-3n/4}$.

Теорема 3.13. *Существует турнир с количеством игроков n , содержащий не менее $n!2^{-n+1}$ гамильтоновых путей.*

ДОКАЗАТЕЛЬСТВО. Пусть \mathcal{T}_n – множество всех турниров на множестве игроков $\{v_1, \dots, v_n\}$. Как отмечалось, $|\mathcal{T}_n| = 2^{\binom{n}{2}}$. Положим

$$\mathcal{U} = \{(T, \Gamma) \mid T \in \mathcal{T}_n, \Gamma \text{ – гамильтонов путь в } T\}.$$

Тогда

$$|\mathcal{U}| = \sum_{T \in \mathcal{T}_n} |\{\Gamma \mid (T, \Gamma) \in \mathcal{U}\}| = \sum_{\Gamma} |\{T \in \mathcal{T}_n \mid (T, \Gamma) \in \mathcal{U}\}|. \quad (28)$$

Зафиксируем произвольный гамильтонов путь Γ . Этот путь фиксирует направление $n - 1$ дуг. Значит, существует $2^{\binom{n}{2} - n + 1}$ турниров,

содержащих Γ . Таким образом,

$$\sum_{\Gamma} |\{T \in \mathcal{T}_n \mid (T, \Gamma) \in \mathcal{U}\}| = n!2^{\binom{n}{2}-n+1},$$

откуда с учетом (28) имеем

$$n!2^{\binom{n}{2}-n+1} = \sum_{T \in \mathcal{T}_n} |\{\Gamma \mid (T, \Gamma) \in \mathcal{U}\}|.$$

В последней сумме $2^{\binom{n}{2}}$ слагаемых. Следовательно, хотя бы одно из них не меньше

$$n!2^{\binom{n}{2}-n+1} / 2^{\binom{n}{2}} = n!2^{-n+1}. \quad \nabla$$

Назовем турнир $T = (V, E)$ *транзитивным*, если существует такая перестановка $(v_{i_1}, \dots, v_{i_n})$ его игроков v_1, \dots, v_n , что при любых $1 \leq j < k \leq n$ имеем $(v_{i_j}, v_{i_k}) \in E$. Пусть $\alpha(n)$ – наибольшее целое число такое, что в любом турнире с количеством игроков n есть транзитивный подтурнир с количеством игроков $\alpha(n)$.

Примеры

$\alpha(2) = 2$, $\alpha(3) = 2$. Нетрудно доказать, что $\alpha(4) = 3$.

Утверждение 3.14. *Справедливо неравенство $\alpha(n) \geq 1 + \lfloor \log_2 n \rfloor$.*

ДОКАЗАТЕЛЬСТВО. При $n \leq 3$ это следует из примера. Пусть утверждение доказано для всех $n' < n$. Рассмотрим произвольный турнир T_n на множестве игроков v_1, \dots, v_n .

Случай 1. *Число игроков, которых победил игрок v_n , не менее $\lceil (n-1)/2 \rceil$.* Не теряя общности, мы можем предположить, что это игроки v_1, \dots, v_k , где $k \geq \lceil (n-1)/2 \rceil = \lfloor n/2 \rfloor$. По индукционному предположению подтурнир T_k на множестве $\{v_1, \dots, v_k\}$ содержит некоторый транзитивный подтурнир T_r на каком-то множестве $\{v_{i_1}, \dots, v_{i_r}\}$, где $r \geq 1 + \lfloor \log_2 k \rfloor \geq 1 + \lfloor \log_2 \lfloor n/2 \rfloor \rfloor$.

Покажем, что для любого натурального n

$$\lfloor \log_2 \lfloor n/2 \rfloor \rfloor = \lfloor \log_2(n/2) \rfloor. \quad (29)$$

Действительно, при четном n имеем $\lfloor n/2 \rfloor = n/2$. Пусть $n = 2m + 1$. Равенство $\lfloor \log_2(n/2) \rfloor = s$ означает, что $2^s \leq n/2 < 2^{s+1}$, т. е. $2^s \leq m + 1/2 < 2^{s+1}$. Но тогда, поскольку m целое, $2^s \leq m$, откуда $s \leq \log_2 m = \log_2 \lfloor n/2 \rfloor$. Последнее неравенство эквивалентно (29).

Таким образом, $r \geq 1 + \lfloor \log_2(n/2) \rfloor = \lfloor \log_2 n \rfloor$. Поскольку v_n победил всех игроков из T_r , в T_n есть транзитивный подтурнир с количеством игроков $r + 1$.

Случай 2. Число игроков, которых победил игрок v_n , меньше, чем $\lceil (n-1)/2 \rceil$. Тогда число победивших v_n больше $\lceil (n-1)/2 \rceil$, и снова можно рассуждать как в случае 1. ∇

Теорема 3.15. *Справедливо неравенство $\alpha(n) \leq 1 + \lfloor 2 \log_2 n \rfloor$.*

ДОКАЗАТЕЛЬСТВО. Нам требуется показать, что в T_n есть турнир, не содержащий транзитивного подтурнира с количеством игроков $k = 2 + \lfloor 2 \log_2 n \rfloor$.

Пусть \mathcal{I} – класс тех турниров из T_n , которые содержат транзитивный подтурнир с количеством игроков k . Тогда

$$\mathcal{I} = \bigcup_A \bigcup_{\sigma} \mathcal{I}_{A,\sigma},$$

где A пробегает все k -элементные подмножества множества $\{1, \dots, n\}$, σ – все перестановки элементов множества A , а $\mathcal{I}_{A,\sigma}$ обозначает множество таких турниров $T \in \mathcal{I}$, что подтурнир турнира T на множестве A транзитивен и старшинство игроков из A порождается перестановкой σ .

Понятно, что $|\mathcal{I}_{A,\sigma}| = 2^{\binom{n}{2} - \binom{k}{2}}$. Следовательно,

$$\begin{aligned} |\mathcal{I}| &\leq \sum_{|A|=k} \sum_{\sigma \in S_k} 2^{\binom{n}{2} - \binom{k}{2}} = \binom{n}{k} k! 2^{\binom{n}{2} - \binom{k}{2}} = 2^{\binom{n}{2}} 2^{-\binom{k}{2}} \frac{n!}{(n-k)!} < \\ &< 2^{\binom{n}{2}} n^k 2^{-k(k-1)/2} \leq 2^{\binom{n}{2}} \left(n 2^{-(k-1)/2} \right)^k \leq \\ &\leq 2^{\binom{n}{2}} \left(n 2^{-(1+\lfloor 2 \log_2 n \rfloor)/2} \right)^k < 2^{\binom{n}{2}} \left(n 2^{-\log_2 n} \right)^k \leq 2^{\binom{n}{2}} = |T_n|. \end{aligned}$$

Значит, $T_n \setminus \mathcal{I} \neq \emptyset$. ∇

Содержание

1	АЛГЕБРА ВЫСКАЗЫВАНИЙ И БУЛЕВЫ ФУНКЦИИ	4
1.1	Высказывания. Логические операции	4
1.2	Эквивалентность. Таблицы истинности	5
1.3	Совершенные нормальные формы	6
1.4	Двойственность, монотонность, линейность. Замкнутые классы	8
1.5	Критерий полноты	10
1.6	Применение алгебры высказываний в теории множеств	13
1.7	Понятие о предикатах	14
1.8	Синтез схем (π -схемы, контактные схемы, схемы из функ- циональных элементов)	16
2	ЭЛЕМЕНТЫ КОМБИНАТОРИКИ	20
2.1	Подсчет числа отображений конечных множеств в конечные множества с различными элементами	20
2.2	Разбиения конечных множеств и числа Стирлинга второго рода	23
2.3	Разбиения чисел на слагаемые. Диаграммы Ферре	25
2.4	Возвратные последовательности	28
2.5	Числа Каталана	32
2.6	Производящие функции	34
2.7	Некоторые вероятностные задачи с конечным пространством элементарных событий	36
2.8	Случайные величины. Схема Бернулли	42
2.9	Формула включений и исключений	46
3	АЗБУКА ТЕОРИИ ГРАФОВ	49
3.1	Основные понятия. Способы задания графов	49
3.2	Деревья, характеристики деревьев	50
3.3	Кодирование деревьев	52
3.4	Эйлеровы обходы	53
3.5	Двудольные графы	54
3.6	Принцип Дирихле	58

Подписано в печать		Формат 60 × 84/16
Офсетная печать		Уч.-изд. л. 4
Заказ N	Цена	Тираж 300 экз.

Редакционно-издательский отдел Новосибирского государственного университета; участок оперативной полиграфии НГУ; 630090, Новосибирск 90, ул. Пирогова, 2.