МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО

ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Московский государственный институт

электроники и математики (Технический университет)

В.А. Носов

Комбинаторика и теория графов

Утверждено Редакционно-издательским

советом института

в качестве учебного пособия

Москва, 1999

УДК 519.1

Носов Валентин Александрович

Комбинаторика и теория графов

Учебное пособие

Пособие содержит изложение основ комбинаторики и теории графов в соответствии с программой семестрового курса для студентов младших курсов, обучающихся по специальности "Прикладная математика"

Рецензенты:
Кафедра математической теории интеллектуальных
систем МГУ им. М.В. Ломоносова
(зав. кафедрой профессор Кудрявцев В.Б.)
профессор Строгалов А.С. (РГГУ)

Электронная версия подготовлена к публикации на web-сервере "Интеллектуальные системы" (http://intsys.msu.ru) кафедры Математической теории интеллектуальных систем механико-математического факультета МГУ имени М.В. Ломоносова

Электронный адрес автора - vnosov@intsys.msu.ru

Оглавление

ВВЕДЕНИЕ

Настоящее пособие подготовлено на основе лекций по одноименному семестровому курсу, читаемому в 2-м семестре для студентов, обучающихся по специальности "Прикладная математика".

В настоящее время имеется ряд обстоятельных руководств как по комбинаторике, так и по теории графов, однако, по мнению автора, ощущается потребность в небольшом пособии, охватывающем все темы курса, ориентированном на читателя со скромной математической подготовкой.

Предлагаемое пособие отличается от известных руководств такого типа двумя существенными обстоятельствами. Изложение организуется так, чтобы кроме необходимых сведений дать материал, относящийся к приложениям и к развитию изучаемой проблематики. Уделено повышенное внимание конструктивному направлению, связанному с разработкой комбинаторных и графических алгоритмов.

Список литературы представлен в конце пособия. Нумерация утверждений и ссылок независима в каждом параграфе.

Знаки ▸ и ◂ означают начало и конец доказательства.

Автор выражает признательность всем прочитавшим рукопись пособия и сделавшим свои замечания по его улучшению.

ГЛАВА I. ВВЕДЕНИЕ В КОМБИНАТОРИКУ.

§ 1. Множества. Отображения.

1. Множества.

Основные понятия теории множеств будут играть в дальнейшем существенную роль. Понятие “множество” является первичным и неопределяемым. Предметы (объекты), составляющие данное множество, называются его элементами. Тот факт, что элемент x принадлежит множеству A записывается так: $x \in A$, в противном случае пишем $x \overline{\in} A$. Для однозначного описания некоторого множества мы будем пользоваться следующими способами:

а) давать список элементов, входящих в данное множество. Если множество A состоит из элементов $a_1, \dots, a_n$ то будем писать $A = \{ a_1, \dots, a_n \}$.

б) указывать общее свойство элементов, принадлежащих множеству A. Будем писать $A = \{x \mid P(x)\}$, что означает “множество всех x, таких, что выполнено P(x)”. Здесь P(x) - означает свойство, характеризующее в точности все элементы множества A.

в) указывать порождающую процедуру, т.е. способ получения элементов множества A.

г) указывать разрешающую процедуру, т.е. правило решения вопроса, верно ли $x \in A$ для любого x.

Если каждый элемент множества A является элементом множества B, то A называется подмножеством множества B. (обозначение $A \subseteq B$). Два множества A и B называются равными, если справедливо $A \subseteq B$ и $B \subseteq A$. (обозначение A = B).

Объединение множеств A и B(обозначение - $A \bigcup B$) есть множество, состоящее из тех и только тех элементов, которые принадлежат хотя бы одному из множеств A или B, т.е.

$$A \bigcup B = \{x \mid x \in A \text{ или } x \in B\}$$

Аналогично определяется объединение произвольной системы множеств $A_1, \dots, A_n$:

$$A_1 \bigcup \dots \bigcup A_n = \{x \mid x \in A_i \text{ для некоторого } i \in \overline{1, n}\}$$

Пересечением множеств A и B (обозначение: $A \bigcap B$) называется множество, состоящее из тех и только тех элементов, которые принадлежат обоим множествам A и B, т.е.

$A \bigcap B = \{x | x \in A \text{ и } x \in B\}$

Аналогично определяется пересечение произвольной системы множеств $A_1, \ldots, A_n$:

$$A_1 \bigcap \ldots \bigcap A_n = \{x | x \in A_i \text{ для всех } i \in \overline{1,n}\}$$

Разностью множеств A и B (обозначение: A\B) называется множество, состоящее из тех и только тех элементов A, которые не принадлежат B, т.е.

$$A \backslash B = \{x | x \in A \text{ и } x \overline{\in} B\}$$

Если A - подмножество множества E, то дополнение множества A в множестве E (обозначение: $\overline{A}$ или $C_E A$) есть множество, состоящее из тех и только тех элементов E, которые не принадлежат A, т.е.

$$\overline{A} = \{x | x \in E \text{ и } x \overline{\in} A\}$$

Множество, не содержащее элементов, называется пустым множеством и обозначается $\varnothing$.

Примем следующее соглашение об обозначениях: Высказывание “из P следует Q” будем обозначать $P \Rightarrow Q$. Если $P \Rightarrow Q$ и $Q \Rightarrow P$, то используем обозначение $P \Leftrightarrow Q$, что эквивалентно высказыванию “P справедливо тогда и только тогда, когда справедливо Q”. Высказывание “для всех x справедливо P(x)” будем обозначать $\forall x\ P(x)$, высказывание “существует x, такое, что справедливо P(x)” будем обозначать $\exists x\ P(x)$. Булеан множества A (обозначение: B(A)) есть множество всех подмножеств множества A, т.е.

$$B(A) = \{x | x \subseteq A\}$$

Прямое (декартово) произведение непустых множеств A и B(обозначение: $A \times B$) определяется как множество всех упорядоченных пар вида (x_1,x_2), где $x_1 \in A$, $x_2 \in B$. Для упорядоченных пар (x_1,x_2), (x_1', x_2') справедливо:

$$(x_1,x_2) = (x_1', x_2') \Leftrightarrow x_1 = x_1',\ x_2 = x_2'.$$

Аналогично определяется прямое произведение системы множеств $A_1, \ldots, A_n$:

$$A_1 \times \ldots \times A_n\ \{ (x_1, \ldots, x_n) | x_1 \in A_1, \ldots, x_n \in A_n \}$$

причем $(x_1, \ldots, x_n) = (x_1', \ldots, x_n') \Leftrightarrow x_i = x_i',\ \forall\ i \in \overline{1,n}$

Если $A_1 = \ldots = A_n = A$, то $A_1 \times \ldots \times A_n$ обозначим A^n.

2. Отображения.

Пусть A и B непустые множества. Если каждому элементу $x \in A$ ставится в соответствие единственный элемент $y \in B$, то говорят, что задано отображение F множества A в множество B(обозначение: $F: A \to B$). Говорят также, что задана функция F с областью определения A и областью значения B. При этом элемент y называется образом элемента x (обозначение: $y = F(x)$), а элемент x - прообразом элемента y. Отображение $F: A \to B$ называется инъективным, если разным элементам из A ставятся в соответствие разные элементы из B, т.е.

$$F \text{ - инъективно} \Leftrightarrow (x_1 \neq x_2 \Rightarrow F(x_1) \neq F(x_2),\ \forall\, x_1, x_2 \in A)$$

Отображение $F: A \to B$ называется сюръективным, если каждый элемент из B является образом некоторого элемента из A, т.е.

$$F \text{ - сюръективно} \Leftrightarrow (\forall\, y \in B, \exists\, x \in A \,\big|\, F(x) = y)$$

Отображение $F: A \to B$ называется биективным, если оно одновременно инъективно и сюръективно. Пусть $N = \{1, 2, \dots\}$ - множество натуральных чисел и $N_n = \{1, 2, \dots, n\}$ - его начальный отрезок из n элементов. Пусть дано множество A и пусть существует биективное отображение множества A в множество N_n. В этом случае говорим, что мощность множества A равна n или A является n-множеством (обозначение: $|A| = n$).

Два отображения $F_1 : A_1 \to B_1$ и $F_2: A_2 \to B_2$ считаются равными, если $A_1 = A_2$, $B_1 = B_2$ и $F_1(x) = F_2(x)$, $\forall\, x \in A$. Если $A = B$, то отображение $F: A \to B$ называется преобразованием множества A, биективное преобразование F множества A называется его подстановкой. Если $|A| = n$, то говорят, что подстановка множества A имеет степень n.

Если A является n-множеством, причем $A = \{x_1, \dots, x_n\}$, то любое отображение $F: A \to B$ может быть задано в виде двустрочной таблицы

$$F = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ F(x_1) & F(x_2) & \dots & F(x_n) \end{pmatrix}$$

Пусть A - конечное множество из n элементов и F - произвольное отображение множества A в себя.

Справедлива

Теорема 1. Следующие утверждения равносильны:

1) Отображение F - инъективно

2) Отображение F - биективно

3) Отображение F - сюръективно.

♦ Пусть F задано в виде двустрочной таблицы:

$$F: \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ F(x_1) & F(x_2) & \dots & F(x_n) \end{pmatrix}, \text{ причем } A = \{x_1, \dots, x_n\}$$

Пусть l_0 - число элементов множества A, которые отсутствуют в нижней строке табличного задания F, l_1 - число элементов множества A, которые в ней представлены точно 1 раз, l_2 - число элементов, представленных точно 2 раза и т.д.

Имеем следующие отношения:

$$l_0 + l_1 + \dots + l_n = n \qquad \text{а)}$$

$$l_1 + 2l_2 + \dots + nl_n = n \qquad \text{б)}$$

В а) просуммированы все элементы, в б) просуммировано число мест в нижней строке табличного задания F.

Пусть теперь F инъективно, тогда $l_2 = \dots = l_n = 0$ и поэтому из а) и б) имеем $l_0 + l_1 = n$, $l_1 = n$. Значит $l_0 = 0$ и F - сюръективно. Отсюда получаем справедливость $1) \Rightarrow 2) \Rightarrow 3)$.

Пусть F - сюръективно. Тогда $l_0 = 0$. Вычтем из б) соотношение а). Имеем

$$l_2 + 2l_3 + \dots + (n-1)l_n = 0$$

Поскольку все $l_i \geq 0$, то отсюда имеем $l_2 = l_3 = \dots = l_n = 0$ и, следовательно, $l_1 = n$, что означает, что F инъективно, т.е. справедливо $3) \Rightarrow 1)$. ♦

Иногда приходится рассматривать частичные отображения $F: A \to B$, для которых F определено только на элементах подмножества $A_1 \subseteq A$ (и не определено на элементах $A \backslash A_1$). Приведем утверждение, известное как диагональный принцип Кантора, часто используемый для доказательства глубоких утверждений теории множеств.

Теорема 2. Пусть A - некоторое множество, F - отображение (вообще говоря, частичное) из A в его булеан B(A). Пусть A_F - область определения F и пусть

$$K = \{x \mid x \in A_F \text{ и } x \overline{\in} F(x)\}$$

(т.е. K - множество всех элементов A, для которых F определено и которые не принадлежат своему образу при F). Тогда K не есть значение отображения F, т.е. $F(x) \neq K$, $\forall x \in A_F$.

♦ Предположим, что существует $b \in A_F$, такое, что $F(b) = K$. Тогда либо $b \in K$, либо $b \overline{\in} K$. Если, $b \in K$, $K = F(b)$ то b принадлежит своему образу, и по условию на K, элемент b не может принадлежать K - получили противоречие. Пусть $b \overline{\in} K$, $K = F(b)$. Тогда b не принадлежит своему образу и, следовательно, по условию на K, он принадлежит множеству K - снова получили противоречие. Таким образом, K не является значением отображения F. ♦

3. Алгебра множеств.

Зафиксируем непустое множество E и рассмотрим его булеан B(E). Множество B(E) замкнуто относительно операций объединения, пересечения и дополнения множеств - элементов B(E). Множество B(E) вместе с введенными операциями $\cup$, $\cap$, - называется булевой алгеброй подмножеств множества E. Перечислим основные законы, которым подчиняются эти операции:

1. $\overline{\overline{A}} = A$

$$\left.\begin{array}{l} 2.\ A\bigcap B = B\bigcap A \\ 3.\ A\bigcup B = B\bigcup A \end{array}\right\}$$ законы коммутативности

$$\left.\begin{array}{l} 4.\ (A\bigcap B)\bigcap C = A\bigcap (B\bigcap C) \\ 5.\ (A\bigcup B)\bigcup C = A\bigcup (B\bigcup C) \end{array}\right\}$$ законы ассоциативности

$$\left.\begin{array}{l} 6.\ A\bigcap (B\bigcup C) = (A\bigcap B)\bigcup (A\bigcap C) \\ 7.\ A\bigcup (B\bigcap C) = (A\bigcup B)\bigcap (A\bigcup C) \end{array}\right\}$$ законы дистрибутивности

$$\left.\begin{array}{l} 8.\ \overline{A\bigcap B} = \overline{A}\bigcup \overline{B} \\ 9.\ \overline{A\bigcup B} = \overline{A}\bigcap \overline{B} \end{array}\right\}$$ законы дополнения

$$\left.\begin{array}{l} 10.\ A\bigcap A = A \\ 11.\ A\bigcup A = A \end{array}\right\}$$ законы идемпотентности

12. $A\bigcap E = A$

13. $A\bigcup \varnothing = A$

14. $A\bigcup \overline{A} = E$

15. $A\bigcap \overline{A} = \varnothing$

Все данные равенства могут быть доказаны по единой схеме, использующей определение равенства двух множеств A и B:

$A = B \Leftrightarrow A \subseteq B$ и $B \subseteq A$.

В качестве примера приведем доказательство равенства 7.

Пусть $x \in A\bigcup(B\bigcap C)$. Тогда либо $x \in A$, либо $x \in B\bigcap C$. Если $x \in A$, то $x \in A\bigcup B$ и $x \in A\bigcup C$, следовательно, $x \in (A\bigcup B)\bigcap(A\bigcup C)$. Если $x \in B\bigcap C$, то

$X \in B$ и $x \in C$, значит $x \in A \bigcup B$ и $x \in A \bigcup C$. Отсюда, $x \in (A \bigcup B) \bigcap (A \bigcup C)$. Таким образом, установлено включение

$$A \bigcup (B \bigcap C) \subseteq (A \bigcup B) \bigcap (A \bigcup C) \qquad (а)$$

Пусть теперь $x \in (A \bigcup B) \bigcap (A \bigcup C)$. Тогда $x \in A \bigcup B$ и $x \in A \bigcup C$. Если $x \in A$, то $x \in A \bigcup (B \bigcap C)$. Если $x \overline{\in} A$, то тогда должно быть $x \in B$ и $x \in C$. Отсюда следует, что $x \in B \bigcap C$ и, следовательно, $x \in A \bigcup (B \bigcap C)$

Таким образом, установлено включение

$$(A \bigcup B) \bigcap (A \bigcup C) \subseteq A \bigcup (B \bigcap C) \qquad (в)$$

Доказанные включения (а) и (в) равносильны равенству 7.

Доказательства остальных равенств 1 - 15 предлагается проделать самостоятельно.

Мы будем считать допустимыми следующие способы образования множеств:

1. Из множества элементов можно выделить его часть посредством точно сформулированного признака.
2. Если имеется совокупность множеств, то можно получить новое множество, являющееся объединением множеств этой совокупности.
3. Для каждого конечного множества можно образовать множество всех его подмножеств.
4. Для любой пары множеств можно образовать новое множество, являющееся их прямым произведением.

Известно, что неограниченное использование средств при построении множеств приводит к логическим парадоксам (парадокс Рассела, парадокс Кантора и др.).

В данном курсе будут применяться только конструкции конечного типа над конечными множествами.

Упражнения

1. Пусть $A_1, \dots, A_n$, B - подмножества некоторого фиксированного множества E.

Доказать равенства:

a) $(\bigcup\limits_{i=1}^{n} A_i)\bigcap B = \bigcup\limits_{i=1}^{n}(A_i \bigcap B)$

в) $(\bigcap\limits_{i=1}^{n} A_i)\bigcup B = \bigcap\limits_{i=1}^{n}(A_i \bigcup B)$

c) $\overline{\bigcup\limits_{i=1}^{n} A_i} = \bigcap\limits_{i=1}^{n}\overline{A}_i$

d) $\overline{\bigcap\limits_{i=1}^{n} A_i} = \bigcup\limits_{i=1}^{n}\overline{A}_i$

2. Для произвольных множеств A и B положим

$A \oplus B = (A \bigcap \overline{B}) \bigcup (\overline{A} \bigcap B)$

Доказать равенства:

a) $A \oplus B = B \oplus A$

b) $(A \oplus B) \oplus C = A \oplus (B \oplus C)$

c) $A \oplus \varnothing = A$

d) $A \oplus A = \varnothing$

e) $A \bigcap (B \oplus C) = (A \bigcap B) \oplus (A \bigcap C)$

f) $A = B \Leftrightarrow A \oplus B = \varnothing$

3. Доказать равенства:

a) $(A \bigcup B) \times C = (A \times C) \bigcup (B \times C)$

b) $(A \bigcap B) \times C = (A \times C) \bigcap (B \times C)$

c) $(A \bigcap B) \times (C \bigcap D) = (A \times C) \bigcap (B \times D)$

4. Установить биективное соответствие между множеством всех отображений множества A в двухэлементное множество {0, 1} и булеаном множества A.

5. Пусть $F\colon X \to Y$, $A \subseteq X$, $B \subseteq X$

Доказать:

a) $A \subseteq B \Rightarrow F(A) \subseteq F(B)$

b) $F(A \bigcup B) = F(A) \bigcup F(B)$

c) $F(A \bigcap B) \subseteq F(A) \bigcap F(B)$

причем возможно и строгое включение.

d) $F(A \bigcap B) = F(A) \bigcap F(B)$ для любых подмножеств A и B тогда и только тогда, когда F - инъективно.

§ 2. Принципы перечисления и примеры.

Элементарные тождества.

При решении перечисленных задач теории множеств широко используются следующие правила для подсчета.

1. Правило равенства. Если A и B - конечные множества и существует биективное отображение F: A $\to$ B, то $|A| = |B|$

2. Правило суммы. Если $A_1, \dots , A_n$ - конечные, попарно непересекающиеся множества, то

$$|A_1 \bigcup \ldots \bigcup A_n| = |A_1| + \ldots + |A_n|$$

3. Правило произведения. Если $A_1, \dots , A_n$ - конечные множества, то $|A_1 \times \ldots \times A_n| = |A_1| \times \ldots \times |A_n|$.

Применим данные принципы для решения перечисленных задач, связанных с введенными объектами.

1. Число отображения n-множества в m-множество. Пусть $A = \{a_1, \dots , a_n\}$ и $B = \{b_1, \dots , b_m\}$. Тогда любое отображение F: A $\to$ B можно задать набором длины n вида $(F(a_1), \dots , F(a_n))$ элементов из множества B. При этом разные наборы такого вида определяют разные отображения, и разные отображения дают разные наборы. Значит, имеется биективное отображение между множеством всех отображений F: A $\to$ B и множеством $B \times \dots \times B$(n раз). Следовательно, число отображений F: A $\to$ B дается формулой

$$|B|^{|A|} = m^n$$

Если нас интересует число частичных отображений из A в B, то нетрудно заметить, что оно дается формулой

$$(1 + |B|)^{|A|} = (1 + m)^n$$

2. Число инъективных отображений n-множества в m-множество. Любое инъективное отображение F: A $\to$ B однозначно задается набором длины n из элементов множества B вида $(F(a_1), \dots , F(a_n))$, где $F(a_i) \neq F(a_j)$ при $i \neq j$. Элемент $F(a_1)$ может принимать $|B|$ значений, при фиксированном $F(a_1)$ элемент $F(a_2)$ может принимать $|B|$ - 1 значений и т.д. Следовательно, число инъективных отображений F: A $\to$ B равно

$$|B|(|B|-1)\cdots(|B|-|A|+1)=m(m-1)\cdots(m-n+1)$$

<u>Следствие.</u> Число подстановок n-множества A равно $n! = n\times(n-1)\ \dots\ 2\times 1$.

3. <u>Число k-элементных подмножеств n-множества.</u> Пусть $A = \{a_1, \dots , a_n\}$ и требуется найти число подмножеств $B \subseteq A$ с условием $|B| = k$, где $0 \le k \le n$. Обозначим через $\binom{n}{k}$ - искомое число, и пусть $B_1, \dots , B_{\binom{n}{k}}$ - все k-элементные подмножества A. Каждому B_i можно поставить в соответствие k! (по числу биекций B_i на себя) инъективных отображений $F: N_k \to A$, положив $F: \begin{pmatrix} 1 & 2 & \cdots & k \\ a_{i_1} & a_{i_2} & \cdots & a_{i_k} \end{pmatrix}$, где $N_k = \{1, 2, \dots , k\}$, $B_i = \{a_{i_1},\dots,a_{i_k}\}$. Таким образом, всем $\binom{n}{k}$ k-элементным подмножествам A будет поставлено в соответствие $\binom{n}{k} * k!$ инъективных отображений. Ясно, что различные подмножества B_i дают попарно различные инъективные отображения $F: N_k \to A$, и каждое инъективное отображение $F: N_k \to A$ может быть получено указанным образом. Значит, число инъективных отображений $F: N_k \to A$ равно числу $\binom{n}{k} * k!$, т.е.

$$n(n-1)\dots(n-k+1) = \binom{n}{k} * k!$$

Отсюда

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

Условимся считать $0! = 1$ и тогда $\binom{n}{0} = 1$.

Кроме того, полагаем $\binom{n}{k} = 0$ при $k > n$. Тогда функция $f_{n,k} = \binom{n}{k}$ будет определена для всех целых неотрицательных чисел. Числа $\binom{n}{k}$ называются биномиальными коэффициентами.

Учитывая важность формулы (*), приведем еще одно доказательство ее. Будем доказывать формулу (*) индукцией по n + k. Для n + k = 1 имеем очевидное утверждение. Пусть даны n, k и пусть формула (*) верна при всех n', k', таких, что $n' + k' < n + k$.

Фиксируем элемент $a \in A$, где $|A| = n$. Разобьем все k-подмножества множества A на два класса:

1. Те, которые содержат элемент а
2. Те, которые не содержат элемента а.

В случае 1. имеем $\binom{n-1}{k-1}$ подмножеств, и по предположению индукции выполнено

$$\binom{n-1}{k-1} = \frac{(n-1)!}{(k-1)!(n-k)!}$$

В случае 2. имеем $\binom{n-1}{k}$ подмножеств и по предположению индукции выполнено

$$\binom{n-1}{k} = \frac{(n-1)!}{(k!)(n-k-1)!}$$

Таким образом, общее число k-подмножеств (по правилу суммы) равно

$$\binom{n-1}{k+1} + \binom{n-1}{k} = \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-k-1)!} = \frac{(n-1)!}{(k-1)!(n-k-1)!}\left[\frac{1}{n-k} + \frac{1}{k}\right] =$$

$$\frac{n!}{k!(n-k)!} = \binom{n}{k}$$

т.е. формула (*) справедлива и для n + k.

4. <u>Число всех подмножеств n-множества.</u> Пусть A - множество из n элементов и B(A) - булеан множества A. Нас интересует число $|B(A)|$. Рассмотрим множество $\{0,1\}$ и установим биективное соответствие между множеством B(A) и множеством всех отображений $F: A \to \{0,1\}$.

Для произвольного подмножества $A_1 \subseteq A$ определим $F_{A_1} : A \to \{0,1\}$, полагая

$$F_{A_1}(a) = \begin{cases} 1, \text{если } a \in A_1 \\ 0, \text{если } a \overline{\in} A_1 \end{cases}$$

Ясно, что если $A_1 \neq A_2$, то $F_{A_1} \neq F_{A2}$ и любому отображению $F: A \to \{0,1\}$ соответствует $A_1 \subseteq A$, где $A_1 = \{a | a \in A \text{ и } F(a) = 1\}$. Значит, нужное биективное соответствие установлено и, согласно предыдущему, имеется 2^n отображений $F: A \to \{0,1\}$. Отсюда, $|B(A)| = 2^n$.

<u>Следствие.</u> Справедливо тождество

$$\sum_{k=0}^{n}\binom{n}{k} = 2^n$$

5. Мультимножества. В ряде случаев приходится рассматривать объекты, в которых элементы множества повторяются. Известный пример - корни алгебраического уравнения. Определим мультимножество над множеством A как пару (A,r) множества A и отображения $r: A \to N_0 = \{0, 1, \dots \}$, задающего кратность элементов из множества A. Мощностью мультимножества (A,r) называется число $\sum_{a\in A} r(a)$.

1. Число мультимножеств мощности m над n-множеством.

Пусть $A = \{a_1, \dots , a_n\}$. Тогда число мультимножеств мощности m равно числу отображений $r: A \to N_0$ с условием

$$r(a_1) + r(a_2) + \dots + r(a_n) = m$$

Каждому такому отображению r поставим в соответствие набор из элементов 0, 1 вида

$$\bar{r} = (0^{r(a_1)} \quad 1 0^{r(a_2)} \quad 1 \cdots 1 0^{r(a_n)}),$$

где $0^{r(a_i)}$ означает 0, повторенный $r(a_i)$ раз. Набор $\bar{r}$ имеет длину $m + n - 1$и содержит m нулей и $n - 1$ единиц. Ясно, что разным отображениям $r_1 : A \to N_0$, $r_2 : A \to N_0$ соответствуют разные наборы $\bar{r}_1, \bar{r}_2$. Далее, произвольный набор из элементов 0, 1 длины $m + n -1$, содержащий $n - 1$единиц определяет отображение $r: A \to N_0$ с условием $\sum_{a\in A} r(a) = m$, если положить $r(a_1)$ равным числу нулей до первой единицы слева, $r(a_2)$ равным числу нулей между первой и второй единицами слева и т.д. Следовательно, число интересующих отображений $r: A \to N_0$ равно числу наборов из 0, 1 длины $m+ n -1$, содержащих $n - 1$ единиц. Поскольку каждый такой набор однозначно определяется множеством номеров координат, принимающих значение единица, то интересующее нас число равно числу (n-1)-подмножеств (m+n-1)-множества, которое, согласно предыдущему, равно

$$\binom{m+n-1}{n-1}$$

Если нас интересует число невырожденных мультимножеств (A,r) мощности m над n-множеством A, т.е. таких, у которых $r(a) > 0$ для всех $a \in A$, то оно равно

$$\binom{m-1}{n-1}$$

Предоставляется этот факт доказать самостоятельно.

Следствие. Число одночленов $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ полной степени m из кольца многочленов $K[x_1, \dots , x_n]$ равно

$$\binom{m+n-1}{n-1}$$

2. <u>Число перестановок мультимножеств мощности m.</u> Пусть дано мультимножество (A,r), где $A = \{a_1, \dots, a_n\}$ и $r\colon A \to N_0$, причем $\sum_{a\in A} r(a) = m$. Перестановкой мультимножества (A,r) будем называть отображение $F\colon \{1, \dots, m\} \to A$, такое, что

$$\left|F^{-1}(a)\right| = r(a), \quad \forall a \in A.$$

Ясно, что любая перестановка F мультимножества однозначно определяется выбором $r(a_i)$ элементов из $\{1, \dots, m\}$, переходящих в a_i. Это можно сделать числом способом, равным

$$\binom{m}{r(a_1)}\binom{m-r(a_1)}{r(a_2)}\cdots\binom{m-r(a_1)-\cdots-r(a_{n-1})}{r(a_n)} = \frac{m!}{r(a_1)!\cdots r(a_n)!}$$

6. <u>Свойства биномиальных коэффициентов и связанные с ними тождества.</u>

В комбинаторных расчетах биномиальные коэффициенты играют важную роль. Для оперирования с ними полезны следующие формулы.

1. $\binom{n}{k} = \binom{n}{n-k}$ - свойство симметрии

2. $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ - свойство сложения

3. $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$ - свойство понижения индексов

4. $\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}$ - свойство замены индексов

Данные формулы проверяются непосредственной выкладкой.

5. $\binom{r}{0} + \binom{r+1}{1} + \dots + \binom{r+n}{n} = \binom{r+n+1}{n}$

♦ Докажем индукцией по n. При n = 1 тождество верно. Пусть оно верно при n. Тогда для n + 1 имеем

$$\binom{r}{0} + \binom{r+1}{1} + \dots + \binom{r+n}{n} + \binom{r+n+1}{n+1} = \binom{r+n+1}{n} + \binom{r+n+1}{n+1} = \binom{r+n+2}{n+1} \ ♦$$

6. $\binom{0}{m} + \binom{1}{m} + \dots + \binom{n}{m} = \binom{n+1}{m+1}$

♦ Запишем последовательность равенств

$$\binom{n}{m+1}+\binom{n}{m}=\binom{n+1}{m+1}$$

$$\binom{n-1}{m+1}+\binom{n-1}{m}=\binom{n}{m+1}$$

$$\ldots$$

$$\binom{0}{m+1}+\binom{0}{m}=\binom{1}{m+1}$$

Теперь складываем данные равенства, получаем нужное тождество. ♦

7. $$\max_{0\le k\le n}\binom{n}{k}=\binom{n}{\left[\frac{n}{2}\right]}$$

♦ Рассматриваем отношение

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

замечаем, что оно больше 1 при $k \le \left[\frac{n}{2}\right]$ и меньше 1 при $k > \left]\frac{n}{2}\right[$. ♦

8. Пусть p - простое число. Тогда

а) $\binom{p}{k}\equiv 0(\mathrm{mod}\,p)$ при $1 \le k \le p - 1$

б) $\binom{p-1}{k}\equiv(-1)^k(\mathrm{mod}\,p)$ при $0 \le k \le p - 1$

♦ Число $\binom{p}{k}=\frac{p!}{k!(p-k)!}$ целое, числа k! и (p - k)! взаимно просты с p, поэтому они сокращаются с (p - 1)!. Отсюда следует а).

Рассмотрим теперь $\binom{p-1}{k}=\frac{(p-1)!}{k!(p-1-k)!}$. Ясно, что справедливы соотношения $\frac{p-1}{1}\equiv\frac{p-2}{2}\equiv\cdots\equiv\frac{p-k}{k}\equiv-1(\mathrm{mod}\,p)$, откуда следует б) при $k \ge 1$. При $k = 0$ утверждение б) очевидно. ♦

9. Пусть x - некоторое переменное из множества действительных чисел, n - натуральное число. Тогда справедливо

$$(1+x)^n = \sum_{k=0}^{n}\binom{n}{k}x^k$$

Полагая x = 1 и, x = -1, получаем тождества

9а. $\sum_{k=0}^{n}\binom{n}{k} = 2^n$

9б. $\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0$

Рассматривая очевидное тождество

$(1 + x)^n(1 + x)^m = (1 + x)^{n+m}$ (n, m - натуральные числа)

и подсчитывая справа и слева коэффициент при x^k, $0 \le k \le n+m$ получим тождество Вандермонда:

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

Используя тождества 4, 9а, 9б легко доказываются тождества

11а. $\binom{n}{0}\binom{n}{p} + \binom{n}{1}\binom{n-1}{p-1} + \cdots + \binom{n}{p}\binom{n-p}{0} = 2^p\binom{n}{p}$

11б. $\binom{n}{0}\binom{n}{p} - \binom{n}{1}\binom{n-1}{p-1} + \cdots + (-1)^p\binom{n}{p}\binom{n-p}{0} = 0$

12. $\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}\binom{n}{i} = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$

♦ Рассмотрим тождество

$$(1-x)^n = \sum_{i=0}^{n}(-1)^i\binom{n}{i}x^i$$

Перенесем влево член при i = 0 и разделим обе части равенства на x.

$$-\frac{(1-x)^n - 1}{(1-x)-1} = \sum_{i=1}^{n}(-1)^i\binom{n}{i}x^{i-1}$$

Это равносильно тождеству

$$-[1 + (1-x) + (1-x)^2 + \ldots + (1-x)^{n-1}] = \sum_{i=1}^{n}(-1)^i\binom{n}{i}x^{i-1}$$

проинтегрируем обе части по x и получим

$$(1-x) + \frac{(1-x)^2}{2} + \cdots + \frac{(1-x)^n}{n} + C = \sum_{i=1}^{n}\frac{(-1)^i}{i}\binom{n}{i}x^i$$

Полагая x = 0, находим постоянную интегрирования C:

$$C = - [1 + \frac{1}{2} + \cdots + \frac{1}{n}]$$

Теперь полагаем x = 1 и получаем нужное тождество. ♦

Упражнения.

Доказать тождества

1. $\sum\limits_{i=0}^{n}\binom{n}{i}^2=\binom{2n}{n}$

2. $\sum\limits_{k=0}^{n}\frac{1}{k+1}\binom{n}{k}=\frac{1}{n+1}(2^{n+1}-1)$

3. $\sum\limits_{k=0}^{n}(-1)^k\frac{1}{k+1}\binom{n}{k}=\frac{1}{n+1}$

4. $1-\binom{n}{2}+\binom{n}{4}-\binom{n}{6}+\cdots=2^{\frac{n}{2}}\cos\frac{n\pi}{4}$

5. $\binom{n}{1}-\binom{n}{3}+\binom{n}{5}-\binom{n}{7}+\cdots=2^{\frac{n}{2}}\sin\frac{n\pi}{4}$

§ 3. Бинарные отношения.

1. Определения.

Пусть дано декартово произведение множеств $A_1 \times \cdots \times A_n$. Подмножество R $\subseteq A_1 \times \cdots \times A_n$ называется n-местным отношением на множествах $A_1, \dots A_n$. Говорят, что элементы $a_1, \dots a_n$ находятся в отношении R, если $(a_1, \dots a_n) \in R$.

Наиболее изучены и часто используются в приложениях двухместные или бинарные отношения. Иногда бинарные отношения R на $A_1 \times A_2$ называют соответствиями из A_1 в A_2. Для бинарных отношений наряду с записью $(a_1,a_2) \in R$ пишут также a_1Ra_2. Если $A_i = A$, $\forall$ i $\in \overline{1,n}$, то говорят, что задано n-местное отношение на множестве A. Далее будут рассматриваться только бинарные отношения.

Если $R \subseteq A_1 \times A_2$ - бинарное отношение, то можно определить проекции $пр_1R$ и $пр_2R$ как подмножества A_1 и A_2 соответственно:

$$пр_1R = \{a_1 | (a_1, a_2) \in R \text{ для некоторого } a_2 \in A_2\}$$

$$пр_2R = \{a_2 | (a_1, a_2) \in R \text{ для некоторого } a_1 \in A_1\}$$

Если $пр_1R = A_1$, то говорят, что отношение R всюду определено. Если $пр_2R = A_2$, то говорят, что отношение R сюръективно. Для задания бинарных отношения можно использовать любые способы задания множеств. Наиболее употребительные способы задания бинарного отношения R на конечном множестве A - матричный и графический. Пусть n-множество A состоит из элементов $a_1, a_2, \dots a_n$. Тогда для бинарного отношения R на A определим матрицу $D_R = (r_{ij})$, i, j $\in \overline{1,n}$, где

$$r_{ij} = \begin{cases} 1, \text{ если } a_iRa_j \\ 0, \text{ в противном случае.} \end{cases}$$

Матрица D_R однозначно определяет бинарное отношение R. При графическом задании отношения R строится граф с множеством вершин $a_1, \dots a_n$ на плоскости, причем от вершины a_i к вершине a_j проводится ориентированная дуга в том и только в том случае, если a_iRa_j. Построенный таким образом граф однозначно характеризует отношение R.

Легко видеть, что отображения являются частным случаем бинарных отношений. Бинарное отношение R на множестве $A_1 \times A_2$ определяет отображение F: $A_1 \to A_2$, если справедливо

a_1Ra_2 и $a_1'Ra_2 \Rightarrow a_1 = a_1'$.

Иногда говорят, что множество пар $(a_1,a_2) \in R$ задает график отображения F.

2. Операции над отношениями.

Исходя из операций над множествами, можно определить теоретико-множественные операции над отношениями. Для простоты считаем, что бинарные отношения заданы на множестве А. Для бинарных отношений R_1 и R_2 их пересечением (обозначение: $R_1 \bigcap R_2$) называется бинарное отношение, являющееся пересечением соответствующих множеств пар элементов из А, т.е.

$$a_1 (R_1 \bigcap R_2)a_2 \Leftrightarrow a_1R_1a_2 \text{ и } a_1R_2a_2$$

<u>Объединением</u> отношений R_1 и R_2 (обозначение: $R_1 \bigcup R_2$) называется отношение, являющееся объединением соответствующих множеств пар элементов из А, т.е.

$$a_1 (R_1 \bigcup R_2)a_2 \Leftrightarrow a_1R_1a_2 \text{ или } a_1R_2a_2$$

Очевидным образом определяется отношение включения для бинарных отношений, пишем $R_1 \subseteq R_2$, если множество пар элементов из А для отношения R_1 содержится в множестве пар для отношения R_2 .

<u>Дополнением</u> отношения R называется отношение $\overline{R}$, определяемое условием: $a_1 \overline{R} a_2 \Leftrightarrow (a_1a_2) \overline{\in} R$. Определим теперь алгебраические операции на бинарных отношениях. Если R - отношение на А, то обратное отношение R^{-1} определяется условием:

$$a_1R^{-1}a_2 \Leftrightarrow a_2Ra_1.$$

Если R_1, R_2 - отношения на А, то их произведение $R_1 * R_2$ определяется условием:

$$a_1(R_1 * R_2)a_2 \Leftrightarrow \exists\, b\in A \mid a_1R_1b \text{ и } bR_2a_2.$$

<u>Транзитивное замыкание</u> $\check{R}$ отношения R определяется так:

$$a_1 \check{R} a_2 \Leftrightarrow \exists\, (z_0 = a_1, z_1, \dots , z_{n-1}, z_n = a_2) \in A^{n+1} \mid z_0Rz_1, \dots , z_{n-1}Rz_n$$

Легко видеть, что $a_1 \check{R} a_2 \Leftrightarrow \exists\, n \mid a_1R^na_2$

Таким образом, $\check{R} = R \bigcup R^2 \bigcup R^3 \bigcup \cdots$

Выясним теперь, как введенные операции над бинарными отношениями выразить с помощью операций на соответствующими им матрицами. Поскольку матрицы отношений состоят из элементов 0, 1, то введем операции умножения (·) и сложения (v) на множестве {0, 1} с помощью таблиц:

.	0	1
0	0	0
1	0	1

v	0	1
0	0	1
1	1	1

Теперь определим операции над матрицами, соответствующие операциям над отношениями. Пусть отношениям R_1 и R_2 на множестве A = {$a_1, \dots, a_n$} соответствуют матрицы $D_{R_1} = (r^1_{ij})$ и $D_{R_2} = (r^2_{ij})$, $i, j \in \overline{1, n}$. Тогда отношению $R_1 \bigcap R_2$ соответствует матрица $D_R = (c_{ij})$, где $c_{ij} = r^1_{ij} \cdot r^2_{ij}, \quad i, j \in \overline{1, n}$.

Отношению $R_1 \bigcup R_2$ соответствует матрица $D_R = (d_{ij})$, где $d_{ij} = r^1_{ij} \vee r^2_{ij}, \quad i, j \in \overline{1, n}$

Отношению $\overline{R}_1$ соответствует матрица $D_R = (f_{ij})$, где $f_{ij} = \overline{r}^1_{ij}, \quad i, j \in \overline{1, n}$

причем $\overline{r}^1_{ij} = \begin{cases} 0, \text{если } r^1_{ij} = 1 \\ 1, \text{если } r^1_{ij} = 0 \end{cases}$

Отношению R_1^{-1} соответствует матрица $D^T_{R_1}$ - транспонированная к матрице D_{R_1} .

Произведению отношений $R_1 \cdot R_2$ соответствует матрица $D_R = (g_{ij})$, где

$$g_{ij} = r^1_{i1} \cdot r^2_{1j} \vee r^1_{i2} \cdot r^2_{2j} \vee \cdots \vee r^1_{in} \cdot r^2_{nj}, \quad i, j \in \overline{1, n}.$$

Действительно, пусть $a_i(R_1R_2)a_j$. Тогда существует a_k, такое, что $a_iR_1a_k$ и $a_kR_2a_j$. Значит, $r^1_{ik} = 1, r^2_{kj} = 1.$. Отсюда $r^1_{ik} \cdot r^2_{kj} = 1$ и тогда $g_{ij} = 1$. Обратно, пусть $g_{ij} = 1$. Тогда среди слагаемых в выражении для g_{ij} хотя бы одно равно 1. Пусть $r^1_{it} \cdot r^2_{tj} = 1$. Отсюда $r^1_{it} = 1$ и $r^2_{tj} = 1.$ По определению матриц $D_{R_1} = (r^1_{ij})$ и $D_{R_2} = (r^2_{ij})$ имеем $a_iR_1a_t$ и $a_tR_2a_j$. Отсюда следует $a_i(R_iR_2)a_j$ и поэтому матрица $D_R = (g_{ij})$ задает отношение $R_1 \cdot R_2$. Матрица для транзитивного замыкания $\overset{\vee}{R}$ вычисляется через операции суммы и степени матрицы D_R :

$$D_{\overset{\vee}{R}} = D_R \vee D_{R^2} \vee D_{R^3} \vee \cdots$$

В качестве упражнение предоставляется установить связь между операциями над отношениями и их графическими представлениями.

3. Свойства операций над отношениями.

Поскольку операции пересечения, объединения, дополнения отношения соответствуют теоретико-множественным операциям, то они обладают теми же свойствами. Рассмотрим теперь алгебраические операции.

1. <u>Свойство обращения:</u> $\left(R^{-1}\right)^{-1} = R$.

♦Имеем $a_1 \left(R^{-1}\right)^{-1} a_2 \quad \Leftrightarrow \quad a_2\, R^{-1}\, a_1 \quad \Leftrightarrow \quad a_1\, R\, a_2$ ♦

2. <u>Ассоциативный закон:</u> $(R_1 \cdot R_2) \cdot R_3 = R_1 \cdot (R_2 \cdot R_3)$

♦ Если $a_1(R_1 \cdot R_2) \cdot R_3a_2$, то существует $z \in A$, такое, что $a_1(R_1 \cdot R_2)z$, zR_3a_2 Далее $a_1(R_1 \cdot R_2)$ влечет существование $w \in A$ такое, что a_1R_1w и wR_2z . Из wR_2z и zR_3a_2 следует $w(R_2 \cdot R_3)a_2$, а из a_1R_1w и $w(R_2 \cdot R_3)a_2$ следует $a_1R_1(R_2 \cdot R_3)a_2$. Обратно, если $a_1R_1(R_2 \cdot R_3) \cdot R_3a_2$, то существует $w \in A$, такое, что a_1R_1w и $w(R_2 \cdot R_3)a_2$. Далее $w(R_2 \cdot R_3)a_2$ влечет существование $z \in A$, такого, что wR_2z и zR_3a_2. Теперь, из a_1R_1w и wR_2z имеем $a_1(R_1 \cdot R_2)z$, и учитывая справедливость zR_3a_2,

получаем $a_1(R_1 \cdot R_2) \cdot R_3a_2$. ♦

3. <u>Правило обращения произведения:</u> $(R_1{\cdot}R_2)^{-1} = R_2^{-1} \cdot R_1^{-1}$

♦ Если $a_1\, (R_1{\cdot}R_2)^{-1}a_2$, то $a_2\, (R_1{\cdot}R_2)a_1$. Значит, существует $z \in A$, такое, что a_2R_1z и zR_2a_1. Следовательно, имеем $a_1\, R_2^{-1} z$ и $z\, R_1^{-1} a_2$, откуда $a_1(R_2^{-1} \cdot R_1^{-1})\, a_2$. Обратно, если $a_1(R_2^{-1} \cdot R_1^{-1})\, a_2$, то существует $z \in A$, такое, что $a_1\, R_2^{-1} z$ и $z\, R_1^{-1} a_2$, откуда имеем a_2R_1z и zR_2a_1. Поэтому $a_2\, (R_1{\cdot}R_2)a_1$ и, следовательно, $a_1\, (R_1{\cdot}R_2)^{-1}a_2$.♦

4. <u>Дистрибутивный закон:</u>

а) $(R_1 \bigcup R_2) \cdot R_3 = (R_1 \cdot R_3) \bigcup (R_2 \cdot R_3)$

в) $R_3 (R_1 \bigcup R_2) = (R_3 \cdot R_1) \bigcup (R_3 \cdot R_2)$

Докажем а). Если $a_1(R_1 \bigcup R_2)\, R_3a_2$, то существует $z \in A$, такое, что $a_1(R_1 \bigcup R_2)\, z$ и zR_3a_2. Но $a_1(R_1 \bigcup R_2)\, z$ означает, что либо a_1R_1z , либо a_1R_2z. Поэтому имеем либо $a_1R_1R_3a_2$, либо $a_1R_2R_3a_2$ и, следовательно, $a_1(R_1 \cdot R_3 \bigcup R_2 \cdot R_3)\, a_2$. Обратно, если $a_1(R_1 \cdot R_3 \bigcup R_2 \cdot R_3)\, a_2$, то либо $a_1R_1R_3a_2$, либо $a_1R_2R_3a_2$. В первом случае существует $z \in A$, такое, что a_1R_1z и zR_3a_2. Но $a_1R_1z \Rightarrow a_1(R_1 \bigcup R_2)\, z$ и поэтому снова получаем

$a_1(R_1 \bigcup R_2)\,R_3a_2$. Во втором случае существует $w \in A$ такое, что a_1R_2w и wR_3a_2 . Далее $a_1R_2w \Rightarrow a_1(R_1 \bigcup R_2)\,w$ и поэтому получаем $a_1(R_1 \bigcup R_2)\,R_3a_2$, что и доказывает равенство а). ♦

Равенство в) доказывается аналогично.

Другой дистрибутивный закон записывается в виде отношения включения:

c) $(R_1 \bigcap R_2) \cdot R_3 \subseteq (R_1 \cdot R_3) \bigcap (R_2 \cdot R_3)$

d) $R_3(R_1 \bigcap R_2) \subseteq R_3 \cdot R_1 \bigcap R_3 \cdot R_2$

Данные соотношения доказываются аналогично. Заметим, что здесь нельзя заменить отношение включения равенством. В качестве упражнения предоставляется доказать следующие свойства отношений:

6. $(R_1 \bigcup R_2)^{-1} = R_1^{-1} \bigcup R_2^{-1}$

7. $(R_1 \bigcap R_2)^{-1} = R_1^{-1} \bigcap R_2^{-1}$

8. $R_1 \subseteq R_2 \Rightarrow R_1^{-1} \subseteq R_2^{-1}$

9. $R_1 \subseteq R_2 \Rightarrow R_1 \cdot R \subseteq R_2 \cdot R$ и $R \cdot R_1 \subseteq R \cdot R_2, \quad \forall R$

10. $R_1 \subseteq R_2 \Rightarrow \check{R}_1 \subseteq \check{R}_2$

11. $\check{\check{R}} = \check{R}$

Упражнения.

1. Доказать, что $\overline{R^{-1}} = (\overline{R})^{-1}$ для любого бинарного отношения R.

2. Доказать, что если $R_1 \subseteq R_2$, то

а. $R_1^{-1} \subseteq R_2^{-1}$

б. $\check{R}_1 \subseteq \check{R}_2$

3. Пусть A - конечное множество из n элементов. Найти число бинарных отношений на множестве A.

§ 4. Специальные классы бинарных отношений.

1. Отношения эквивалентности.

Бинарное отношение R на множестве A называется рефлексивным, если справедливо aRa, $\forall a \in A$. Рефлексивные отношения представляются матрицами, у которых на главной диагонали стоят единицы.

Отношение R называется симметричным, если для любых $a_1,a_2 \in A$ из a_1Ra_2 следует a_2Ra_1 . Симметричные отношения R представляются симметричными матрицами $D_R = (r_{ij})$, т.е. матрицами с условием $r_{ij} = r_{ji}$, $\forall i, j \in \overline{1, n}$.

Отношение R называется транзитивным, если для любых $a_1,a_2,a_3 \in A$ из a_1Ra_2 и a_2Ra_3 следует a_1Ra_3. Свойство транзитивности отношения R хорошо интерпретируется на графе, изображающем отношение R. Именно, если из вершины a_1 имеется дуга в вершину a_2, а из вершины a_2 имеется дуга в вершину a_3, то имеется также дуга из вершины a_1 в вершину a_3. Бинарное отношение R на множестве A называется отношением эквивалентности или просто эквивалентностью, если оно рефлексивно, симметрично и транзитивно. Данное определение отвечает интуитивному понятию одинаковости или неразличимости предметов. Пусть R - отношение эквивалентности на множестве A. Определим класс эквивалентности, содержащий элемент $a \in A$ (обозначение: R[a]), как множество элементов из A, находящихся в отношении R с элементом a, т.е.

$$R[a] = \{x \mid x \in A \text{ и } xRa\}$$

Теорема 1. Отношение эквивалентности R разбивает множество A на попарно непересекающиеся классы эквивалентных элементов таким образом, что каждый элемент A принадлежит точно одному классу эквивалентности.

♦ Покажем, что если два класса эквивалентности содержат общий элемент, то они совпадают. Пусть $z \in R[a_1]$ и $z \in R[a_2]$. Тогда справедливо zRa_1 и zRa_2. По симметричности отношения R имеем a_1Rz, а по транзитивности R из a_1Rz, zRa_2 следует a_1Ra_2. Следовательно, $a_1 \in R[a_2]$. Аналогично имеем $a_2 \in R[a_1]$. Отсюда получаем, $R[a_1] \subseteq R[a_2]$, поскольку $xRa_1, a_1Ra_2 \Rightarrow xRa_2$ и аналогично заключаем $R[a_2] \subseteq R[a_1]$. Следовательно, $R[a_1] = R[a_2]$. Отсюда следует, что каждый элемент A находится не более, чем в одном классе эквивалентности. Поскольку из рефлексивности R следует $a \in R[a]$, $\forall a \in A$, то значит каждый элемент $a \in A$ находится по крайней мере в одном классе эквивалентности. ♦

Если R - отношение эквивалентности, то число классов эквивалентности называется рангом отношения R.

Пример. Рассмотрим множество целых чисел Z. Зафиксируем натуральное число n и определим отношение R_n на Z. $xR_ny \Leftrightarrow$ x - y делится на число n (обозначение: $x \equiv y(\mathrm{mod}\ n)$). Легко проверяется, что отношение R_n есть отношение эквивалентности. Класс эквивалентности [a] будет состоять из всех целых чисел вида $a + kn$, $k \in Z$. Поэтому, [0], [1], … , [n - 1] - различные классы эквивалентности. Других классов нет, так как любое число a может быть записано в виде $a = nq + r$, где $0 \le r < n$ и поэтому $a \in [r]$. Ранг отношения R_n равен n. Класс [a] называется классом вычетов по модулю n.

Пусть A - произвольное множество. Говорят, что семейство множеств $X = (X_i)$, $i \in S$, где S - множество индексов, $X_i \subseteq A$ образует разбиение множества A, если выполнены условия:

1. $\bigcup\limits_{i \in S} X_i = A$

2. $X_i \bigcap X_j = \varnothing$ при $i \ne j$, $i, j \in S$.

Справедливо обращение предыдущей теоремы.

Теорема 2. Пусть $X = (X_i)$, $i \in S$ - разбиение множества A. Пусть R - бинарное отношение на A, определенное условием:

$$a_1Ra_2 \Leftrightarrow \exists i \in S \mid a_1, a_2 \in X_i$$

Тогда отношение R есть отношение эквивалентности.

♦ Ясно, что R - рефлексивное отношение, поскольку по условию каждое $a \in A$ находится в некотором X_i . Симметричность R следует из определения. Осталось проверить транзитивность R. Пусть имеем a_1Ra_2 и a_2Ra_3. Значит, по определению, существуют $i_1, i_2 \in S$ такие, что $a_1, a_2 \in X_{i_1}$ и $a_2, a_3 \in X_{i_2}$. Из условий $a_2 \in X_{i_1}$ и $a_2 \in X_{i_2}$ по свойству разбиения имеем $i_1 = i_2$, и тогда a_1, a_3 лежат в одном множестве X_{i_1}, поэтому имеем a_1Ra_3, что и доказывает транзитивность R. ♦

Рассмотрим теперь, какие операции над отношениями эквивалентности дают в результате отношение эквивалентности. Легко доказать следующие утверждения:

1. Если R - отношение эквивалентности, то R^{-1} - также отношение эквивалентности.

2. Если R_1, R_2 - отношения эквивалентности, то $R_1 \bigcap R_2$ - также отношение эквивалентности.

Заметим, что вообще говоря, объединение отношений эквивалентности не является отношением эквивалентности.

Справедлива следующая

Теорема 3. Объединение $R_1 \bigcup R_2$ отношений эквивалентности R_1 и R_2 является отношением эквивалентности в том и только в том случае, когда выполняется условие $R_1 \cdot R_2 = R_1 \bigcup R_2$

Произведение отношений эквивалентности также, вообще говоря, не является отношением эквивалентности. Аналогично может быть доказана

Теорема 4. Произведение $R_1 \cdot R_2$ отношения эквивалентности R_1 и R_2 является отношением эквивалентности в том и только в том случае, когда выполняется условие $R_1 \cdot R_2 = R_2 \cdot R_1$.

2. Отношения толерантности.

Бинарное отношение R на множестве A называется отношением толерантности, если оно рефлексивно и симметрично. Данное определение отвечает интуитивному представлению о сходстве или похожести предметов. Множество A вместе с заданным на нем отношением толерантности называют также пространством толерантности (обозначение: (A,R)).

Пример. Пусть H - произвольное множество, $B_1(H)$ - множество непустых подмножеств множества H. Определим отношение R на элементах множества $B_1(H)$ условием

$$xRy \Leftrightarrow x \bigcap y \neq \varnothing, \quad x, y \in B_1(H)$$

Симметричность и рефлексивность данного отношения R очевидны, и поэтому оно будет отношением толерантности.

Пример. Пусть H_1, H_2 - произвольные множества. Обозначим через $M(H_1,H_2)$ - множество всех отображений $F : H_1 \rightarrow H_2$. Определим на множестве $M(H_1,H_2)$ отношение R условием

$$F_1RF_2 \Leftrightarrow \exists\, h \in H \mid F_1(h) = F_2(h)$$

Симметричность и рефлексивность данного отношения R также очевидны, и поэтому оно будет отношением толерантности. Над отношениями толерантности можно производить обычные операции. Нетрудно установить, что если T_1, T_2 - отношения толерантности, то отношениями толерантности также будут следующие отношения:

$$T_1\bigcup T_2,\quad T_1\bigcap T_2,\quad T_1^{-1},\quad \check{T}_1$$

Произведение отношений толерантности, вообще говоря, не будет отношением толерантности. Может быть доказана

Теорема 5. Для того, чтобы произведение $T_1 \cdot T_2$ отношений толерантности T_1, T_2 было отношением толерантности, необходимо и достаточно, чтобы выполнялось условие:

$$T_1 \cdot T_2 = T_2 \cdot T_1$$

3. Отношения частичного порядка.

Бинарное отношение R на множестве A называется антисимметричным, если справедливо свойство: aRb, bRa $\Rightarrow$ a = b. Отношение R называется отношением частичного порядка, если оно рефлексивно, антисимметрично и транзитивно. Множество A вместе с заданным на нем отношением частичного порядка R называется частично упорядоченным множеством. Для обозначения отношения частичного порядка будет также использоваться знак $\le$.

Пример 1. Пусть B(A) - булеан множества A. Тогда отношение теоретико-множественного включения $\le$ задает на B(A) отношение частичного порядка.

Пример 2. Пусть $E_m = \{0, 1, \dots , m\}$ и пусть $\le$ - обычное отношение сравнимости для целых чисел. Рассмотрим множество $E_m^n = E_m \times \dots \times E_m$ (n раз) и определим отношение частичного порядка на E_m^n, обозначаемое также $\le$, с помощью условия:

$$(x_1, \dots , x_n) \le (y_1, \dots , y_n) \iff x_i \le y_i, \quad \forall\ i \in \overline{1, n}$$

в смысле сравнимости элементов E_m, $x_i, y_i \in E_m$, $i \in \overline{1, n}$.

Легко проверяется, что введенное отношение есть отношение частичного порядка. При m = 1 мы получаем единичный n-мерный куб, (обозначение: E^n), представляющий собой множество двоичных набором длины n из элементов 0, 1.

Весом набора $\alpha = (\alpha_1, \dots , \alpha_n)$ (обозначение - $\|\alpha\|$) называется число единичных координат. Заметим, что булеан B(A) n-элементного множества $A = \{a_1, \dots , a_n\}$ однозначно представляется единичным n-мерным кубом E^n :

$$X \subseteq B(A) \iff \alpha_X = (\alpha_1, \dots , \alpha_n)$$

где

$$\alpha_i = \begin{cases} 1, \text{ если } a_i \in X \\ 0, \text{ в противном случае.} \end{cases}$$

Данное соответствие определяет изоморфизм двух частично упорядоченных множеств $\langle B(A), \subseteq \rangle$ и $\langle E^n, \leq \rangle$. Элементы a, b частично упорядоченного множества (A, ≤) называются сравнимыми, если $b \leq a$ или $a \leq b$, в противном случае - несравнимыми. Частичный порядок называется линейным порядком (также - цепь), если любые два элемента сравнимы. Произвольное множество элементов частично упорядоченного множества называется антицепью, если любые два его элемента не сравнимы. Примером линейного порядка является лексикографический порядок слов. Пусть дан алфавит A с зафиксированным на нем порядком букв. Рассмотрим множество A* слов (т.е. последовательностей букв из алфавита A конечной длины). Определим линейный порядок на A* (обозначение: $\propto$) следующим образом:

1. На словах, состоящих из одной буквы, отношение $\propto$ совпадает с порядком букв в алфавите A.

2. Для произвольных двух слов $s_1 = a_{11}a_{12} \ldots a_{1m}$ и $s_2 = a_{21}a_{22} \ldots a_{2n}$ в алфавите A полагаем $s_1 \propto s_2 \Leftrightarrow$ выполнено одно из условий:

   1. $s_1 = pa_iq_1$, $s_2 = pa_jq_2$ и $a_i \propto a_j$. Здесь p, q_1, q_2 - некоторые слова (возможно пустые), $a_i, a_j \in A$.

   2. $s_2 = s_1p$, где p - непустое слово.

Легко проверяется, что данное отношение есть отношение линейного порядка. Наиболее известным примером лексикографического упорядочения является упорядочение слов в словарях.

Замечание. Если рассматривать числа в позиционных системах счисления (например, в двоичной или десятичной) как слова в алфавите цифр, то их лексикографическое упорядочение совпадает с обычным, если рассматриваемые числа имеют одинаковое число разрядов. В общем виде эти два упорядочения могут не совпадать. Например,

$$10 < 1088 \text{ и } 10 \propto 1088, \text{ но } 20 < 1088 \text{ и } 1088 \propto 20.$$

Для того, чтобы оба вида упорядочения совпадали, нужно выравнять число разрядов у всех сравниваемых чисел, приписав слева нули. В данном примере получим $0020 \propto 1088$. Такое выравнивание автоматически происходит при записи целых чисел в ЭВМ.

Над отношениями частичного порядка можно производить обычные операции. Нетрудно установить, что если R_1, R_2 - отношения частичного порядка, то отношения R_1^{-1}, $R_1 \bigcap R_2$ есть отношения частичного порядка. Объединение отношений частичного порядка, вообще говоря, не является отношением частичного порядка. Может быть доказана

Теорема 6. Объединение $R_1 \bigcup R_2$ отношения частичного порядка является отношением частичного порядка тогда и только тогда, когда справедливо включение $R_1 \cdot R_2 \bigcup R_2 \cdot R_1 \subseteq R_1 \bigcup R_2$

4. Приведем теперь количественные соотношения, связанные с введенными бинарными отношениями. Пусть A - множество из n элементов.

1. Число бинарных отношений на множестве A равно 2^{n^2}.

2. Число рефлексивных отношений на множестве A равно 2^{n^2-n}.

3. Число симметричных отношений на множестве A равно $2^{n(n+1)\frac{1}{2}}$.

4. Число отношений толерантности на множестве A равно $2^{n(n-1)\frac{1}{2}}$.

Эти факты легко следуют из матричного представления отношения R.

Справедлива

Теорема 7. Пусть p_n - число отношения n-эквивалентности на n-элементном множестве. Тогда справедлива формула

$$p_{n+1} = \sum_{i=0}^{n} \binom{n}{i} p_i \text{ , } p_0 = 1$$

♦ Зафиксируем некоторый элемент $a \in A$, где $|A| = n + 1$. Тогда для произвольного отношения эквивалентности элемент a будет находиться в классе эквивалентности вместе с i другими элементами, где i = 0, 1, … , n. Подмножество из i элементов может быть выбрано $\binom{n}{i}$ способами. Оставшиеся n - i элементов разбиваются на классы эквивалентности p_{n-i} способами - по числу отношений эквивалентности. Применяя правило суммы и произведения, получим

$$p_{n+1} = \sum_{i=0}^{n} \binom{n}{i} p_{n-i} = \sum_{i=0}^{n} \binom{n}{i} p_i \text{ ,}$$

что и требовалось. ♦

Приведем таблицу нескольких первых значений функций p_n.

n	0	1	2	3	4	5	6	7	8	9
p_n	1	1	2	5	15	52	203	877	4140	21147

Числа p_n называются числами Белла. Обозначим p_{nk} - число отношений эквивалентности ранга k на n-элементном множестве.

Теорема 8. Для чисел p_{nk} справедливо соотношение

$$p_{nk} = p_{n-1,k-1} + k\, p_{n-1,k}$$

$$p_{00} = 1,\ p_{10} = 0$$

Пусть $A = \{a_1, \dots , a_n\}$. Все множество отношений эквивалентности ранга k на A разобьем на два класса. Класс 1 составляют те отношения, в которых элемент a_n образует класс $[a_n] = \{a_n\}$, состоящий из одного элемента. Класс 2 составляют все остальные отношения эквивалентности ранга k. Ясно, что число элементов в классе 1 равно $p_{n-1,k-1}$ - по числу отношений эквивалентности ранга k - 1на (n - 1)-множестве $A\setminus \{a_n\}$. Далее, число элементов в классе 2 равно $k\, p_{n-1,k}$, поскольку любое разбиение $A\setminus \{a_n\}$ на k непустых частей дает k разбиений A на k непустых частей путем добавления k способами элемента a_n в одну из частей. Обратно, каждое разбиение $A\setminus\{a_n\}$ на k непустых частей может быть получено из k разбиений A на k частей из класса 2 удалением элемента a_n . Применяя правило суммы, получаем утверждение. ♦

Комбинаторные числа p_{nk} называются числами Стирлинга 2-го рода. Применяя полученное соотношение, можно построить следующую таблицу для чисел p_{nk}

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

Упражнения.

1. Доказать, что на множестве из n элементов имеется $2^{n-1} - 1$ отношений эквивалентности ранга 2.

2. Доказать, что на множестве из n элементов имеется $\dfrac{3^{n-1}+1}{2} + 2^{n-1}$ отношений эквивалентности ранга 3.

3. Показать, что всякое подмножество E_n (множество двоичных наборов длины n), содержащее не менее n + 2 набора, содержит пару несравнимых наборов.

4. Доказать, что для любого набора $x \in E_n$, содержащего k единиц ($0 \le k \le n$), имеется $2^k + 2^{n-k} - 1$ сравнимых с ним наборов.

5. Для множества E_5 указать покрытие, состоящее из минимального числа цепей.

§ 5. Элементы теории подстановок.

1. Подстановки были введены в § 1. Они играют большую роль в дискретной математике, поэтому мы займемся изучением их элементарных свойств. Пусть дано множество $N_n = \{1, 2, \dots , n\}$. Тогда любая подстановка F множества N_n представляется в виде таблицы

$$F: \begin{pmatrix} 1 & 2 & \cdots & n \\ F(1), & F(2), & \cdots & F(n) \end{pmatrix}$$

При этом число названо степенью подстановки F. Определим подстановку E множества N_n условием:

$$E(i) = i, \quad i \in N_n.$$

Такая подстановка называется тождественной или единичной. Определим теперь умножение подстановок как результат последовательного выполнения соответствующих биективных отображений. Ясно, что результирующее отображение при этом будет биективным. Если взять подстановку G, определяемую таблицей:

$$G: \begin{pmatrix} 1 & 2 & \cdots & n \\ G(1), & G(2), & \cdots & G(n) \end{pmatrix}$$

то по определению полагаем

$$F\bullet G = \begin{pmatrix} 1 & 2 & \cdots & n \\ F(G(1)), & F(G(2)), & \cdots & F(G(n)) \end{pmatrix}$$

Например, пусть $F = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1, & 4 & 2 \end{pmatrix}$, $G = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$, то

$$F\bullet G = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

Ясно, что для тождественной подстановки E выполнено $E\bullet F = F\bullet E = F$ для любой подстановки F.

Легко видеть, что, вообще говоря, $F\bullet G \neq G\bullet F$

Умножение подстановок ассоциативно, т.е. для любых подстановок F, G, H выполнено

$$F\bullet(G\bullet H) = (F\bullet G)\bullet H$$

Это следует из доказанного выше утверждения об ассоциативности умножения бинарных отношений.

Для произвольной подстановки F определим обратную подстановку F^{-1}, для которой справедливо $F^{-1} \bullet F = F \bullet F^{-1} = E$

Обратной к подстановке F, где

$$F = \begin{pmatrix} 1 & 2 & \cdots & n \\ F(1), & F(2), & \cdots & F(n) \end{pmatrix}$$

является подстановка

$$F^{-1} = \begin{pmatrix} F(1) & F(2) & \cdots & F(n) \\ 1 & 2 & \cdots & n \end{pmatrix}$$

которая определяется корректно, т.к. в строке $F(1), F(2), \dots, F(n)$ все элементы различны и представлены точно 1 раз.

Таким образом, множество подстановок конечного множества N_n удовлетворяет аксиомам группы, определение которой известно из курса Алгебры. Множество всех подстановок множества N_n называется симметрической группой множества N_n и обозначается $S(N_n)$. Ясно, что число подстановок в группе $S(N_n)$, называемое порядком группы $S(N_n)$, равно n!

2. Для подстановок часто используется запись в виде произведения независимых циклов. Пусть P - некоторая подстановка множества N_n. Фиксируем некоторый элемент $a_1 \in N_n$ и рассмотрим элемент $P(a_1)$.

Если $P(a_1) = a$, то говорим, что элемент a_1 образует цикл длины 1, и обозначим его (a_1) .

Если $P(a_1) \neq a_1$, то образуем последовательность

$$a_1, a_2, a_3, \dots, \quad \text{где } a_2 = P(a_1), a_3 = P(a_2) \quad \text{и т.д.}$$

Поскольку множество N_n конечно, то в данной последовательности найдутся повторения. Пусть a_{t+1} - первый повторившийся элемент, т.е. $a_{t+1} = a_k$, $k \le t+1$ Тогда выполнено $a_{t+1} = a_1$. Если, напротив, $a_{t+1} = a_i$ для $i \ge 2$, то тогда имеем $P(a_{i-1}) = a_i$, $P(a_t) = a_i$ и в силу биективности P получаем $a_{i-1} = a_t$, что противоречит тому, что a_{t+1} - первое повторение. В последовательности $a_1, a_2, \dots, a_t$ все элементы различны. Данная последовательность называется циклом длины t и обозначается $(a_1, \dots, a_t)$. Теперь любая подстановка P может быть записана в виде произведения независимых циклов с помощью следующей процедуры:

- начинаем с любого элемента $a_1 \in N_n$ и выписываем цикл, содержащий a_1. Если этот цикл содержит все элементы N_n , то останавливаемся. Если нет, то удаляем из N_n элементы построенного цикла и повторяем процедуру.

Полученное представление подстановки называется цикловой записью подстановки. Например, пусть дана подстановка

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 1 & 3 & 8 & 6 & 5 & 9 & 2 & 4 \end{pmatrix}$$

Тогда ее цикловое разложение имеет вид

$$(1\ 7\ 9\ 4\ 8\ 2)\ (3)\ (5\ 6\ )$$

Ясно, что цикловое представление однозначно определяет подстановку. Подстановке соответствует цикловое представление с точностью до порядка следования циклов.

Если подстановка в цикловом представлении содержит один цикл, то она называется <u>полноцикловой.</u> Если подстановка степени n имеет в цикловом представлении k_i циклов длины i, $i \in \overline{1,n}$, то система чисел $(k_1, k_2, \dots , k_n)$ называется цикловой структурой подстановки и обозначается $\left[1^{k_1}\ 2^{k_2}\ \dots n^{k_n}\right]$. Ясно, что выполнено соотношение $1k_1 + 2k_2 + \dots + nk_n = n$

Покажем, что число полноцикловых подстановок степени n равно (n - 1)!

♦ Действительно, любая полноцикловая подстановка степени имеет цикловую запись $(1, i_2, \dots , i_n)$, где $i_2, \dots , i_n$ - различные элементы множества $\{2, \dots , n\}$. Число наборов $i_2, \dots , i_n$ равно (n - 1)!, и разные такие наборы опреде- ляют разные подстановки. ♦

Можно доказать, что число подстановок степени n с цикловой структурой $\left[1^{k_1}\ 2^{k_2}\ \dots n^{k_n}\right]$ выражается формулой

$$\frac{n!}{1^{k_1} \cdot k_1!\, 2^{k_2} \cdot k_2! \cdots n^{k_n} \cdot k_n!}$$

Пусть подстановка P имеет цикловое представление:

$$(a_{11}\ a_{12} \dots\ a_{1t_1})\ (a_{21}\ a_{22} \dots\ a_{2t_2})\ \dots\ (a_{s1}\ a_{s2} \dots\ a_{st_s})$$

Тогда подстановка P^{-1} имеет цикловое представление:

$$(a_{st_s} \dots a_{s2}\ a_{s1}) \dots (a_{2t_2}\ \dots a_{22}\ a_{21})\ (a_{1t_1}\ \dots a_{12}\ a_{11})$$

Данное утверждение проверяется непосредственным вычислением.

3. Зафиксируем некоторую подстановку F и определим последовательность подстановок

$$F, F^2, F^3, \dots$$

здесь $F^k = \underbrace{F\circ\cdots\circ F}_{k\,раз}$

В силу конечности числа подстановок существуют натуральные k, ℓ ($k > \ell$), для которых выполнено

$$F^k = F^{\ell}$$

Отсюда следует $F^{\ell - k} = E$, $k - \ell > 0$.
Значит, для любой подстановки F существует натуральное числор, такое, что $F^p = E$.
Наименьшее из таких натуральных чисел называется порядком подстановки F.

<u>Теорема.</u> Порядок подстановки равен наименьшему общему кратному длин ее циклов.

♦ Всякому циклу z соответствует подстановка $\check{z}$ в которой элементы, не входящие в цикл, остаются на месте.
Если z_1, z_2 - два цикла, не имеющие общих элементов, то справедливо

$$\check{z}_1 \bullet \check{z}_2 = \check{z}_2 \bullet \check{z}_1$$

Пусть для подстановки F имеем ее цикловое представление $F = z_1 z_2 \dots z_t$, то выполнено

$$F^k = \check{z}_1^k \cdot \check{z}_2^k \cdot \dots \check{z}_t^k$$

Кроме того ясно, что $F^k = E \Leftrightarrow \check{z}_i^k = E$ для всех $i \in \overline{1,t}$ в силу независимости циклов.
Поскольку порядок цикла z_i равен его длине, то порядок F равен наименьшему k, которое делится на длины всех циклов z_i, $i \in \overline{1,t}$. ♦

4. Пусть $S(N_n)$ - симметрическая группа подстановок на элементах $N_n = \{1, 2, \dots, n\}$. Будем говорить, что подстановки $g_1, \dots, g_k$ <u>порождают</u> $S(N_n)$ или подстановки $g_1, \dots, g_k$ являются <u>системой образующих</u> для $S(N_n)$, если любая подстановка F представляется как произведение $x_1, \dots, x_t$, где $x_i \in \{g_1, \dots, g_k, g_1^{-1}, \cdots, g_k^{-1}\}$.
В этом случае пишут, $S(N_n) = \langle g_1, \dots, g_k \rangle$. Подстановка, имеющая цикловую структуру $k_1 = n - 2, k_2 = 1, k_3 = \dots = k_n = 0$, называется <u>транспозицией.</u> Если единственный цикл длины 2 содержит элементы i, j, то транспозиция обозначается (i,j) (циклы длины 1 опускаются в записи).
Непосредственно проверяется, что справедливо равенство

$$(a_1, \dots, a_t) = (a_1, a_t) \ \dots \ (a_1, a_3)(a_1, a_2)$$

Поскольку каждая подстановка представляется в виде произведения циклов, а каждый цикл - в виде произведения транспозиций, то получаем

Теорема. Множество транспозиций является системой образующих для симметрической группы.

Укажем теперь другие системы образующих

а) (1, 2), (2, 3), … , (n - 1, n)

в) (1, 2), (1, 3), … , (1, n)

с) (1, 2), (1, 2, … , n)

Легко проверяются следующие равенства:

(i, j) = (1, i)(1, j)(1, i)

(i, j) = (i, 1) (1, 2) … (j - 1, j)(j - 1, j - 2) … (2, 1)(i, 1)

$(1, 2, \dots, n)^j (1, 2)(1, 2)(1, 2, \dots, n)^{-j} = (j + 1, j + 2)$

Из данных равенств следует, что множества а), в), с) являются образующими для симметрической группы $S(N_n)$.

5. Рассмотрим две подстановки степени n, имеющие одинаковые цикловые структуры:

$A_1 = (a_{11}, \dots, a_{1k_1}) (a_{21}, \dots, a_{2k_2}) \dots (a_{t1}, \dots, a_{tk_t})$

$A_2 = (b_{11}, \dots, b_{1k_1}) (b_{21}, \dots, b_{2k_2}) \dots (b_{t1}, \dots, b_{tk_t})$

Определим теперь подстановку F с помощью двустрочной записи:

$$F = \begin{pmatrix} a_{11} \cdots a_{1k_1} a_{21} \cdots a_{2k_2} \cdots a_{t1} \cdots a_{tk_t} \\ b_{11} \cdots b_{1k_1} b_{21} \cdots b_{2k_2} \cdots b_{t1} \cdots b_{tk_t} \end{pmatrix}$$

Непосредственным вычислением можно проверить, что справедливо равенство

$$F^{-1}A_2F = A_1 \qquad (\alpha)$$

Подстановки A_1, A_2 , для которых существует подстановка F, удовлетворяющая соотношению (α), называются сопряженными.

Легко проверить, что отношение сопряженности является отношением эквивалентности на множестве подстановок. Значит, все множество подстановок распадается на классы сопряженных подстановок.

Из предыдущего следует, что любые две подстановки, имеющие одинаковую цикловую структуру, - сопряжены.

Верно и обратное, если две подстановки сопряженны, то они имеют одинаковую цикловую структуру.

♦ Действительно, если $z = (a_{11}, \dots, a_{1p})$ - цикл длины p, то для любой подстановки F имеем $F^{-1}zF = (F^{-1}(a_{11}), \dots, F^{-1}(a_{1p}))$ - цикл длины p. Далее, если

$z_1 \dots z_t$ - произведение независимых циклов, то

$$F^{-1}z_1 \dots z_tF = F^{-1}z_1F \cdot F^{-1}z_2F \dots F^{-1}z_tF \ -$$

также произведение независимых циклов тех же длин. ♦

Заметим, что сопряженные подстановки имеют одинаковый порядок.

Уравнение (α), в котором заданы подстановки A_1, A_2 и неизвестна подстановка F, называется уравнением Коши. Как следует из предыдущего, оно разрешимо тогда и только тогда, когда подстановки A_1, A_2 имеют одинаковую цикловую структуру.

Можно доказать, что если цикловая структура подстановок A_1, A_2 есть, $\left[1^{k_1}\ 2^{k_2} \dots n^{k_n}\right]$, то имеется точно $\left[1^{k_1} k_1!\, 2^{k_2} k_2! \dots n^{k_n} k_n!\right]$ решений уравнения Коши.

Упражнения.

1. Найти число подстановок степени n, имеющих порядок 2.

2. Решить уравнение Коши $X^{-1}AX = B$,

где $A = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,4\,1\,2\,5 \end{pmatrix}$, $B = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 4\,2\,5\,1\,3 \end{pmatrix}$

3. Множество подстановок $S(N_3)$ разбить на классы сопряженных.

§ 6. Порождение сочетаний и перестановок.

1. Рассмотрим теперь алгоритмические вопросы, связанные с порождением сочетаний и перестановок. Пусть дано множество $A = \{1, 2, \dots , n\}$.

Порождение сочетаний. Приведем алгоритм, порождающий все сочетания (подмножества) множества A.

Алгоритм “сочетания”.

1. Дано: множество A. Выход: последовательность подмножеств A.
2. Начало: Пустое множество $\varnothing$.
3. Пусть порождено множество S. Тогда следующее множество S' получается включением в S наименьшего элемента, не принадлежащего S, и удалением из него всех элементов, меньших включенного. Если таких элементов нет, стоп.

♦ Справедливость алгоритма следует индукцией по n, если заметить, что алгоритм порождает сначала все подмножества множества $A' = \{1, 2, \ , n - 1\}$, затем повторяет эту последовательность, добавляя к каждому подмножеству n. Последним членом в последовательности будет само множество A, и алгоритм автоматически остановится. ♦

Укажем теперь алгоритм, который порождает все подмножества множества A, так, что каждое следующее отличается от предыдущего не более, чем на один элемент. Данный алгоритм определим индуктивно.

Алгоритм “Сочетания добавлением/изъятием одного элемента”.

Если $n = 1$, то выход алгоритма есть последовательность $\varnothing$, $\{1\}$.

Пусть для $n - 1$ выходом алгоритма есть последовательность L_{n-1} . Обозначим $\overline{L_{n-1}}$ - последовательность L_{n-1}, написанную в обратном порядке. Тогда для n выходом алгоритма будет последовательность

$$L_n = L_{n-1}\ ,\ \overline{L}_{n-1} \vee \{n\}\ ,$$

где $\overline{L}_{n-1} \vee \{n\}$ означает, что к каждому члену последовательности $\overline{L_{n-1}}$ добавлен элемент n.

Пример: $L_2 = \varnothing, \{1\}, \{1, 2\}, \{2\}$

$L_3 = \varnothing, \{1\}, \{1, 2\}, \{2\}, \{2, 3\}, \{1, 2, 3\}, \{1, 3\}, \{3\}$.

Справедливость алгоритма легко устанавливается индукцией по n, если заметить, что L_{n-1} заканчивается множеством $\{n - 1\}$. Первая половина последовательности L_n совпадает с L_{n-1} и по индукции удовлетворяет нужным требованиям. Следующий элемент после L_{n-1} есть $\{n - 1, n\}$, и затем проходится последовательность L_{n-1} в обратном порядке с

добавлением элемента $\{n\}$, и нужные требования снова выполняются. Поскольку первый элемент в L_{n-1} есть $\varnothing$, то последний элемент в L_n есть $\{n\}$. Если длина L_{n-1} есть 2^{n-1}, то длина L_n есть
$2 \cdot 2^{n-1} = 2^n$. ♦

Представим теперь алгоритм, который порождает все r-сочетания n-множества $A = \{1, 2, \dots, n\}$ в лексикографическом порядке. Каждое r-сочетание представляется числами $a_1 < a_2 < \dots < a_r$.
Начало алгоритма: $a_1 = 1, a_2 = 2, \dots, a_r = r$.
Пусть порождено r-сочетание $a_1, a_2, \dots, a_r$. Тогда определяется наибольшее a_i, такое, что $a_i + 1$ не входит в данное сочетание. Если таких a_i нет (это происходит только в случае $a_1 = n - r + 1, \dots, a_r = n$), то стоп.
Если такое a_i есть, то образуем новое сочетание $a_1', \dots, a_r'$, полагая

$$a_1' = a_1, \dots, a_{i-1}' = a_{i-1}, a_r' = a_i + 1, a_{i+1}' = a_i + 2, \dots, a_r' = a_i + r - i.$$

Проиллюстрируем алгоритм для $n = 4$, $r = 2$

Шаги	Сочетания	a_i
1	1,2	2
2	1,3	3
3	1,4	1
4	2,3	3
5	2,4	2
6	3,4	стоп

Предоставляется доказать в качестве упражнения индукцией по n, что описанный алгоритм порождает все r-сочетания n-множества.

2. Перейдем теперь к вопросу порождения n-перестановок n-множества $A = \{1, 2, \dots, n\}$. Определим сначала индуктивный алгоритм A(n). Для $n = 1$ выход A(1) есть перестановка (1). Пусть для $n - 1$ алгоритм построил все $(n - 1)$-перестановки чисел $1, 2, \dots, n - 1$. Тогда A(n) действует так.

Каждой $(n - 1)$-перестановке $b_1, \dots, b_{n-1}$ чисел $1, 2, \dots, n - 1$ ставится в соответствие n перестановок чисел $1, 2, \dots, n$ следующим образом:

$(b_1', \dots, b_{n-1}', 1)$, где $b_i' = b_i + 1, \quad i = \overline{1, n-1}$

$(b_1'', \dots, b_{n-1}'', 2)$, где $b_i'' = b_i$ если $b_i = 1$

$$b_i'' = b_i + 2 \quad \text{если } b_i \geq 2.$$

$$\ldots$$

$$(b_1^{(n)}, \ldots, b_{n-1}^{n}, n), \quad \text{где } b_i^{(n)} = b_i, \quad i = \overline{1, n-1}$$

Корректность данного алгоритма следует из того, что для любого $s \in \overline{1, n}$ последовательность $b_1^{(s)}, \ldots, b_{n-1}^{(s)}$ есть перестановка чисел 1, 2, … , s - 1, s + 1, … , n.

Представим теперь алгоритм порождения всех n! перестановок n-множества A = {1, 2, … , n} , в котором переход от одной перестановки к следующей осуществляется одной транспозицией соседних элементов. Транспозиция - это перемена местами двух элементов. Каждый элемент снабжается “направлением”, обозначаемым “→“ или “←“. Число k называется подвижным, если существует меньшее его число, соседнее с ним со стороны стрелки.

Алгоритм “Перестановки”.

Начало - конфигурация $\overleftarrow{1}\ \overleftarrow{2} \ldots \overleftarrow{n}$

Шаг алгоритма

1. Если нет подвижных элементов, то стоп.
2. Находится наибольшее подвижное число m
3. Число m переставляется с соседним элементом, на которое указывает направление m.
4. Направления всех элементов k, k > m меняются на противоположные.
5. Повторить шаг 1.

Проиллюстрируем алгоритм для n = 3.

Шаг	Конфигурация	Максимальное подвижное число
1	$\overleftarrow{1}\,\overleftarrow{2}\,\overleftarrow{3}$	3
2	$\overleftarrow{1}\,\overleftarrow{3}\,\overleftarrow{2}$	3
3	$\overleftarrow{3}\,\overleftarrow{1}\,\overleftarrow{2}$	2
4	$\overrightarrow{3}\,\overleftarrow{2}\,\overleftarrow{1}$	3
5	$\overleftarrow{2}\,\overrightarrow{3}\,\overleftarrow{1}$	3

6	$\overleftarrow{2}\,\overleftarrow{1}\,\overrightarrow{3}$	нет, стоп

Корректность данного алгоритма устанавливается индукцией по n. Пусть алгоритм правильно работает для n, и покажем его правильность для n + 1. (Случай n = 1 тривиален). Ясно, что если начинать работу с конфигурации $\overleftarrow{1}\ \overleftarrow{2} \ldots \overleftarrow{n}\ \overleftarrow{n+1}$, что n + 1 - максимальное подвижное число, и оно им остается до тех пор, пока не будет получена конфигурация $\overleftarrow{n+1}\ \overleftarrow{1} \ldots \overleftarrow{n}$. При этом будут порождены n+1 перестановок, в которых число n+1 занимает места n + 1, n, … , 1. Теперь максимальное подвижное число n, и переставляются элементы множества 1, 2, … ,n. Теперь снова максимальное подвижное число n + 1, после смены его направления оно будет двигаться влево n + 1 раз, порождая n + 1 перестановок. Когда будет получена перестановка $a_1\ a_2 \ldots a_n\ \overrightarrow{n+1}$, число n+1 не будет неподвижным, и алгоритм будет применяться к множеству
1, 2, …n, после чего число n + 1 снова становится подвижным. Таким образом, алгоритм порождает n + 1 перестановок и применяется к множеству 1, 2, … , n. Когда будет достигнута последняя перестановка чисел 1, 2, … , n, то число n +1 через n + 1 шагов перестанет быть подвижным, и алгоритм останавливается. Общее число шагов алгоритма (n + 1)·n! = (n + 1)!.

ГЛАВА II. МЕТОДЫ ПЕРЕЧИСЛЕНИЯ

§ 1. Метод включения-исключения.

Предположим, что имеется множество X из N элементов. Пусть имеется t свойств $P_1, \ldots, P_t$, так, что любой элемент множества X может обладать или не обладать любым из этих свойств. Пусть $N(P_i)$ - число элементов из X, обладающих свойством P_i. Для любого подмножества свойств $\{P_{i_1}, \ldots, P_{i_r}\}$ обозначим $N(P_{i_1}, \ldots, P_{i_r})$ - число элементов из X, обладающих свойствами $P_{i_1}, \ldots, P_{i_r}$ (возможно также и некоторыми другими свойствами).

<u>Теорема 1.</u> Число элементов N(0) множества X, не обладающих ни одним из названных свойств, задается формулой

$$N(0) = S_0 - S_1 + S_2 - \ldots + (-1)^t S_t \qquad (1)$$

где $S_0 = N$

$$S_k = \sum_{1 \le i_1 < \ldots < i_k \le t} N(P_{i_1}, \ldots, P_{i_k}), \qquad k \in \overline{1, t}$$

Формула (1) называется формулой <u>включения-исключения.</u>

♦ Элемент $a \in X$, не обладающий ни одним из указанных свойств учитывается один раз в члене S_0 и не входит ни в один из остальных слагаемых правой части (1). Элемент $a \in X$ со свойством P_j учитывается один раз в члене S_0 и один раз в члене $S_1 = \sum_{i=1}^{t} N(P_i)$, причем в члене S_0 1 раз, а в члене S_1 - 1 раз и общий его вклад равен $1 + (-1) = 0$. Элемент $a \in X$, обладающий точно r свойствами $P_{i_1}, \ldots, P_{i_r}$ $(r \ge 1)$, учитывается один раз в члене S_0 и дает вклад 1, далее $\binom{r}{1}$ раз в члене S_1 и дает вклад - $\binom{r}{1}$, затем $\binom{r}{2}$ раз в члене S_2 и дает вклад $\binom{r}{2}$ и, вообще, учитывается $\binom{r}{k}$ раз в члене S_k и дает вклад $(-1)^k\binom{r}{k}$, где $k \le r$. Следовательно, общий вклад элемента a в правую часть (1) равен

$$1 - \binom{r}{1} + \binom{r}{2} - \ldots + (-1)^k\binom{r}{k} + \ldots + (-1)^r\binom{r}{r}, = (1-1)^r = 0$$

Значит, правая часть (1) учитывает точно 1 раз каждый элемент, не обладающий ни одним из указанных свойств, а всякий другой элемент учитывается 0 раз, следовательно, правая часть (1) равна N(0) . ♦

Формула (1) может быть обобщена следующим образом.

<u>Теорема 2.</u> Число элементов N(r) множества X, обладающих точно r свойствами из указанных свойств, дается формулой

$$N(r) = S_r - \binom{r+1}{r} S_{r+1} + \ldots + (-1)^s \binom{r+s}{r} S_{r+s} + \ldots + (-1)^{t-r} \binom{t}{r} S_t \quad (2)$$

♦ В правой части (2) элемент $a \in X$, обладающий точно r свойствами, учитывается 1 раз в первом слагаемом и не учитывается в остальных слагаемых. Пусть теперь элемент $a \in X$ обладает точно k свойствами, $r < k \le t$. Тогда он учитывается в слагаемых $S_r, S_{r+1}, \ldots, S_k$ число раз, равное $\binom{r}{r}\binom{k}{r}, \binom{r+1}{r}\binom{k}{r+1}, \ldots, \binom{k}{r}\binom{k}{k}$ соответственно.

Значит общий вклад элемента $a \in X$ равен

$$\binom{r}{r}\binom{k}{r} - \binom{r+1}{r}\binom{k}{r+1} + \binom{r+2}{r}\binom{k}{r+2} - \ldots + (-1)^{k-r}\binom{k}{r}\binom{k}{k} \qquad (3)$$

Воспользуемся легко проверяемым тождеством $\binom{b}{a}\binom{c}{b} = \binom{c}{a}\binom{c-a}{b-a}$ и преобразуем сумму (3).

$$\binom{k}{r}\binom{k-r}{0} - \binom{k}{r}\binom{k-r}{1} + \binom{k}{r}\binom{k-r}{2} - \ldots + (-1)^{k-r}\binom{k}{r}\binom{k-r}{k-r}$$

Следовательно имеем

$$\binom{k}{r}\left[\binom{k-r}{0} - \binom{k-r}{1} + \binom{k-r}{2} - \cdots + (-1)^{k-r}\binom{k-r}{k-r}\right] = 0$$

Значит, формула (2) учитывает каждый элемент, обладающий точно r свойствами 1 раз, а остальные элементы из X учитываются 0 раз. ♦

Дальнейшее обобщение формулы включения-исключения может быть сделано следующим образом. Предположим, что каждый элемент $a \in A$ обладает весом w(a), представляющим собой элемент некоторого поля F. Для любого подмножества свойств $\{P_{i_1}, \ldots, P_{i_r}\}$ обозначим через $W(P_{i_1}, \ldots, P_{i_r})$ сумму весов всех элементов X, обладающих свойствами $P_{i_1}, \ldots, P_{i_r}$ (возможно также и некоторыми другими). Положим

$W(r) = \sum_{1 \le i_1 < \ldots < i_r \le t} W(P_{i_1}, \ldots, P_{ir})$, W(0) - сумма весов всех элементов из X. Пусть E(r) - сумма весов всех элементов из X, обладающих точно r свойствами.

Теорема 3. Справедлива формула

$$E(r) = W(r) - \binom{r+1}{r} W(r+1) + \binom{r+2}{r} W(r+2) - \ldots + (-1)^{t-r} \binom{t}{r} W(t) \quad (4)$$

♦ Доказательство почти дословно повторяет доказательство формулы (2) и потому опускается. ♦

Рассмотрим приложения формулы включения-исключения.

1. Пусть $X_1, \ldots, X_n$ - семейство подмножеств множества X. Тогда справедливо тождество

$$|X_1 \bigcup \ldots \bigcup X_n| = \sum_{i=1}^{n} |X_i| - \sum_{1 \le i < j \le n} |X_i \bigcap X_j| + \cdots + (-1)^{n-1} |X_1 \bigcap \ldots \bigcap X_n| \quad (5)$$

♦ Пусть $x \in X_1 \bigcup \ldots \bigcup X_n$. Говорим, что элемент x обладает свойством P_i, $i \in \overline{1, n}$, если $x \in X_i$. Пусть X(0) - число элементов из $X_1 \bigcup \ldots \bigcup X_n$, не обладающих ни одним из указанных свойств P_i, $i \in \overline{1, n}$. По формуле включения-исключения имеем

$$N(0) = | X_1 \bigcup \ldots \bigcup X_n | - \sum_{i=1}^{n} |X_i| + \sum_{1 \le i < j \le n} |X_i \bigcap X_j| + \cdots + (-1)^{n} |X_1 \bigcap \ldots \bigcap X_n|$$

Поскольку N(0) = 0, то отсюда следует формула (5). ♦

2. Пусть X, Y - произвольные множества, $|X| = n$, $|Y| = m$. Тогда число W_{nm} сюръективных отображений $f : X \to Y$ $(n \ge m)$ дается формулой.

$$W_{nm} = m^n - \binom{m}{1}(m-1)^n + \binom{m}{2}(m-2)^n - \cdots + (-1)^n \binom{m}{m}(m-m)^n \quad (6)$$

♦ На множестве всех отображений $f : X \to Y$ введем m свойств $P_1, \ldots, P_m$ следующим образом: отображение $f : X \to Y$ обладает свойством P_i, если в образ отображения f не входит элемент $y_i \in Y$, где $Y = \{y_1, \ldots, y_m\}$. Значит, отображения $f : X \to Y$, не обладающие ни одним из указанных свойств $P_1, \ldots, P_m$, есть очевидно сюръективные отображения. Далее, имеем следующие соотношения:

$N = m^n$ - число всех отображений $f : X \to Y$

$N(P_i) = (m - 1)^n$

…

$N(P_{i_1}, \ldots, P_{i_k}) = (m - k)^n$

Теперь по формуле включения-исключения получаем формулу (6).

3. Пусть X , Y - произвольные множества, $|X| = k$, $|Y| = m$. Рассмотрим функцию n переменных $f(x_1, \dots , x_n)$, где $x_i \in X$ со значениями из множества Y. Переменная x_i называется фиктивной, если справедливо

$$f(x_1, \dots , x_{i-1}, x', x_{i+1}, \dots , x_n) = f(x_1, \dots , x_{i-1}, x'', x_{i+1}, \dots , x_n) , \forall x_i, x', x'' \in X \quad (6')$$

Найдем число N_0 функций f, $f : X^n \to Y$, не имеющих фиктивных переменных. На множестве всех функций данного вида определим n свойств $P_1, \dots , P_n$, где свойство P_i означает, что переменная x_i фиктивна, $i \in \overline{1, n}$. Ясно, что справедливы соотношения

$$N = m^{k^n}$$

$$N(P_i) = m^{k^{n-1}}$$

$$N(P_i, P_j) = m^{k^{n-2}}$$

. . . .

$$N(P_{i_1},\dots,P_{i_t}) = m^{k^{n-t}}$$

. . . .

По формуле включения-исключения получаем

$$N_0 = m^{k^n} - \binom{n}{1} m^{k^{n-1}} + \binom{n}{2} m^{k^{n-2}} - \dots + (-1)^n \binom{n}{n} m^{k^{n-n}} \quad (6'')$$

4. Пусть имеем n-множество $X = \{x_1, \dots , x_n\}$. Две подстановки φ_1, φ_2 множества X называются толерантными, если для них справедливо: $\exists\, x \in X \mid \varphi_1(x) = \varphi_2(x)$.

Не толерантные подстановки φ_1, φ_2 называются противоречивыми. Число Q_n пар противоречивых подстановок n-множества X дается формулой

$$Q_n = (n!)^2 \left(1 - \frac{1}{1!} + \frac{1}{2!} - \dots + (-1)^n \frac{1}{n!}\right) \quad (7)$$

♦ Зафиксируем подстановку φ_1, которая выбирается n! способами, и найдем число D_n подстановок φ_2, противоречивых с φ_1. Покажем, что справедливо

$$D_n = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \dots + (-1)^n \frac{1}{n!}\right) \quad (8)$$

Действительно, введем свойства $P_1, \dots , P_n$ на множестве всех подстановок $\{\varphi\}$ множества X, где свойство P_i, $i \in \overline{1, n}$ означает, что выполнено $\varphi(x_i) = \varphi_1(x_i)$. .

Интересующие нас подстановки φ_2 есть подстановки, не обладающие ни одним из названных свойств $P_1, \dots , P_n$.

Имеем $N = n!$, $N(P_i) = (n - 1)!$, … , $N(P_{i_1},\dots,P_{i_k}) = (n - k)!$. Применяя формулу включения-исключения, получаем справедливость формулы (8), а следовательно, и формулы (7). ♦

Зафиксируем теперь число k, $0 \le k \le n$. Две подстановки φ_1, φ_2 множества X называются k-толерантными, если имеется точно k элементов $x \in X$, для которых
$\varphi_1(x) = \varphi_2(x)$.
Аналогично предыдущему, используя формулы (2), можно показать, что число Q_{nk} пар k-толерантных подстановок n-множества выражается формулой

$$Q_{nk} = \frac{(n!)^2}{k!}\left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^{n-k}\frac{1}{(n-k)!}\right) \qquad (9)$$

Если вместо подстановок рассматривать отображения, то вопросы их толерантности решаются легко. Пусть имеется n-множество $X = \{x_1, \dots, x_n\}$ и m-множество $Y = \{y_1, \dots, y_m\}$. Два отображения $f, g : X \to Y$ называются толерантными, если существует $x \in X$, такое, что $f(x) = g(x)$. Не толерантные отображения f, g называются противоречивыми. Число M_{mn} пар противоречивых отображений n-множества X в m-множество Y дается формулой

$$M_{mn} = m^n (m - 1)^n \qquad (10)$$

Зафиксируем число k, $0 \le k \le n$. Два отображения $f, g : X \to Y$ называются k-толерантными, если существует точно k элементов $x \in X$, таких, что $f(x) = g(x)$. Число Nmn пар k-толерантных отображений n-множества X в m-множество Y дается формулой

$$N_{mn} = \binom{n}{k}(m-1)^{n-k} \cdot m^n \qquad (11)$$

5. Рассмотрим задачу построения подстановок n-множества $X = \{x_1, \dots, x_n\}$ методом бесповторного набора. Суть метода заключается в следующем. Фиксируется число $t \ge n$ и рассматривается произвольная последовательность $\bar{a} = (a_1, a_2, \dots, a_t)$ элементов множества X длины t. Тогда по последовательности $\bar{a}$ строится подстановка π_a следующим образом: $\pi_a(x_1) = a_1$. Если определены $\pi_a(x_1), \dots, \pi_a(x_k)$, то $\pi_a(x_{k+1}) = a_l$, где l - наименьший индекс, такой, что $a_l \ne \pi_a(x_1)$, $a_l \ne \pi_a(x_2)$, … , $a_l \ne \pi_a(x_k)$. Данный метод построения подстановки - “частотный”, т.е. не для всякой последовательности $\bar{a}$ может быть построена подстановка π_a. Примером такой последовательности является последовательность $\bar{a} = (x_1, x_1, \dots, x_1)$. Данный метод приводит к результату тогда и только

тогда, когда в последовательности $\bar{a}$ содержатся все элементы
$x_1, \dots, x_n$.

Число R_{nt} последовательностей $\bar{a} = (a_1, \dots, a_t)$ в алфавите $X = \{x_1, \dots, x_n\}$, содержащих все элементы X $(t \ge n)$выражается формулой

$$R_{nt} = n^t - \binom{n}{1}(n-1)^t + \binom{n}{2}(n-2)^t - \dots + (-1)^n \binom{n}{n}(n-n)^t \qquad (12)$$

♦ Представляя последовательность $\bar{a} = (a_1, \dots, a_t)$ как отображение $\varphi : Y \to X$, где $Y = \{1, 2, \dots, t\}$и отождествляя $(a_1, \dots, a_t) \equiv (\varphi(1), \varphi(2), \dots, \varphi(t))$, получаем, что последовательности $(a_1, \dots, a_t)$, содержащие все элементы $X = \{x_1, \dots, x_n\}$, есть сюръективные отображения $\varphi : Y \to X$. Остается применить формулу (6). ♦

6. Пусть $X = \{x_1, \dots, x_n\}$. найдем число U_n подстановок φ множества X, таких, что $\varphi(x_i) \ne x_i$ и $\varphi(x_i) \ne x_{i+1}$, $i \in \overline{1, n-1}$, $\varphi(x_n) \ne x_n$ и $\varphi(x_n) \ne x_1$. Другими словами, нас интересует число U_n подстановок, противоречивых двум подстановкам:

$$\begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_1 & x_2 & \dots & x_n \end{pmatrix} \text{ и } \qquad \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_2 & x_3 & \dots & x_1 \end{pmatrix}$$

<u>Теорема 4.</u> Для чисел U_n $(n > 1)$ справедлива формула

$$U_n = n! - \frac{2n}{2n-1}\binom{2n-1}{1}(n-1)! + \frac{2n}{2n-2}\binom{2n-2}{2}(n-2)! - \dots + (-1)^n \frac{2n}{n}\binom{n}{n}0!$$

♦ Предварительно докажем две леммы.

1. Два элемента из X вида (x_i, x_{i+1}) называются соседними ($i \in \overline{1, n-1}$). Число f(n, k) подмножеств X из k элементов и не содержащих соседних элементов равно

$$f(n, k) = \binom{n-k+1}{k} \qquad (14)$$

♦ Каждое такое подмножество $Y \subseteq X$ будем характеризовать двоичным вектором длины n $a_1, \dots, a_n$, где $a_i = 1 \Leftrightarrow x_i \in Y$. Интересующим нас подмножествам соответствуют вектора с k единицами и не содержащие двух единиц подряд. Число таких векторов можно подсчитать так. Если взять последовательность n - k нулей, то k единиц могут размещаться только в промежутках между нулями. Число мест для единиц n - k +1 , число единиц k. Следовательно, число интересующих нас подмножеств выражается формулой (14). ♦

2. Пусть теперь считаются соседними элементы X вида (x_i, x_{i+1}), $(i \in \overline{1, n-1})$, а также (x_1, x_n). Тогда число $g(n, k)$ подмножеств X из k элементов и не содержащих соседних элементов равно

$$g(n, k) = \frac{n}{n-k}\binom{n-k}{k} \qquad (15)$$

♦ Разобьем все такие подмножества $Y \subseteq X$ на два класса: те, которые содержат x_1, и те, которые не содержат x_1. Подмножество, содержащее x_1, не содержит x_2 и x_n. Значит, число таких подмножеств равно числу (k - 1)-подмножеств из (n - 3)-множества $X' = \{x_3, \ldots, x_{n-1}\}$, не содержащих соседних элементов, и по предыдущему это число равно $\binom{n-3-(k-1)+1}{k-1} = \binom{n-k-1}{k-1}$. Число подмножеств второго класса равно числу k-подмножеств из (n - 1)-множества $X'' = \{x_2, x_3, \ldots, x_n\}$, не содержащих соседних элементов, и, согласно предыдущему, это число равно $\binom{n-1-k+1}{k} = \binom{n-k}{k}$. Следовательно, интересующее нас число k-подмножеств по правилу суммы равно

$$g(n, k) = \binom{n-k-1}{k-1} + \binom{n-k}{k} = \frac{n}{n-k}\binom{n-k}{k} \quad ♦$$

Завершим теперь доказательство теоремы 4. На множестве n! подстановок множества $X = \{x_1, \ , x_n\}$ введем 2n свойств $P_1, \ldots, P_n, \ , P_1', \ldots, P_n'$, где $\forall \ i \in \overline{1, n}$ свойство P_i подстановки ψ означает, что $\psi(x_i) = x_i$, свойство P_i' означает, что $\psi(x_i) = x_{i+1}$ при $i \in \overline{1, n-1}$, при $i = n$ P_n' означает, что $\psi(x_n) = x_1$.

Расположим указанные свойства в ряд

$$P_1, P_1', P_2, P_2', \ldots, P_n, P_n' \qquad (16)$$

Теперь для любого k-подмножества множества этих свойств определим число V_k подстановок, обладающих каждым из свойств, входящих в k-подмножество. Оно равно (n - k)!, если выбранные k свойств совместимы и 0 в противном случае. Чтобы применить формулу включения-исключения остается найти число способов выбора из 2n свойств (16) k-подмножество совместимых свойств. Ясно, что несовместимыми свойствами являются два соседних в последовательности (16), при этом свойства P_n' и P_1 считаются соседними. Число способов выбора k-подмножеств совместимых свойств согласно предыдущему равно $\frac{2n}{2n-k}\binom{2n-k}{k}$. По формуле включения-исключения получаем формулу (13). ♦

§ 2. Метод рекуррентных соотношений

Данный метод состоит в том, что решение комбинаторной задачи с n предметами выражается через решение аналогичной задачи с меньшим числом предметов с помощью некоторого соотношения, называемого рекуррентным. Говорят, что последовательность элементов $u_0, u_1, \ldots u_n, \ldots$ над полем комплексных чисел C удовлетворяет рекуррентному соотношению порядка k, если

$$u_n = F(u_{n-1}, \ldots , u_{n-k}), \quad \forall \ n \geq k \qquad (1)$$

Если задать $u_0, u_1, \ldots u_{k-1}$, то u_n, $\forall \ n \geq k$ определено однозначно. Рекуррентное соотношение называется линейным, если

$$u_n = a_1 u_{n-1} + \ldots + a_k u_{n-k}, \quad \forall \ n \geq k \qquad (2)$$

где $a_1, \ldots , a_k$ - коэффициенты из C. Соотношения такого типа естественным образом возникают при решении комбинаторных задач.

Пример. Пусть имеется последовательность позиций, занумерованных числами 1, 2, … , n, … и в начальный момент предмет находится в 1-ой позиции. За один ход предмет продвигается вперед на 1 и 2 позиции. Найти число способов попадания в n-ю позицию.

♦ Пусть u_n - интересующее нас число. Ясно, что $u_2 = 1$, $u_3 = 2$. Далее, разобьем все способы попадания в позицию с номером n на два класса: те, при которых на последнем шаге предмет передвигается на 1 шаг и те, при которых он передвигается на 2 шага. Ясно, что в первом случае имеем u_{n-1} вариантов, во втором u_{n-2} вариантов. Следовательно, имеем

$$u_n = u_{n-1} + u_{n-2} \qquad (3)$$

В качестве начальных условий можно взять $u_1 = 1$, $u_2 = 1$. ♦

Полученные числа u_n называются числами Фибоначчи. Наиболее известной частью рекуррентных соотношений являются линейные рекуррентные соотношения. Свяжем с линейным соотношением (2) многочлен над C

$$P(x) = x^k - a_1x^{k-1} - \ldots - a_k \qquad (4)$$

Многочлен P(x) называется характеристическим для линейного рекуррентного соотношения (2). Заметим, что всякая рекуррентная последовательность k-го порядка однозначно определяется заданием k ее первых членов.

Пусть λ - корень характеристического многочлена P(x).

Теорема 1. Последовательность $u_0, u_1, \ldots u_n, \ldots$, где $u_n = c\lambda^n$, c - произвольная константа из C, удовлетворяет линейному рекуррентному соотношению (2).

♦Подставляя данные значения u_n, $n = 0, 1, \dots$ в (2), имеем

$c\lambda^n - a_1 c\lambda^{n-1} - a_2 c\lambda^{n-2} - \dots - a_k c\lambda^{n-k} = c\lambda^{n-k} (\lambda^k - a_1 \lambda^{k-1} - \dots - a_k) \equiv 0$. ♦

<u>Теорема 2.</u> Пусть последовательности u_n, v_n, $n = 0, 1, \dots$ удовлетворяют линейному рекуррентному соотношению (2). Тогда этим свойством обладает последовательность r_n, $n = 0, 1, \dots$, где $r_n = \alpha u_n + \beta v_n$, $\forall\, n$, α, β - произвольные константы из C.

♦ Доказательство очевидно. ♦

<u>Теорема 3.</u> Пусть $\lambda_1, \dots, \lambda_k$ - простые (т.е. не являющиеся кратными) корни характеристического многочлена P(x) для последовательности (2).

Тогда общее решение данного рекуррентного соотношения имеет вид

$$u_n = c_1\lambda_1^n + c_2\lambda_2^n + \dots + c_k\lambda_k^n, \qquad \forall\, n \tag{5}$$

где $c_1, \dots, c_k$ - подходящие константы из C.

♦ Согласно предыдущему замечаем, что последовательностьu_n, $n = 0, 1, \dots$ есть решение соотношения (2). Чтобы доказать, что любое решение имеет вид (5) достаточно показать, что для произвольной последовательности v_n, $n = 0, 1, \dots$, удовлетворяющей (2), существуют константы $c_1, \dots, c_k$, такие, что $u_n = v_n$, $\forall\, n$. Для этого достаточно, чтобы выполнялось $v_0 = u_0$, $v_1 = u_1$, …, $v_{k-1} = u_{k-1}$. Рассмотрим данные условия

$$\begin{aligned} u_0 &= c_1 + c_2 + \dots + c_k = v_0 \\ u_1 &= c_1\lambda_1 + c_2\lambda_2 + \dots + c_k\lambda_k = v_1 \\ &\dots\dots\dots\dots\dots\dots \\ u_{k-1} &= c_1\lambda_1^{k-1} + c_2\lambda_2^{k-1} + \dots + c_k\lambda_k^{k-1} = v_{k-1} \end{aligned} \tag{6}$$

Покажем, что для любых $v_0, v_1, \dots, v_{k-1}$ данная система уравнений всегда разрешима относительно $c_1, c_2, \dots, c_k$. Определитель этой системы есть определитель Вандермонда и согласно (7, стр. 118).

$$\det \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \lambda_1 & \lambda_2 & \cdots & \lambda_k \\ . & . & . & . \\ \lambda_1^{k-1} & \lambda_2^{k-1} & \dots & \lambda_k^{k-1} \end{vmatrix} = \prod_{i<j} (\lambda_i - \lambda_j) \neq 0$$

согласно предположению о корнях $\lambda_1, \dots, \lambda_k$. Отсюда и следует утверждение. ♦ В качестве примера рассмотрим рекуррентное соотношение (3). Имеем характеристический многочлен

$$P(x) = x^2 - x - 1$$

Его корни равны $\lambda_1 = \dfrac{1+\sqrt{5}}{2}$, $\lambda_2 = \dfrac{1-\sqrt{5}}{2}$, Общее решение имеет вид

$$u_n = c_1\left(\frac{1+\sqrt{5}}{2}\right)^n + c_2\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Система уравнений для констант c_1, c_2 :

$$c_1\left(\frac{1+\sqrt{5}}{2}\right) + c_2\left(\frac{1-\sqrt{5}}{2}\right) = 1$$

$$c_1\left(\frac{1+\sqrt{5}}{2}\right)^2 + c_2\left(\frac{1-\sqrt{5}}{2}\right)^2 = 1$$

Откуда получаем $c_1 = \frac{1}{\sqrt{5}}$, $c_2 = -\frac{1}{\sqrt{5}}$.

Пусть теперь λ - корень кратности r характеристического многочлена P(x). Аналогично предыдущему доказывается

<u>Теорема 4.</u> Последовательности $c_1\lambda^n, c_2 n\lambda^n, \ldots, c_r n^{r-1}\lambda^n$, n = 0, 1, … для произвольных констант $c_1, \ldots, c_r$ из C удовлетворяют соотношению (2).

<u>Теорема 5.</u> Пусть характеристический многочлен P(x) имеет корни $\lambda_1, \ldots, \lambda_s$ кратностей $r_1, \ldots, r_s$ $(r_1 + \ldots + r_s = k)$. Тогда общее решение рекуррентного соотношения (2) имеет вид

$$u_n = \sum_{i=1}^{s}(c_{i1} + c_{i2}n + \ldots + c_{ir_i}n^{r_i-1})\lambda_i^n, \quad c_{ij} \in C \qquad (7)$$

Укажем еще одно полезное свойство линейных рекуррентных соотношений.

<u>Теорема 6.</u> Пусть имеем соотношение

$$u_n = a_1u_{n-1} + \ldots + a_ku_{n-k}$$

с начальными условиями $u_1, \ldots, u_k$. Тогда справедливо соотношение при всех $n \ge k$

$$\begin{pmatrix} a_1 & a_2 & a_3 & . & . & . & a_k \\ 1 & 0 & 0 & . & . & . & 0 \\ 0 & 1 & 0 & . & . & . & 0 \\ . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & 1 & 0 \end{pmatrix}^{n-k} \begin{pmatrix} u_k \\ u_{k-1} \\ . \\ . \\ u_1 \end{pmatrix} = \begin{pmatrix} u_n \\ u_{n-1} \\ . \\ . \\ u_{n-k+1} \end{pmatrix} \qquad (8)$$

♦ Доказательство индукцией по n. При n = k равенство (8) справедливо. Пусть оно верно при n. При n + 1 имеем

$$\begin{pmatrix} a_1 & a_2 & a_3 & . & . & . & a_k \\ 1 & 0 & 0 & . & . & . & 0 \\ 0 & 1 & 0 & . & . & . & 0 \\ . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & 1 & 0 \end{pmatrix}^{n+1-k} \begin{pmatrix} u_k \\ u_{k-1} \\ . \\ . \\ u_1 \end{pmatrix} =$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 & . & . & . & a_k \\ 1 & 0 & 0 & . & . & . & 0 \\ 0 & 1 & 0 & . & . & . & 0 \\ . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & a_2 & a_3 & . & . & . & a_k \\ 1 & 0 & 0 & . & . & . & 0 \\ 0 & 1 & 0 & . & . & . & 0 \\ . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & 1 & 0 \end{pmatrix}^{n-k} \begin{pmatrix} u_k \\ u_{k-1} \\ . \\ . \\ u_1 \end{pmatrix} =$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 & . & . & . & a_k \\ 1 & 0 & 0 & . & . & . & 0 \\ 0 & 1 & 0 & . & . & . & 0 \\ . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & 1 & 0 \end{pmatrix} \begin{pmatrix} u_n \\ u_{n-1} \\ . \\ . \\ u_{n-k+1} \end{pmatrix} = \begin{pmatrix} u_{n+1} \\ u_n \\ . \\ . \\ u_{n-k+2} \end{pmatrix} \blacklozenge$$

В большинстве случаев, однако, при изучении перечислительных задач возникают нелинейные рекуррентные соотношения, для разрешения которых используются специфические приемы. Некоторые из них будут рассмотрены в дальнейшем. Приведем важный пример нелинейного рекуррентного соотношения.

<u>Теорема 7.</u> Пусть C(n, k) - число подстановок n-элементного множества, имеющих точно k циклов. Тогда справедливо

$$C(n, k) = C(n - 1, k - 1) + (n - 1)C(n - 1, k) \qquad (9)$$

$$C(0, 0) = 1, \quad C(0, 1) = 0$$

♦ Разобьем множество подстановок множества X = {1, 2, … n,} имеющих точно k циклов, на два класса - подстановки, в которых элемент n содержится в единичном цикле, и подстановки, в которых элемент n находится в цикле длины l, l > 1. В первом случае число подстановок совпадает с числом подстановок множества X′ = {1, 2, …, n - 1}, имеющих k - 1 циклов, т.е. C(n - 1, k - 1). Во втором случае, удаляя элемент n, получаем подстановку множества X′ = {1, 2, …, n - 1} с k циклами, число которых равно C(n - 1, k). Выясним теперь, каким числом способов в подстановку степени n - 1 с k циклами можно добавить элемент n. Если имеется цикл длины i, то это можно сделать i способами. Общее число способов равно $i_1 + \ldots + i_k$, где $i_1, \ldots, i_k$ - длины циклов подстановки. Однако $i_1 + \ldots + i_k = n - 1$. Значит число подстановок второго класса равно (n - 1)C(n - 1, k). Отсюда и получаем (9). ♦

Полученные числа C(n, k) связаны с известными числами Стирлинга первого рода $s_{n,k}$, которые определяются так:

$$s_{n,k} = (-1)^{n+k}\, C(n, k)$$

Приведем таблицу нескольких первых значений чисел $s_{n,k}$.

n	$s_{n,0}$	$s_{n,1}$	$s_{n,2}$	$s_{n,3}$	$s_{n,4}$	$s_{n,5}$
0	1	0	0	0	0	0
1	0	1	0	0	0	0
2	0	-1	1	0	0	0
3	0	2	-3	1	0	0
4	0	-6	11	-6	1	0
5	0	24	-50	35	-10	1
6	0	-120	274	-225	85	-15

Табл. Числа Стирлинга первого рода

§ 3. Производящие функции и формулы обращения

1. Пусть $a_0, a_1, \dots, a_n, \dots$ некоторая последовательность чисел. Свяжем с этой последовательностью ряд

$$R(x) = a_0 + a_1x + \dots + a_nx^n + \dots$$

называемый производящей функцией для последовательности $\{a^n\}$. Если ряд R(x) сходится в некотором круге радиуса $R > 0$ к некоторой функции F(x), то функцию F(x) также называют производящей для $\{a_n\}$.

Если R(x) и Q(x) - производящие функции для последовательностей $\{a_n\}$и $\{b_n\}$ соответственно, то естественным образом определяются операции:

а) Умножение на константу. Если α - некоторая константа, то $\alpha R(x) = \alpha a_0 + \alpha a_1 x + \dots + \alpha a_n x^n + \dots$, т.е. $\alpha R(x)$ - производящая функция для последовательности $\{\alpha a_n\}$.

в) Сложение.

$$R(x) + Q(x) = (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_n + b_n)x^n + \dots$$

т.е. R(x) + Q(x) - производящая функция последовательности $\{a_n + b_n\}$.

с) Умножение.

$$R(x)\cdot Q(x) = a_0\, b_0 + (a_0b_1 + a_1b_0)\, x + \dots + (\textstyle\sum_{i=0}^{n} a_i \cdot b_{n-i})x^n + \dots$$

и значит $R(x)\cdot Q(x)$ - производящая функция свертки последовательностей $\{a_n\}$и $\{b_n\}$.

Обратной к производящей функции R(x) называется функция Q(x) такая, что $Q(x)\cdot R(x) = 1$.

<u>Теорема 1.</u> Обратная функция к R(x) существует тогда и только тогда, когда $a_0 \neq 0$.

♦ Действительно, запишем условия обращения функции R(x)

$$
\begin{aligned}
&a_0b_0 = 1\\
&a_0b_1 + a_1b_0 = 0 \qquad\qquad (1)\\
&\dots\\
&\dots\\
&\textstyle\sum_{i=0}^{n} a_i \cdot b_{n-i} = 0
\end{aligned}
$$

Легко видеть, что система (1) разрешима относительно $b_0, b_1, \dots, b_n, \dots$ тогда и только тогда, когда $a_0 \neq 0$.

Решением в этом случае служит: $b_0 = \frac{1}{a_0}$, $b_1 = -\frac{a_1}{a_0^2}$.

Если $b_0, b_1, \dots, b_{n-1}$ уже определены, то

$$b_n = \frac{1}{a_0}(-a_1b_{n-1} - \dots - a_nb_0). \ \blacklozenge$$

Экспоненциальной производящей функцией для последовательности $\{a_n\}$называется ряд

$$E(x) = a_0 + a_1x + \dots + \frac{a_n}{n!}x^n + \dots \qquad (2)$$

Операция сложения, умножения на константу для экспоненциальных производящих функций определяются так же, как и для обычных производящих функций.

Произведение их определяется так: Если $E_a(x)$, $E_b(x)$ - экспоненциальные производящие функции для последовательностей $\{a_n\}$ и $\{b_n\}$ соответственно, то

$$E_a(x)\cdot E_b(x) = c_0 + c_1x + \dots + \frac{c_n}{n!}x^n + \dots \qquad (3)$$

где $c_n = a_0b_n + \binom{n}{1}a_1b_{n-1} + \dots + \binom{n}{k}a_kb_{n-k} + \dots + a_nb_0$.

Производящие функции являются полезным инструментом для решения перечислительных задач, получения различных тождеств и решения рекуррентных соотношений.

Пример. Найти последовательность a_n, $n = 0, 1, \dots$, для которой функция $(1 - 4x)^{-1/2}$ является производящей.

Решение. Согласно биномиальной теореме имеем

$$(1+x)^{\alpha} = 1 + \sum_{r=1} \frac{\alpha(\alpha-1)\cdots(\alpha-r+1)}{r!}x^r$$

где верхний предел суммирования равен α, если α - положительное целое, и бесконечен в противном случае.

Значит $(1-4x)^{-1/2} = 1 + \sum_{r=1}^{\infty} \frac{(-\frac{1}{2})(-\frac{1}{2}-1)\dots(-\frac{1}{2}-r+1)}{r!}(-4x)^r =$

$$= 1 + \sum_{r=1}^{\infty} \frac{4^r(1/2)(3/2)\dots(2r-1/2)}{r!}x^r =$$

$$= 1 + \sum_{r=1}^{\infty} \frac{2^r\cdot 1\cdot 3\cdots(2r-1)}{r!}x^r = 1 + \sum_{r=1}^{\infty} \frac{2^r\cdot r!\cdot 1\cdot 3\cdots(2r-1)}{r!\cdot r!}x^r =$$

$$= 1 + \sum_{r=1}^{\infty} \frac{(2\cdot 4\cdots 2r)(1\cdot 3\cdots (2r-1))}{r!\qquad\qquad r!} x^r = 1 + \sum_{r=1}^{\infty} \binom{2r}{r} x^r$$

Значит, данная функция будет обыкновенной производящей для последовательности $a_n = \binom{2n}{n}$, n = 0, 1, … и будет экспоненциальной производящей для последовательности $b_n = n!\binom{2n}{n}$, n = 0, 1, … .

<u>Теорема 2.</u> Для любого t справедливо тождество

$$\sum_{i=0}^{t} \binom{2i}{i}\binom{2t-2i}{t-i} = 4^t \tag{5}$$

♦ Действительно, согласно предыдущей задаче $\binom{2i}{i}$ - коэффициент при x^i в разложении $(1 - 4x)^{-1/2}$, а $\binom{2t-2i}{t-i}$ - коэффициент при x^{t-i} в $(1 - 4x)^{-1/2}$. Значит левая часть (5) - это коэффициент при x^t в произведении $(1 - 4x)^{-1/2} \cdot (1 - 4x)^{-1/2}$. Но $(1 - 4x)^{-1/2} \cdot$ $\cdot(1 - 4x)^{-1/2} = (1 - 4x)^{-1} = 1 + 4x + (4x)^2 + \ldots + (4x)^t + \ldots$

Отсюда получаем тождество (5).

<u>Теорема 3.</u> Пусть дана рекуррентная последовательность

$$F(n) = F(n - 1) + F(n - 2)\ ,\quad F(0) = a,\quad F(1) = b$$

Тогда функция

$$\Phi(x) = \frac{a + (b-a)x}{1 - x - x^2} \tag{6}$$

является (обыкновенной) производящей функцией для чисел F(n).

Напишем систему равенств

$$F(0) = a$$
$$F(1) = b$$
$$F(2) = F(1) + F(0)$$
$$\ldots$$
$$F(n) = F(n - 1) + F(n - 2)$$

Умножаем i-ое уравнение на x^i и полученные уравнения сложим. Слева получим функцию Φ(x). Справа получаем в первом столбце $x\Phi(x) - xa + a$, во втором столбце $xb + x^2\Phi(x)$.

Следовательно, $\Phi(x) = x\Phi(x) - xa + a + xb + x^2\Phi(x)$

или $(1 - x - x^2)\Phi(x) = a + (b - a)x$, откуда и следует (6). ♦

Аналогичным образом производящие функции применяются для решения произвольного линейного рекуррентного соотношения.

Пусть дано линейное рекуррентное соотношение

$$u_{n+k} = a_1u_{n+k-1} + \dots + a_ku_n.$$

Отсюда следует, что справедливы соотношения:

$$u_k = a_1u_{k-1} + \dots + a_ku_0$$

$$u_{k+1} = a_1u_k + \dots + a_ku_1$$

$$\cdots$$

$$u_{n+k} = a_1u_{n+k-1} + \dots + a_ku_n$$

Пусть $F(x) = \sum_{n=0} u_nx^n$ – соответствующая производящая функция. Тогда имеем

$$\begin{aligned}
F(x) = u_0+u_1x+ \dots +u_{k-1}x^{k-1} &+a_1(u_{k-1}x^k+u_kx^{k+1}+ \dots)+\\
&+a_2(u_{k-2}x^k+u_{k-1}x^{k+1}+ \dots)+\\
&\cdots\\
&+a_k(u_0x^k+u_1x^{k+1}+ \dots) =\\
= u_0+u_1x+ \dots +u_{k-1}x^{k-1} &+a_1x(u_{k-1}x^{k-1}+u_kx^k+ \dots)+\\
&+a_2x^2(u_{k-2}x^{k-2}+u_{k-1}x^{k-1}+ \dots)+\\
&\cdots\\
&+a_kx^k(u_0+u_1x+ \dots) =\\
= u_0+u_1x+ \dots +u_{k-1}x^{k-1} &+a_1x(F(x) - u_0 - u_1x - \dots - u_{k-2}x^{k-2})+\\
&+a_2x(F(x) - u_0 - u_1x - \dots - u_{k-3}x^{k-3})+\\
&\cdots\\
&+a_kx^k(F(x)).
\end{aligned}$$

Следовательно, справедливо соотношение

$F(x)(1 - a_1x - a_2x^2 - \dots - a_kx^k) = G(x)$, где

$G(x)$ – многочлен степени не выше $k - 1$, определенный начальными условиями.

Отсюда следует равенство

$$F(x) = \frac{G(x)}{1 - a_1x - a_2x^2 - \dots - a_kx^k}$$

<u>Теорема 4.</u> Пусть дано рекуррентное соотношение

$$T_n = T_0 \cdot T_{n-1} + T_1 \cdot T_{n-2} + \dots + T_{n-1} \cdot T_0, \quad T_0 = 1 \tag{7}$$

Тогда его решением является $T_n = \frac{1}{n+1}\binom{2n}{n}$.

♦ Составим производящую функцию

$$f(x) = T_0 + T_1x + T_2x^2 + \ldots + T_nx^n + \ldots$$

и положим

$$F(x) = x\,f(x) = xT_0 + T_1x^2 + \ldots + T_nx^{n+1} + \ldots$$

и возведем F(x) в квадрат.

Имеем

$$F^2(x) = T_0^2x^2 + (T_0 \cdot T_1 + T_1 \cdot T_0)x^3 + \ldots + (T_0 \cdot T_{n-1} + T_1 \cdot T_{n-2} + \ldots\ T_{n-1} \cdot T_0)x^{n+1} + \ldots$$

Откуда, используя рекуррентное соотношение, получаем

$$F^2(x) = T_1x^2 + T_2x^3 + \ldots + T_nx^{n+1} + \ldots = F(x) - T_0 \cdot x$$

Значит $F^2(x) - F(x) + x = 0$

Решая данное уравнение относительно F(x), получаем

$$F(x) = \frac{1-(1-4x)^{1/2}}{2}$$

(Знак “+” не годится, поскольку F(0) = 0).

По формуле бинома имеем коэффициент u_n при x^n :

$$u_n = \frac{\frac{1}{2}(\frac{1}{2}-1)\cdots(\frac{1}{2}-n+1)(-4x)^n(-\frac{1}{2})}{n!} = \frac{1\cdot 3\cdots(2n-3)\cdot 2^{n-1}}{n!} =$$

или, умножая и деля на (n - 1) !, получаем

$$= \frac{1\cdot 3\cdots(2n-3)\cdot 2\cdot 4\cdots(2n-2)}{n!(n-1)!} = \frac{(2n-2)!}{n!(n-1)!}$$

Поскольку при $|x| < \frac{1}{4}$ ряд для F(x) сходится, то все производимые операции законны и значит $T_n = u_{n+1}$.

Следовательно,

$$T_n = \frac{1}{n+1}\binom{2n}{n}\ ♦$$

Полученные числа T_n называются числами Каталана. Они появляются во многих комбинаторных задачах. Приведем таблицу первых значений чисел T_n.

n	0	1	2	3	4	5	6	7
T_n	1	1	2	5	14	42	132	429

Таблица. Числа Каталана

Пример. Найти число способов вычисления неассоциативного произведения $x_1\, x_2 \ldots x_n$ с помощью бинарных умножений.

Решение. Пусть u_n - число способов вычисления данного произведения.

Имеем $x_1\, x_2 = (x_1\, x_2)$ и $u_2 = 1$

$x_1\, x_2\, x_3 := ((x_1\, x_2)\, x_3), (x_1\, (x_2\, x_3))$ и $u_3 = 2$

Произведение $x_1\, x_2 \ldots x_n$ вычисляется на последнем этапе как произведение результата вычисления умножения первых r символов и соответствующего результата для последних n - r символов для некоторого r, т.е.

$$x_1 \ldots x_n = (x_1 \ldots x_r)(x_{r+1} \ldots x_n)$$

Первые r символов перемножаются u_r способами, последние n - r u_{n-r} способами. В итоге можно написать соотношение

$$u_n = u_1\, u_{n-1} + u_2\, u_{n-2} + \ldots + u_{n-1}\, u_1 \qquad (8)$$

Положим $u_1 = 1$.

Аналогично тому, как сходное соотношение решалось в теореме (4), образуем производящую функцию

$$f(x) = u_1\, x + u_2\, x^2 + \ldots + u_n\, x^n + \ldots$$

Возвышая в квадрат f(x) и пользуясь соотношением (8) имеем

$$f^2(x) = f(x) - x$$

Решая квадратное уравнение, получаем

$$f(x) = \frac{1-(1-4x)^{1/2}}{2} \qquad \text{(т.к. } f(0) = 0\text{, то берем знак минус)}$$

Отсюда получаем, что

$$u_n = \frac{(2n-2)!}{n!(n-1)!} = \frac{1}{n}\binom{2n-2}{n-1}$$

Широкая область приложений производящих функций - получение формул обращения. Рассмотрим примеры.

Теорема 5. Пусть имеем две последовательности $\{u_n\}$ и $\{v_n\}$, связанные соотношением для некоторого натурального t

$$u_n = \sum_{k=0}^{n} (-1)^k \binom{t}{k} v_{n-k} \qquad (9)$$

тогда

$$v_n = \sum_{k=0}^{n} \binom{t+k-1}{k} u_{n-k} \qquad (10)$$

Обратно равенство (10) влечет (9).

♦ Рассмотрим производящие функции

$$u(x) = \sum_{n=0}^{\infty} u_n x^n \quad \text{и } v(x) = \sum_{n=0}^{\infty} v_n x^n$$

и рассмотрим тождество

$$(1 - x)^t = \sum_{k=0}^{t} (-1)^k \binom{t}{k} x^k$$

Отсюда

$$v(x)(1 - x)^t \quad \text{дает} \quad R(x) = a_0 + a_1 x + \ldots + a_n x^n + \ldots$$

где $a_n = \sum_{k=0}^{n} (-1)^k \binom{t}{k} v_{n-k}$ согласно (9) и значит $v(x)(1 - x)^t = u(x)$

Следовательно, $v(x) = u(x)\,(1 - x)^{-t}$

Поскольку $(1 - x)^{-t} = \sum_{k=0}^{\infty} \frac{(-t)(-t-1)\cdots(-t-k+1)}{k!}(-x)^k = \sum_{k=0}^{\infty} \binom{t+k-1}{k} x^k$

то $v_n = \sum_{k=0}^{n} \binom{t+k-1}{k} u_{n-k}$ ♦

<u>Теорема 6.</u> Пусть имеем две последовательности $\{a_n\}$ и $\{b_n\}$, связанные соотношением

$$b_n = \sum_{k=0}^{n} \binom{n}{k} a_{n-k} \qquad (11)$$

Тогда

$$a_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} b_{n-k} \qquad (12)$$

Обратно, равенство (12) влечет (11).

♦ Рассмотрим экспоненциальные производящие функции

$$A(x) = \sum_{n=0}^{\infty} \frac{a_n}{n!} x^n \quad \text{и} \quad B(x) = \sum_{n=0}^{\infty} \frac{b_n}{n!} x^n$$

и возьмем ряд

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots + \frac{x^n}{n!} + \ldots$$

Рассмотрим произведение

$$e^x A(x) = F(x) = f_0 + \frac{f_1}{1!} x + \frac{f_2}{2!} x^2 + \ldots + \frac{f_n}{n!} x^n + \ldots$$

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

откуда

$$f_n = \sum_{k=0}^{n} \binom{n}{k} a_{n-k} = b_n$$

Значит $F(x) = B(x) = e^x A(x)$

Откуда $A(x) = e^{-x} B(x)$

Имеем $e^{-x} = \sum_{k=0}^{\infty} (-1)^k \frac{x^k}{k!}$. Следовательно, или $\frac{a_n}{n!} = \sum_{k=0}^{n} (-1)^k \frac{1}{k!} \frac{b_{n-k}}{(n-k)!}$

Утверждения теорем 5 и 6 называются формулами обращения. ♦

§ 4. Обращение Мебиуса.

1. Напомним сначала определение важной теоретико-числовой функции Мебиуса:

$$\mu(n)=\begin{cases} 1, \text{ если } n = 1 \\ 0, \text{ если существует простое число } p,\ p^2 \mid n \\ (-1)^k, \text{ если } n = p_1\dots p_k \text{ - произведение } k \text{ различных простых множителей.}\end{cases}$$

Докажем основное свойство функции Мебиуса:

<u>Теорема 1.</u>

$$\sum_{d|n}\mu(d)=\begin{cases}1, \text{Њ–‘Џ}\ n=1\\ 0, \text{Њ–‘Џ}\ n>1\end{cases} \qquad (1)$$

♦ Если n = 1, то единственный делитель d = 1 и (1) верно, т.к. $\mu(1) = 1$.

Пусть теперь n > 1. Представим его в виде

$$n = p_1^{s_1}p_2^{s_2}\dots p_k^{s_k},$$

где p_i, $i \in \overline{1,k}$ - простые числа, s_i - их степени. Если d - делитель n, то $d = p_1^{d_1}p_2^{d_2}\dots p_k^{d_k}$, где $0 \le d_i \le s_i$, $i \in \overline{1,k}$. Если $d_i > 1$ для некоторого $i \in \overline{1,k}$, то $\mu(d) = 0$. Значит в (1) нужно рассмотреть только такие d, для которых $d_i \le 1$, $\forall\ i \in \overline{1,k}$. Каждый такой делитель состоит из произведения r различных простых чисел, где $r \in \overline{1,k}$, причем его вклад в сумму (1) равен $(-1)^r$ и всего их $\binom{k}{r}$. Таким образом, получаем

$$\sum_{d|n}\mu(d) = 1-\binom{k}{1}+\ldots+(-1)^k\binom{k}{k} = 0.\ ♦$$

<u>Теорема 2.</u> (Формула обращения Мебиуса). Пусть f(n) и g(n) - функции натурального аргумента. Тогда равенство

$$g(n) = \sum_{d|n} f(d) \qquad (2)$$

справедливо тогда и только тогда, когда справедливо равенство

$$f(n) = \sum_{d|n}\mu(d)g(\tfrac{n}{d}) \qquad (3)$$

♦ Пусть (2) справедливо для любого n. Тогда

$$g(\tfrac{n}{d}) = \sum_{d' \mid \frac{n}{d}} f(d')$$

Подставляя в правую часть (3), получаем

$$\sum_{d \mid n} \mu(d) g(\tfrac{n}{d}) = \sum_{d \mid n} \mu(d) \cdot \sum_{d' \mid \frac{n}{d}} f(d')$$

Двойное суммирование справа проводится по всем парам d, d′ , таким, что

$d \cdot d' \mid n$. Если выбрать d′, то d будет пробегать все делители $\dfrac{n}{d'}$. Таким образом

$$\sum_{d \mid n} \mu(d) g(\tfrac{n}{d}) = \sum_{d' \mid n} f(d') \cdot \sum_{d' \mid \frac{n}{d'}} \mu(d')$$

Но согласно (1) имеем $\sum_{d' \mid \frac{n}{d'}} \mu(d') = \begin{cases} 0 & \text{при} \quad n > d' \\ 1 & \text{при} \quad n = d' \end{cases}$

Значит, равенство (3) установлено. Пусть теперь (3) справедливо для любого n. Тогда $\sum_{d \mid n} f(d) = \sum_{d \mid n} \sum_{d' \mid d} \mu(d') g(\tfrac{d}{d'})$, $d'' = d / d'$ - является делителем n и двойная сумма может быть переписана в виде

$$\sum_{d'' \mid n} \sum_{d' \mid n/d''} \mu(d') g(d'') = \sum_{d'' \mid n} g(d'') \cdot \sum_{d' \mid n/d''} \mu(d')$$

Согласно (1) последняя сумма превращается в единицу в случае $d'' = n$, в остальных случаях она есть ноль. Это доказывает (2). ♦

2. Рассмотрим приложение обращения Мебиуса.

Пусть дан алфавит A из s букв. Имеется s^n слов длины n в данном алфавите. Для каждого слова $w_0 = a_1 a_2 \ldots a_n$ можно определить n - 1 слов $w_1 = a_2 a_3 \ldots a_n a_1$, $w_2 = a_3 a_4 \ldots a_1 a_2$, … , $w_{k-1} = a_n a_1 \ldots a_{n-1}$, , получаемых один из другого циклическими сдвигами. На множестве всех s^n слов введем отношение эквивалентности: два слова объявим эквивалентными, если один из другого получается циклическим сдвигом. Нас будут интересовать число классов, которые содержат точно n слов. Такая задача возникает в теории синхронизирующих кодов.

Будем называть слово w вырожденным, если класс эквивалентности, содержащий w, состоит из менее, чем n слов. Назовем w периодическим, если существует слово u и натуральное число m, такое, что w = u u … u (m раз).

Теорема 3. Слово w периодическое тогда и только тогда, когда оно вырождено.

♦ Ясно, что если w периодическое, то оно вырождено. Пусть w вырождено. Пусть p - минимальное целое, такое, что $w = w_p$. Тогда если $w = a_1 a_2 \dots a_n$, то $w_p = a_{1+p} a_{2+p} \dots a_{n+p}$ (индексы по модулю n). Отсюда получаем, что в качестве u можно взять $a_1 a_2 \dots a_p$, а в качестве $m = \frac{n}{p}$. (Легко видеть, что $p \mid n$). ♦ Обозначим через M(d) - число квадратов, которые содержат d слов. Из предыдущего имеем $d \mid n$. Таким образом, справедлива формула $\sum_{d \mid n} dM(d) = s^n$.

Применим формулу обращения Мебиуса для случая $g(n) = s^n$, $f(d) = dM(d)$. Тогда получаем

$$nM(n) = \sum_{d \mid n} \mu(d) s^{n/d}$$

или

$$M(n) = \frac{1}{n} \sum_{d \mid n} \mu(d) s^{n/d}$$

Таким образом, M(n) - интересующее нас число. Если n = p - простое число, то

$$M(p) = \frac{1}{p}(s^p - s)$$

Имеется мультипликативный вариант обращения Мебиуса. Справедлива

<u>Теорема 4.</u> Пусть f(n) и g(n) - функции натурального аргумента, связанные соотношениями

$$f(n) = \prod_{d \mid n} g(d) \qquad (4)$$

Тогда
$$g(n) = \prod_{d \mid n} f(d)^{\mu(n/d)} \qquad (5)$$

и обратно, из (5) следует (4).

Используя формулу обращения Мебиуса, можно решить важную в практическом отношении задачу о числе неприводимых многочленов фиксированной степени над конечным полем. Пусть GF(q) - поле из q элементов и m - натуральное число. Тогда для числа $\Phi_m(q)$ неприводимых многочленов над полем GF(q) справедлива формула

$$\Phi_m(q) = \frac{1}{m} \sum_{d \mid n} \mu(m/d) q^d \qquad (6)$$

Приведем таблицу нескольких первых значений функции $\Phi_m(2)$

m	1	2	3	4	5	6
$\Phi_m(2)$	2	1	2	3	6	9

§ 5. *Перманенты и их применение к перечислительным задачам.*

1. Для решения многих комбинаторных задач используются перманенты. Рассмотрим числовую матрицу

$$A = (a_i, j), \quad i = \overline{1, n}, \quad j = \overline{1, m}, \; n \le m$$

<u>Перманент</u> матрицы A (обозначение - per A) определяется равенством

$$\text{per } A = \sum_{(j_1, \ldots, j_n)} a_{1j_1} \cdot a_{2j_2} \cdot \ldots \cdot a_{nj_n} \qquad (1)$$

где суммирование производится по всем n-перестановкам из m элементов 1, 2, , m. Другими словами, перманент матрицы равен сумме произведений элементов, взятых по одному из каждой строки и разных столбцов.

Из формулы (1) следуют некоторые очевидные свойства перманента, аналогичные свойствам определителя для квадратных матриц.

1. Если одна из строк $(n \times m)$-матрицы A $(n \le m)$ состоит из нулей, то per A = 0. При n = m то же верно и для столбцов.

2. При умножении всех элементов одной из строк матрицы A на некоторое число значение перманента A умножается на то же число.

3. Перманент не меняется при перестановке ее строк и столбцов.

Обозначим через A_{ij} - матрицу, полученную из A вычеркиванием i-ой строки и j-го столбца.

4. Справедлива формула разложения перманента по i-ой строке

$$\text{per } A = a_{i1} \text{ per } A_{i1} + a_{i2} \text{ per } A_{i2} + \ldots + a_{im} \text{ per } A_{im} \quad (2)$$

таким образом, многие свойства перманентов аналогичны свойствам определителей. Однако, основное свойство определителей $\det(A \cdot B) = \det A \cdot \det B$ не выполняется для перманентов, и это обстоятельство сильно затрудняет их вычисление.

Например, $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}$

$$\text{per} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = 2, \ \text{per} \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix} = 8$$

Однако, $4 = \text{per} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \text{per} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \neq \text{per} \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix} = 8 \qquad (3)$

рассмотрим одно из важнейших применений понятия перманента в комбинаторных задачах. Пусть $X = \{x_1, \ , x_m\}$ - конечное множество, а $X_1, \dots , X_n$ - система подмножеств множества X. Набор элементов $x_1, \ , x_n$ называется системой различных представителей или трансверсалью для множеств $X_1, \dots , X_n$, если выполнены условия

$$x_i \in X_i, \qquad i = \overline{1, n} \qquad (4)$$

$$x_i \neq x_j \qquad \text{при } i \neq j.$$

При этом говорят, что элемент x_i представляет множество X_i . Необходимость нахождения системы различных представителей возникает при решении многих прикладных задач. Рассмотрим следующую задачу кодирования. Пусть имеется некоторое предложение, т.е. упорядоченный набор слов в некотором алфавите. Требуется закодировать данное предложение так, чтобы каждому слову ставилась в соответствие одна буква, причем эта буква должна входить в состав этого слова, а разным словам должны соответствовать разные буквы.

Пример: Предложение abc abd abe cde cde можно закодировать как abecd. В то же время, предложение ab ab bc abc bcd не может быть закодировано подобным образом, поскольку первые четыре слова в совокупности содержат только три буквы. Для системы множеств $X_1, \dots , X_n$ определим матрицу инцидентности $A = (a_{ij})$, $i = \overline{1, n}$, $j = \overline{1, m}$, где

$$a_{ij} = \begin{cases} 1, \text{ если } x_i \in X_i \\ 0, \text{ в противном случае.} \end{cases} \qquad (5)$$

Справедлива

Теорема 1. Пусть $A = (a_{ij})$, $i = \overline{1, n}$, $j = \overline{1, m}$, $(n \le m)$ матрица инцидентности множеств $X_1, \dots , X_n$, где $X_i \subseteq X$, $i = \overline{1, n}$, $X = \{x_1, \dots , x_m\}$. Тогда для числа систем различных представителей $R(X_1, \dots , X_n)$ множеств $X_1, \dots , X_n$ справедливо равенство

$$R(X_1, \dots , X_n) = \operatorname{per} A \qquad (6)$$

♦ Действительно, поскольку в матрице A элемент $a_{ij} = 1$, если $x_j \in X_i$ и $a_{ij} = 0$, если $x_j \notin X_i$, то набор $(x_{i_1}, x_{i_2}, \dots, x_{i_n})$ элементов X является системой различных представителей для $X_1, \dots , X_n$ в том и только в том случае, когда $a_{1i_1}, a_{2i_2}, \dots, a_{ni_n} = 1$ и элементы $a_{1i_1}, \dots, a_{ni_n}$ находятся в разных столбцах матрицы A. Суммируем числа $a_{1i_1}, \dots, a_{ni_n}$ по всем n-перестановкам элементов 1, 2, … , m. Тогда получим с одной стороны число систем различных представителей для $X_1, \dots , X_n$, а с другой - значение перманента матрицы A. ♦

<u>Следствие.</u> Система различных представителей для $X_1, \dots, X_n$ существует тогда и только тогда, когда для соответствующей матрицы инциденция A выполнено:

$$\operatorname{per} A > 0 \qquad (7)$$

Поскольку в формуле (1) m(m - 1) … (m - n +1) членов, то вычисление перманента на основе определения затруднительно. Приведем для этой цели общую формулу.

2. Ограничимся рассмотрением квадратных числовых матриц $A = (a_{ij})$, $i, j = \overline{1, n}$.

Тогда $\operatorname{per} A = \sum\limits_{(i_1,\dots,i_n)} a_{1i_1} \cdot a_{2i_2} \cdots a_{ni_n}$

где сумма распространяется по всем перестановкам $i_1, \dots, i_n$ элементов

1, 2, … , n. Применим формулу включения-исключения для вычисления перманента матрицы A. Каждому набору $i_1, \dots, i_n$ поставим в соответствие <u>вес</u>, равный $a_{1i_1}, \dots, a_{ni_n}$.

Значит перманент A - это сумма весов тех наборов, которые соответствуют перестановкам. Введем n свойств $P_1, \dots, P_n$ на множестве всех наборов $i_1, i_2, \dots, i_n$ из 1, 2, … , n, где свойство P_i означает, что в наборе $i_1, \dots, i_n$ нет элемента i. Таким образом, перманент A - это сумма весов наборов $i_1, \dots, i_n$, не обладающих ни одним из свойств $P_1, \dots, P_n$. Осталось определить сумму весов $W(P_{i_1}, \dots, P_{i_k})$ наборов, обладающих k свойствами

$P_{i_1}, \dots, P_{i_k}$. Имеем для суммы весов W(0) всех наборов $i_1, \dots, i_k$.

$$W(0) = \sum_{i_1,\dots,i_n} a_{1i_1}, \dots, a_{ni_n} = (a_{11} + \dots + a_{1n})(a_{21} + \dots + a_{2n}) \cdots (a_{n1} + \dots + a_{nn}) \qquad (8)$$

$$W(N(P_i)) = \sum_{\substack{i_1,\dots,i_n \\ \neq i}} a_{1i_1}, \dots, a_{ni_n} = (a_{11} + \dots + \hat{a}_{1i} + \dots + a_{1n}) \cdots (a_{n1} + \dots \hat{a}_{ni} + \dots + a_{nn}) \ (9)$$

где знак ^ над элементом матрицы A означает, что этот элемент следует опустить.

Аналогично для s_{ij} $(i < j)$ имеем

$$W(N(P_i, P_j)) = (a_{11} + \dots + \hat{a}_{1i} + \dots + \hat{a}_{1j} + \dots + a_{1n}) \cdots (a_{n1} + \dots \hat{a}_{ni} + \dots + \hat{a}_{nj} + \dots + a_{nn}) \ (10)$$

Теперь, используя формулу включения-исключения, получаем <u>формулу Райзера</u> для перманента A:

$$\operatorname{per} A = \prod_{i=1}^{n}(a_{i1} + \dots + a_{in}) - \sum_{i=1}^{n} \prod_{k=1}^{n}(a_{k1} + \dots + \hat{a}_{ki} + \dots + a_{kn}) + \dots +$$

$$+(-1)^s \sum_{1 \le i_1 < \dots < i_s \le n} \prod_{k=1}^{n}(a_{k1} + \dots + \hat{a}_{ki_1} + \dots + \hat{a}_{ki_s} + \dots + a_{kn}) + \cdots \qquad (11)$$

Вычисление перманента по формуле Райзера можно организовать так, что потребуется

$(2^n - 1)(n - 4)$ умножений и $(2^n - 2)(n + 1)$ сложений. Хотя эта величина растет быстро с ростом n, данная формула дает наиболее эффективный способ вычисления перманентов.

3. Выясним теперь вопрос об условиях равенства нулю перманента (0, 1)-матрицы. Ограничимся случаем квадратной матрицы.

<u>Теорема 2.</u> Пусть $A = (a_{ij})$, $i, j = \overline{1, n}$ - (0, 1)-матрица порядка n. Тогда per A= 0 в том и только в том случае, когда в A существует подматрица из нулей размера $s \times t$, где $s + t = n + 1$.

♦ Пусть такая нулевая подматрица в A существует. Поскольку перманент не меняется от перестановок строк и столбцов, то можно считать, что эта подматрица расположена в левом нижнем углу, т.е.

$$A = \begin{pmatrix} B & C \\ O & D \end{pmatrix}$$

где O - $(s \times t)$ - матрица из нулей, подматрица B имеет размер $(n - s) \times t$. Любой член перманента A должен содержать по одному элементу из первых t столбцов. Поэтому, если искать положительный член перманента, то элементы этих столбцов должны принадлежать попарно различным строкам с номерами 1, 2, … , n - s. Однако $n - s = t - 1 < t$ и поэтому данное условие выполнить нельзя, т.е. per A = 0.

Пусть теперь per A = 0. Доказательство теоремы проводим индукцией по n. При n = 1 утверждение очевидно (A = (0)). Пусть оно справедливо для всех порядков, меньших n. Если A - нулевая матрица порядка n, то утверждение очевидно. Если A - не нулевая матрица, то пусть $a_{ij} = 1$. Запишем разложение A по строке i:

$$\text{per } A = a_{i1}A_{i1} + \ldots + a_{in}A_{in}$$

Поскольку per A = 0, то per $A_{ij} = 0$. Но A_{ij} имеет размер $(n - 1) \times (n - 1)$ и по предположению индукции для нее существует подматрица из нулей размера $s_1 \times t_1$, причем $s_1 + t_1 = n - 1 + 1 = n$. Переставим строки и столбцы так, чтобы эта нулевая подматрица оказалась в нижнем левом углу:

$$A \to B = \begin{pmatrix} C & E \\ O & D \end{pmatrix}$$

где O - нулевая подматрица размера $s_1 \times t_1$, $s_1 + t_1 = n$, C - имеет размер $(n - s_1) \times t_1$, D - имеет размер $s_1 \times (n - t)$. Значит, матрицы C и D - квадратные и имеют порядок $(t_1 \times t_1)$ и $(s_1 \times s_1)$ соответственно. Согласно определению перманента имеем per B = per A и , per B = per C · per D и поэтому из per A = 0 следует, что либо per C = 0, либо per D = 0. Пусть per C = 0. По предположению индукции в C найдется нулевая подматрица размера

$u \times v$, где $u + v = t_1 + 1$. Пусть она расположена в строках с номерами $i_1, \dots , i_u$ и столбцами с номерами $j_1, \dots , j_v$. Рассмотрим подматрицу B, состоящую из строк $i_1, \dots , i_u, t_1+ 1, \dots , n$ и столбцов $j_1, \dots , j_v$. Это нулевая подматрица размера $(u + n - t_1) \times v$, где $u + n - t_1 + v = n + +1$. Итак, в матрице B указана нулевая подматрица размера $s \times t$, где $s + t = n + 1$. Так как матрицы A и B отличаются перестановкой строк и столбцов, то теорема доказана. ♦

Рассмотрим теперь важный частный случай матрицы A. Обозначим через A(k, n) - матрицу из элементов 0,1 размера $n \times n$ с k единицами к каждой строке и каждом столбце ($k > 0$).

<u>Теорема 3.</u> Для любой матрицы A(k, n) справедливо per A(k, n) > 0.

♦ Допустим противное, что per A(k, n) = 0. Тогда по теореме 2 существует нулевая подматрица размера $s \times t$, где $s + t = n + 1$. Тогда, переставляя строки и столбцы матрицы A(k, n) получим матрицу

$$\begin{pmatrix} B & C \\ O & D \end{pmatrix}$$

где O - нулевая $(s \times t)$-матрица.

Подсчитаем число единиц в матрицах B и D. Поскольку A(k, n) имеет k единиц в каждой строке и каждом столбце, то в каждом столбце B и каждой строке D имеется точно k единиц. Всего в A(k, n) имеется $n \cdot k$ единиц, поэтому $nk \geq tk + sk = (t + s)n$. Таким образом, $n \geq t + s$, что невозможно, т.к. $s + t = n + 1$ Из данного противоречия следует справедливость утверждения. ♦

Аналогично доказывается

<u>Теорема 3а.</u> Пусть A - (0,1)-матрица размера $n \times m$ ($n \leq m$). Тогда perA = 0 в том и только в том случае, когда содержит нулевую подматрицу размера $s \times t$, где $s+t=m+1$.

4. Рассмотрим теперь приложение рассматриваемых вопросов к построению латинских квадратов. <u>Латинским $(n \times m)$-прямоугольником</u> над множеством $X=\{x_1,\dots,x_m\}$ называется $(n \times m)$ -матрица из элементов X, в которой каждая строка есть n-перестановка X, а каждый столбец есть m-перестановка множества X. При n=m латинский прямоугольник называется <u>латинским квадратом.</u>

Ясно, что при n=1 число латинских $1 \times m$ прямоугольников равно m!. При n=2 после того, как выбрана первая строка, в качестве второй можно взять любую перестановку, противоречащую выбранной. Число таких перестановок D_m, поэтому число $2 \times m$ - латинских прямоугольников равно $m! \cdot D_m$.

Возникает естественный вопрос в связи с индуктивным построением латинских квадратов. Пусть мы построили латинский (n×m)-прямоугольник (n<m). Можно ли его расширить до ((n+1)×m) -прямоугольника добавлением (n+1)-й строки?

Справедлива

Теорема 4. Всякий латинский (n×m) -прямоугольник n<m можно расширить до латинского квадрата (n×n) добавлением m-n новых строк.

♦Пусть $X=\{x_1,\dots,x_m\}$ и L- латинский (n×m)-прямоугольник с элементами из X. Рассмотрим набор множеств $A_1,\dots,A_m$ где A_i - элементы i -го столбца латинского прямоугольника L. Пусть A - матрица инцидентности системы множеств $A_1,\dots,A_m$. Она имеет размер m×m , и каждая строка матрицы A содержит точно n единиц, поскольку $|A_i| = n$, $i=\overline{1,m}$. Каждый элемент $x_i \in X$ может появиться в столбцах L не более m раз, иначе нашлась бы строка, в которой этот элемент встретится дважды. Общее число элементов L равно m·n, поэтому каждый элемент $x_i \in X$ появляется в столбцах точно n раз. Отсюда следует, что и каждый столбец матрицы A содержит точно n единиц. Рассмотрим теперь матрицу $\overline{A}$, полученную заменой каждой единицы на нуль и каждого нуля на единицу. Матрица $\overline{A}$ есть матрица инциденций системы множеств $X_1, \dots, X_n$, где $X_i = X \setminus A_i$, $i=\overline{1,m}$. Она содержит по m - n единиц в каждой строке и в каждом столбце. По теореме 3 per $\overline{A} > 0$. Пусть $a_{i1} \dots a_{mi_m} \neq 0$. Тогда имеем $x_{i_1} \in X_1,\dots,x_{i_m} \in X_m$ и все элементы $x_{i_1},\dots,x_{i_m}$ попарно различны. Строка $x_{i_1},\dots,x_{i_m}$ может быть взята в качестве (n + 1)-ой для латинского (n × m)-прямоугольника L. Продолжая эту процедуру, получим латинский квадрат. ♦

Обозначим ℓ_n - число латинских квадратовпорядка n, с элементами из множества X = {1, 2, … , n}, у которых элементы первого столбца и первой строки идут в естественном порядке. Приведем таблицу нескольких известных значений числа ℓ_n :

n	1	2	3	4	5	6	7	8
ℓ_n	1	1	1	4	56	9408	16942080	535281401856

5. Матрица A = (a_{ij}) размера n × n с действительными, неотрицательными элементами называется дважды стохастической, если

$$\sum_{j=1}^{n} a_{ij} = 1$$

для всех $\quad i \in \overline{1, n}$ и

$$\sum_{i=1}^{n} a_{ij} = 1$$

для всех $\quad j \in \overline{1, n}$

Дважды стохастические матрицы играют большую роль в теории вероятностей. С перманентами таких матриц связана знаменитая проблема Ван дер Вардена, поставленная им в 1926 году: 1. Доказать, что для любой дважды стохастической матрицы A справедливо $\quad \text{per } A \geq \frac{n!}{n^n}$

2. Равенство достигается лишь для $(n \times n)$-матрицы $J = (1/n)$, все элементы которой равны $1/n$.

Эта проблема была положительно решена в 1980 году.

Упражнения

1. Найти число r-мерных наборов чисел 0, 1, 2, 3, в которых каждое число 1, 2, 3 появится хотя бы один раз.

Ответ: $4^r - 3 \cdot 3^r + 3 \cdot 2^r - 1$

2. Пусть $a_1, a_2, \ldots, a_n$ - целые неотрицательные числа. Доказать соотношение

$$\text{Max}(a_1, a_2, \ldots, a_n) = \sum_{i=1}^{n} a_i - \sum_{i<j} \text{Min}(a_i a_j) + \ldots + (-1)^{n-1} \text{Min}(a_1, \ldots, a_n)$$

3. Решить рекуррентное уравнение

$$a_n + 6a_{n-1} + 12a_{n-2} + 8a_{n-3} = 0$$

$$a_0 = 1,\ a_1 = -2,\ a_2 = 8$$

Ответ: $a_n = \left(\frac{n^2}{2} - \frac{n}{2} + 1\right)(-2)^n$

4. Вычислить перманент $(n \times n)$-матрицы

$$\begin{pmatrix} 1\cdot 1 & 1\cdot 2 & \dots & 1\cdot n \\ 2\cdot 1 & 2\cdot 2 & \dots & 2\cdot n \\ \dots & \dots & \dots & \dots \\ n\cdot 1 & n\cdot 2 & \dots & n\cdot n \end{pmatrix}$$

Ответ: $(n!)^3$

ГЛАВА III. ВВЕДЕНИЕ В ТЕОРИЮ ГРАФОВ.

§ 1. Основные понятия теории графов.

1. Граф G(V,E) - комбинаторный объект, состоящий из двух конечных множеств: V - называемого множеством вершин и множества пар элементов из V, т.е. $E \subseteq V \times V$, называемого множеством ребер, если пары неупорядочены, и множеством дуг, если пары упорядочены. В первом случае граф G(V,E) называется <u>неориентированным,</u> во втором <u>ориентированным.</u> Если $e = (v_1, v_2)$,

$e \in E$, то говорят, что ребро e соединяет вершины v_1, v_2, если $v_1 = v_2$, то ребро e называется петлей. Две вершины v_1, v_2 называются смежными, если существует соединяющее их ребро. Аналогично, два различных ребра смежны. если они имеют общую вершину.

<u>Степенью</u> вершины v называется число ребер d(v), инцидентных ей, при этом петля учитывается дважды. В случае ориентированного графа различают степень $d_0(v)$ по выходящим дугам и $d_i(v)$ - по входящим.

<u>Путь</u> - это последовательность ребер $e_1, e_2, \dots, e_m$, такая, что e_i, e_{i+1} имеют общую вершину. Число ребер называется <u>длиной</u> пути. Если ни одна из вершин не появляется более одного раза, то путь называется <u>простым.</u> Ясно, что в простом пути ни одно ребро не используется дважды.

Путь называется <u>циклом</u>, если его начальная вершина совпадает с конечной, простым циклом, если это не выполняется для других вершин.

В случае ориентированного графа, если путь проходит в направлении дуг, он называется ориентированным. Аналогично определяется ориентированный цикл.

Граф называется <u>связным</u>, если для любых двух вершин существует путь, их соединяющий. Ориентированный граф называется сильно связным, если для любых двух вершин существует ориентированный путь, их соединяющий. Для ориентированного графа определяем скелетный граф, как неориентированный граф, полученный снятием ориентации исходного графа.

Примеры графов:

1. <u>Полный граф</u> K_n. Это граф на n вершинах, у которого смежны любые две различные вершины. Ясно, что граф K_n имеет $\binom{n}{2}$ ребер.

2. <u>Граф отображения</u> $F: X \to X$. Это ориентированный граф с множеством вершин X, при этом вершины x_i и x_j соединяются дугой, если $x_j = F(x_i)$.

3. Двудольные графы. Это графы, у которых множество вершин можно разбить на два множества V_1, и V_2,, так что каждое ребро графа соединяет только некоторую вершину из V_1 с некоторой вершиной из V_2.

4. Граф единичного n-мерного куба B_n. Вершины графа - n-мерные двоичные наборы. Ребра соединяют вершины, отличающиеся одной координатой.

Факт 1. Любой граф содержит четное число вершин нечетной степени.

♦ Если граф G имеет x_i вершин степени i, то

$$x_1 + 2x_2 + \ldots + kx_k = 2\,|E| \qquad (1)$$

поскольку мы подсчитываем число концевых вершин ребер, а каждое ребро имеет точно две концевые вершины. Отсюда получаем, что $x_1 + x_3 + \ldots + x_{2S+1}$ - четное число. ♦

Число ребер в графе существенно влияет на его связность. Заметим, что любой граф можно разбить на связные части - компоненты связности, задав следующее отношение эквивалентности на множестве его вершин: две вершины эквивалентны, если существует путь из одной вершины в другую. Таким образом, связный граф состоит из одной компоненты.

Факт 2. Пусть G - граф с n вершинами и k компонентами. Тогда число m его ребер удовлетворяет неравенствам

$$n - k \le m \le \frac{(n-k)(n-k+1)}{2} \qquad (2)$$

♦ Нижнюю оценку доказывают индукцией по числу ребер в G. Если множество ребер пусто, то утверждение очевидно. Если в графе G число ребер минимально (скажем m_0), удаление любого ребра приводит к увеличению числа компонент на единицу. Значит, в графе k + 1 компонента и m_0 - 1 ребро. По предположению индукции , $m_0 - 1 \ge n - (k + 1)$, откуда $m_0 \ge n - k$. Для доказательства верхней оценки считаем каждую компоненту графа G полным графом. Если C_i и C_j - две компоненты с n_i и n_j вершинами ($n_i \ge n_j > 1$), то заменяя их на полные графы с $n_i + 1$ и $n_j - 1$ вершинами, мы, не меняя числа вершин, увеличиваем число ребер. Действительно,

$$\frac{(n_i+1)n_i}{2} + \frac{(n_j-1)(n_j-2)}{2} - \frac{n_i(n_i-1)}{2} - \frac{n_j(n_j-1)}{2} = n_i - n_j + 1 > 0$$

Значит, максимальное число ребер имеет граф G , у которого k - 1 изолированных вершин и компонента из полного графа на n - k + 1 вершинах. Отсюда и следует верхняя оценка. ♦

Следствие. Любой граф с n вершинами, имеющий более, чем $\frac{(n-1)(n-2)}{2}$ ребер, связан.

♦ Действительно, если граф имеет k компонент, то по предыдущему, число его ребер не превышает $\frac{(n-k)(n-k+1)}{2}$. Но неравенство $\frac{(n-1)(n-2)}{2} < \frac{(n-k)(n-k+1)}{2}$ справедливо только при k = 1. ♦

Убедимся теперь в том, что степени вершин существенно влияют на наличие циклов в графе.

Факт 3. Если степень каждой вершины графа G(V,E) не меньше двух, то G содержит цикл.

♦ Пусть v - произвольная вершина из V. Строим последовательность ребер (v,v_1), (v_1,v_2), … , выбирая v_1 смежной с v, … , v_{i+1} - смежной с v_i, и отличной от v_{i-1}. По условию вершина v_{i+1} существует. В силу конечности V на некотором шаге будет выбрана вершина, уже встретившаяся раньше. Пусть это v_k. Тогда часть последовательности ребер между вхождениями v_k образует цикл. ♦

2. Пусть G – связный граф, u, v – произвольные вершины. Определим d(u, v) – расстояние между u и v как длину кратчайшего пути из u в v. При этом полагаем d(u, v) = 0 при u = v.

Ясно, что введенное таким образом расстояние удовлетворяет аксиомам метрики:

1. $d(u, v) \geq 0$
2. $d(u, v) = 0 \Leftrightarrow u = v$
3. $d(u, v) = d(v, u)$
4. $d(u, v)+d(v, w) \geq d(u, w)$ (неравенство треугольника)

Для связного графа G диаметр d(G) определяется как

$$d(G) = \max_{u,v} d(u,v)$$

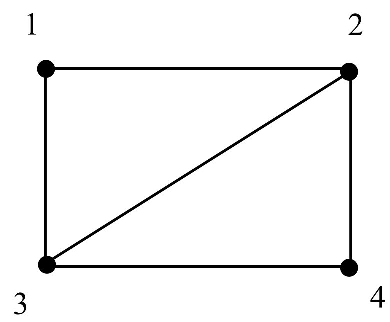
3. Графы $G_1(V_1, E_1)$ и $G_2(V_2, E_2)$ называются изоморфными, если существует биекция $f: V_1 \to V_2$, такая, что выполнено

$$(v_1, v_2) \in E_1 \Leftrightarrow (f(v_1), f(v_2)) \in E_2.$$

При этом f называется изоморфизмом графов G_1 и G_2. Изоморфизм графа G на себя называется автоморфизмом.

Пример 1. Следующие графы имеют только тождественные автоморфмы

Пример 2. Следующий граф имеет, кроме тождественного, автоморфизмы (1, 3) , (2, 4) , (13)(24).



Широко известна так называемая проблема изоморфизма графов, в которой для любых двух графов требуется установить, изоморфны они или нет. Для знакомства с результатами по данной проблеме следует обратиться к приведенному списку литературы.

4. Поскольку графы можно рассматривать как частные случаи бинарных отношений, то для них могут быть определены аналогичные операции. Укажем некоторые из них.

Пусть $G_1 + (V_1, E_1)$, $G_2 = (V_2, E_2)$ – два графа.

Объединение графов G_1 и G_2 есть граф, у которого $V = V_1 \cup V_2$, $E = E_1 \cup E_2$.

Соединение графов G_1+G_2 есть граф, у которого $V = V_1 \cup V_2$, $E = E_1 \cup E_2 \cup \{(v_1, v_2)\}$ для всех $v_1 \in V_1$, $v_2 \in V_2$.

Прямое произведение графов есть граф, у которого $V = V_1 \times V_2$, $((c_1, v_2),(v'_1, v'_2)) \in E \Leftrightarrow (v_1, v'_1) \in E_1$ и $(v_2, v'_2) \in E_2$.

<u>Пример.</u> Пусть даны графы отображений $f_1\colon V_1 \to V_1$, $f_2\colon V_2 \to V_2$. Тогда их прямое произведение соответствует отображению $f_1 \times f_2\colon V_1 \times V_2 \to V_1 \times V_2$, где $f_1 \times f_2(v_1, v_2) = (f_1(v_1), f_2(v_2))$.

Пусть f_1 и f_2 имеют ℓ_0^1 и ℓ_0^2 начальных вершин соответственно. Тогда $f_1 \times f_2$ будет иметь $\ell_0 = \ell_0^1 \cdot |v_2| + \ell_0^2 |v_1| - \ell_0^1 \cdot \ell_0^2$ начальных вершин.

5. Некоторые классы графов допускают характеристическое описание. В качестве примера приведем критерий двудольности графа (Кёниг, 1936 г.)

Теорема. Для двудольности графа необходимо и достаточно, чтобы он не содержал циклов нечетной длины.

▸ Пусть $G = (V, E)$ – двудольный граф, C – один из его циклов длины k. Фиксируем вершину $v_1 \in C$ и проходим цикл, начиная с v_1. Пусть это вершины $v_1, v_2, ..., v_k$. Поскольку концы каждого ребра лежат в разных долях, то k – четное число.

Пусть $G = (V, E)$ – связный и все его циклы четной длины. Определим разбиение $V = V_1 \cup V_2$ следующим образом: Фиксируем произвольную вершину $v_1 \in V$ и включаем ее в V_1. Теперь включаем $u \in V_1 \Leftrightarrow d(u, v_1)$ – четное число. Остальные вершины включаем в V_2.

Покажем, что граф G двудольный. Пусть, напротив, существует ребро (v', v''), где $v', v'' \in V_1$. Следовательно, $d(v_1, v')$, $d(v_1, v'')$ – четны. Ребро (v', v'') дает цикл нечетной длины, содержащий путь от v_1 к v', ребро (v', v''), путь от v'' к v_1. Аналогично показываем, что нет ребер (v', v''), $v', v'' \in V_2$. ◂

§ 2. Эйлеровы графы.

Эйлеровым путем графа $G(V,E)$ называется путь $e_1, e_2, \ldots, e_t$ такой, что каждое ребро появляется ровно 1 раз, т.е. $t = |E|$. Граф $G(V,E)$ называется эйлеровым, если он имеет замкнутый эйлеровый путь, и полуэйлеровым, если существует эйлеров путь, не являющийся замкнутым.

Теорема 1. Связный граф G является эйлеровым тогда и только тогда, когда каждая вершина G имеет четную степень.

♦ Предположим, что P является эйлеровым циклом в графе G. Тогда при всяком прохождении цикла через любую вершину графа используется одно ребро для входя и одно ребро для выхода. Поскольку каждое ребро используется один раз, то каждая вершина должна иметь четную степень. Обратное утверждение доказываем индукцией по числу ребер в графе G. Пусть граф G связен и степень каждой вершины четна. На основании Факта 3 граф содержит цикл C. Если C содержит каждое ребро, то все доказано. Если же нет, то удаляем из графа G все ребра, принадлежащие циклу C. Получаем новый граф G_1, возможно несвязный. Число ребер в G_1 меньше чем в G, и каждая вершина имеет четную степень. По индуктивному предположению в каждой компоненте графа G_1 имеется эйлеров цикл. В силу связности графа G каждая компонента графа G_1 имеет общие вершины с циклом C. Теперь проходим ребра графа G следующим образом: идем по ребрам цикла C до первой неизолированной вершины графа G_1. Затем проходим эйлеров цикл в компоненте графа G_1, затем снова двигаемся по циклу C до следующей неизолированной вершины графа G_1. Ясно, что процесс заканчивается в исходной вершине, что и показывает существование эйлерова цикла. ♦

Аналогичным образом доказывается

Теорема 2. Связный граф G является полуэйлеровым тогда и только тогда, когда в нем существует точно две вершины нечетной степени. ♦ Аналогичное определение можно сделать для ориентированных графов. Ориентированный эйлеров путь это ориентированный путь, содержащий каждую дугу точно один раз. Ориентированный граф называется эйлеровым, если в нем существует ориентированный эйлеров путь.

Аналогично теореме 1 можно доказать следующее утверждение.

Теорема 3. Ориентированный граф $G(V,E)$, у которого связан соответствующий скелетный граф, является Эйлеровым тогда и только тогда, когда либо для всех вершин v, $d_i(v) = d_0(v)$, либо существуют точно две вершины v_1 и v_2 такие, что $d_0(v_1) = d_i(v_1) + 1$, $d_0(v_2) + 1 = d_i(v_2)$, а для остальных вершин

$d_i(v) = d_0(v)$. (3)

В первом случае любой эйлеров путь является ориентированным циклом, во втором - начинается в вершине v_1 заканчивается в вершине v_2.

Теорема 4. Пусть G - связный граф, имеющий точно $2s > 0$ вершин нечетной степени. Тогда существует s и не существует меньшего числа путей $P_1, \dots, P_s$, которые в совокупности содержат все ребра графа G точно по одному разу. При этом каждый из путей $P_1, \dots, P_s$ начинается в одной нечетной вершине и кончается в другой.

♦ Согласно факта 1 в графе G имеется четное число 2s вершин нечетной степени. Разобьем эти вершины на s пар $(v_1, w_1), \dots, (v_s, w_s)$. Образуем теперь новый граф G_1, добавив каждой паре (v_i,w_i), $i = \overline{1,s}$ ребро. Тогда G - связный граф, у которого все вершины четны. Согласно теореме 1 в графе G_1 существует эйлеров цикл C, проходящий по всем ребрам точно по одному разу. Удалим из цикла C добавленные ребра и получим s путей $P_1, \dots, P_s$, проходящих каждое ребро точно один раз. Ясно, что каждый путь начинается и кончается в нечетной вершине. Пусть теперь имеется t путей $t < s$ $P_1, \dots, P_t$, содержащих все ребра графа G. Тогда каждая нечетная вершина должна быть концом пути и, значит, имея 2s нечетных вершин, нельзя покрыть все ребра графа G менее, чем s путями. ♦

Приведем теперь алгоритм построения эйлерового пути в данном эйлеровом графе.

Теорема 5. Пусть G - эйлеров граф. Тогда следующая процедура всегда возможна и приводит к построению эйлеровой цепи графа G.

Выходя из произвольной вершины, идем по ребрам графа произвольным образом, соблюдая следующие правила:

1) стираем ребра по мере их прохождения (вместе с изолированными вершинами, которые при этом образуются);

2) на каждом этапе идем по ребру, удаление которого нарушает связность, только в том случае, когда нет других возможностей.

♦ Убедимся сначала, что указанная процедура может быть выполнена на каждом этапе. Пусть мы достигли некоторой вершины v, начав с вершины u, $v \neq u$. Удалив ребра пути из v в u, видим, что оставшийся граф G_1 связен и содержит ровно две нечетных вершины v и u. Согласно теореме 2 граф G_1 имеет эйлеров путь P из v в u. Поскольку удаление первого ребра инцидентного u пути P либо не нарушает связности G_1, либо происходит удаление вершины u и оставшийся граф G_2 связен с двумя нечетными вершинами, то отсюда получаем, что описанное выше построение всегда возможно на каждом шаге. (Если v = u, то доказательство не меняется, если имеются ребра, инцидентные u). Покажем, что данная процедура приводит к эйлерову пути. Действительно, в G не может быть ребер, оставшихся непройденными после использования последнего ребра, инцидентного u, поскольку в противном случае удаление ребра, смежному одному из оставшихся, привело бы к несвязному графу, что противоречит 2). ♦

В качестве одного из применений эйлеровых графов приведем следующее.

Пусть A = {0, 1, … , m-1} - алфавит из m букв. Ясно, что имеется m^n различных слов длины n в алфавите A. Последовательностью де Брейна называется циклическое слово $a_0\, a_1 \dots a_{L-1}$ в алфавите A, такое, что подпоследовательности вида $a_i\, a_{i+1} \dots a_{i+n-1}$ i = 0, … , L-1 состоят из всех возможных $L = m^n$ слов длины n. Наиболее важный случай для приложений m = 2. Последовательности де Брейна производятся полноцикловыми регистрами сдвига. Покажем существование последовательностей де Брейна.

Пример. n = 1, m = 2 01

n = 2, m = 2 0011

n = 3, m = 2 $\begin{cases} 00010111 \\ 00011101 \end{cases}$

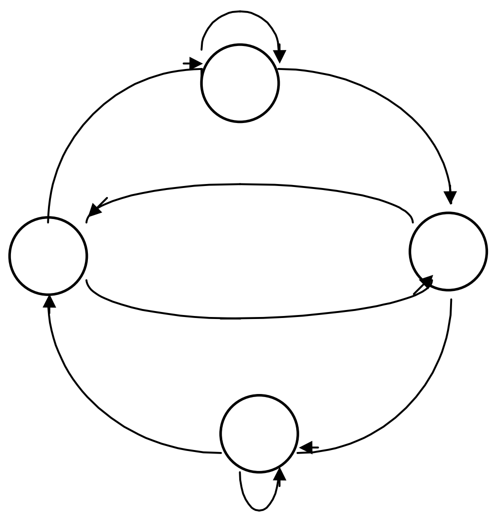
Определим ориентированный граф $G_{m,n}(V,E)$ следующим образом:

1) V является множеством всех m^{n-1} слов длины n-1 над A.

2) E является множеством всех m^n слов длины n над A.

3) дуга $(a_1, a_2, \dots, a_n)$ имеет начальной вершиной $(a_1, \dots, a_{n-1})$и конечной вершиной $(a_2, \dots, a_n)$.

Приведем граф $G_{2,3}$:



Ясно, что последовательности де Брейна соответствует замкнутый путь в графе $G_{m,n}$, содержащий каждую дугу точно один раз. Обратно, ориентированный цикл в $G_{m,n}$, содержащий каждую дугу точно один раз, приводит к построению цикла де Брейна, если выписывать соответствующие дуги подряд.

Пример. Для графа $G_{2,3}$ имеем эйлеров путь

000, 001, 011, 111, 110, 101, 010, 100

а соответствующую последовательность де Брейна

00011101

Теорема 6. Для любых целых m и n граф $G_{m,n}$ имеет ориентированный эйлеров цикл.

♦ Покажем сначала, что граф $G_{m,n}$ сильно связен, а значит его соответствующий скелетный граф связен. Действительно, пусть $b_1, \dots, b_{n-1}$ и $c_1, \dots, c_{n-1}$ две вершины. Тогда их соединяет следующий ориентированный путь

$(b_1, b_2, \dots, b_{n-1}, c_1), (b_2, \dots, b_{n-1}, c_1, c_2), \dots, (b_{n-1}, c_1, \dots, c_{n-1})$.

Далее $d_i(v) = d_0(v) = m$ для любой вершины v.

Действительно, из вершины $v = (b_1, b_2, \dots, b_{n-1})$ выходят дуги вида:

$(b_1, b_2, \dots, b_{n-1}, c)$

и входят дуги вида $(c, b_1, \dots, b_{n-1})$, $c \in A$.

Теперь по теореме 3 в графе $G_{m,n}$ существуют эйлеровы циклы.

Следствие. Для любых целых m, n последовательности де Брейна существуют.

♦ Известен следующий результат.

Теорема 7. Для любых натуральных m, n существует точно $\dfrac{(m!)^{m^{n-1}}}{m^n}$ последовательностей де Брейна.

$\S$ 3. Гамильтоновы графы.

Изучаемое понятие связано с существованием в графе цикла, проходящего ровно один раз через каждую вершину. Граф называется гамильтоновым, если в нем такой цикл существует и полугамильтоновым, если существует путь, проходящий через каждую вершину точно один раз. Ясно, что это определение можно распространить на ориентированные графы, если путь считать ориентированным. В отличие от эйлеровых графов, где имеется критерий для графа быть эйлеровым, для гамильтоновых графов такого критерия нет. Большинство известных фактов имеет вид: “если граф G имеет достаточное количество ребер, то граф является гамильтоновым”. Приведем одну из таких теорем, известную как теорема Дирака.

Теорема 1. Пусть в графе $G(V,E)$ с n вершинами ($n \geq 3$) выполняется условие $d(v) \geq \frac{n}{2}$ для любого $v \in V$. Тогда граф G является гамильтоновым.

♦ Заметим сначала следующее. Если к любому графу G добавить некоторое количество новых вершин, соединяя каждую из них с каждой вершиной графа, то мы получаем гамильтонов граф G'. Пусть мы добавили к графу $G(V,E)$ минимальное число k новых вершин, $k > 0$, после чего граф стал гамильтоновым. Рассмотрим гамильтонов цикл $v_1, w, v_2, \ldots, v_1$ в графе G', где $v_i \in V$, w - одна из новых вершин. Следовательно, v_2 не является смежной с v_1 в графе G, поскольку тогда мы могли не использовать вершину w, что противоречило бы минимальности числа k. Далее, пусть вершина v_2' смежная с v_2, а v_1' - смежная с v_1. Тогда v_2' не может следовать за v_1' в цикле. Действительно, в этом случае цикл $v_1, w, v_2, \ldots, v_1', v_2', \ldots, v_1$ можно заменить на $v_1, v_1', \ldots, v_2, v_2', \ldots, v_1$ и снова высвободить вершину w. Значит, число вершин графа G', не являющихся смежными с v_2, не меньше числа вершин, смежных с v_1, поскольку на гамильтоновом цикле за любой вершиной, смежной с v_1, следует вершина, не смежная с v_2. Число вершин, смежных с v_1, не меньше, чем $\frac{n}{2} + k$, то же и для вершины v_2. Далее, поскольку любая вершина графа G' является либо смежной, либо не смежной вершине v_2, то, значит, общее число вершин $n + k$ не меньше, чем $2(\frac{n}{2} + k) = n + 2k$. Полученное противоречие показывает, что
$k = 0$, т.е. исходный граф гамильтонов. ♦

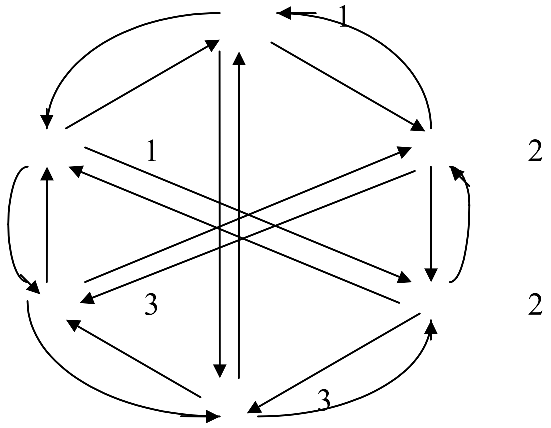
Приведем примеры гамильтоновых графов.

1. Полный граф K_n гамильтонов.

2. Граф единичного куба B_n гамильтонов.

3. Определим ориентированный граф $\Gamma(S_n)$ - вершинами которого являются n! перестановок. При этом от перестановки s_1 к перестановке s_2 идет дуга, если существует транспозиция, переводящая перестановку s_1 в s_2. Полученный граф $\Gamma(S_n)$является гамильтоновым.

В качестве примера приведем граф $\Gamma(S_3)$:



Из предыдущего следует, что многие важные прикладные задачи сводятся к построению гамильтонова цикла некоторого графа. Учитывая важность задачи перечисления перестановок. приведем еще один такой алгоритм на языке построения гамильтонова цикла в $\Gamma(S_n)$. Алгоритм построения цикла опишем индуктивно. Пусть L_n - список всех перестановок символов 1, 2, … , n. Обозначим через $L_n(i)$ $(1 \le i \le n+1)$ множество перестановок символов 1, … , i-1, i+1, … , n+1, полученных следующим образом: $L_n(n+1) = L_n$ и $L_n(i)$, $(1 \le i \le n)$ получено из $L_n(i+1)$ заменой всех появлений i на i+1.

Тогда положим

$$L_{n+1}= L_n(n+1)\vee(n+1),\ \overline{L}_n(n)\vee n,\ L_n(n-1)\vee(n-1),\ \overline{L}_n(n-2)\vee(n-2),\ \dots \quad (4)$$

Здесь символ $\vee$ означает, что в списке $L_n(i)\vee i$ все перестановки из $L_n(i)$ дополняются дописыванием справа элемента i. Список $\overline{L}_n(i)$ - это список $L_n(i)$, написанный в обратном порядке. Нетрудно показать индукцией по n, что таким образом построенная последовательность перестановок содержит каждую перестановку точно один раз и каждая последующая перестановка отличается от предыдущей одной транспозицией.

<u>Пример.</u> n = 3 Имеем:

$L_2(3)$:	$(12) \to (21)$
$L_2(2)$:	$(13) \to (31)$
$L_2(1)$:	$(23) \to (32)$

$L_3 = L_2(3) \vee 3,\ \overline{L}_2(2) \vee 2,\ L_2(1) \vee 1 =$

$= (123) \to (213) \to (312) \to (132) \to (231) \to (321)$.

Понятие "почти все" графы.

Пусть G(n) – множество всех графов на множестве вершин V = {1, 2, ..., n}. Пусть P – некоторое свойство, которым каждый граф из G(n) может обладать или нет. Пусть $G_p(n)$ – множество тех графов из G(n), которые обладают свойством P.

Говорят, что почти все графы обладают свойством P, если

$$\lim_{n\to\infty} \frac{|G_p(n)|}{|G(n)|} = 1$$

и почти нет графов со свойством P, если

$$\lim_{n\to\infty} \frac{|G_p(n)|}{|G(n)|} = 0$$

В качестве примера использования данного понятия докажем один результат.

Теорема. Почти нет эйлеровых графов.

► Пусть $G_1(n)$ – множество эйлеровых графов, G(n) – множество всех графов, $G_2(n)$ – множество графов, вершины которых имеют четную степень. По теореме Эйлера имеем $G_1(n) \subseteq G_2(n)$, т.к. в G_2 не учтена связность.

Ясно, что графы из $G_2(n)$ можно получить из графов G(n – 1) добавлением новой вершины и соединением ее со всеми вершинами нечетной степени.

Имеем

$$|G(n-1)| = 2^{\binom{n-1}{2}}$$

$$|G_2(n)| \le 2^{\binom{n-1}{2}} = 2^{\binom{n}{2}-n+1}$$

$$|G(n)| = 2^{\binom{n}{2}}$$

Отсюда получаем, что

$$|G_2(n)| = 0(|G(n)|)$$

и $$|G_1(n)| = 0(|G(n)|)$$

что и доказывает утверждение. ◄

Отметим без доказательства другие утверждения такого типа.

Теорема. Почти все графы связны.

Теорема. Диаметры почти всех графов равны 2.

Теорема. Почти все графы гамильтоновы.

Теорема. Множество автоморфизмов почти каждого графа состоит из одного тождественного автоморфизма.

§ 4. Кратчайшие пути.

Пусть G(V,E) - конечный неориентированный граф и пусть заданы две его вершины s и t. Требуется найти кратчайший путь (длина пути равна числу входящих в него ребер) от вершины s к вершине t. Сначала мы опишем алгоритм, который находит длину кратчайшего пути.

Алгоритм ДЛИНА

1) Помечаем вершину s пометкой 0. Полагаем i = 0.

2) Находим все непомеченные вершины, связанные ребром с вершинами, имеющими отметку i. Если таких вершин нет, t недостижимо из s, стоп. Если такие вершины есть, помечаем их i+1.

3) Если вершина t помечена, переходим к 4). Если нет, то увеличиваем i на 1 и повторяем шаг 2).

4) Длина кратчайшего пути от s к t равна i+1, стоп.

Корректность алгоритма следует из следующего утверждения.

Факт 1. Вершина v графа G(V,E) помечается в алгоритме пометкой $\ell(v)$ тогда и только тогда, когда длина кратчайшего пути от вершины s к v равна $\ell(v)$.

♦ Доказательство индукцией по i. Ясно, что при i = 0, $\ell(v) = 0$ влечет v = s и утверждение справедливо. Предположим, что утверждение верно для всех вершин v, для которых $\ell(v) \leq m$. Если вершина u не помечена, значит нет пути от s к u, меньше чем m+1. Если u связана ребром с вершиной, помечной,то ее пометка , во-первых , будет равна m+1 , во-вторых , имеется путь длины m от s к данной вершине и, значит, длина кратчайшего пути от s к u равна m+1. Если u не связана ребром с вершиной, имеющей пометку m, то не существует пути, короче, чем m+1 от s к u, поскольку предыдущая вершина на этом пути имела бы пометку m.

Сделаем к данному алгоритму дополнительные замечания.

1. Если граф G конечен и нет пути от s к t, то алгоритм остановится после того, как будут помечены все вершины, достижимые из s.

2. Если граф G ориентирован и ищется ориентированный путь из s к t, то алгоритм применим, и в этом случае, если шаг 2) записать в виде: 2′) Найти все непомеченные вершины, которые достижимы дугами, выходящими из вершин, имеющих пометку i. Когда Алгоритм ДЛИНА выдал нам значение $\ell(t)$ кратчайшего пути от s к t, то нетрудно теперь найти некоторый такой путь, используя пометки $\ell(v)$. Приводимый ниже алгоритм выдает путь v(0), v(1), … , v($\ell(t)$) такой, что v(0) = s, v($\ell(t)$) = t.

Алгоритм ПУТЬ.

1) Полагаем i = ℓ(t) и помечаем v(i) = t.

2) Находим вершину u такую, что u связана ребром с v(i) и ℓ(u) = i-1. Помечаем v(i-1) = u.

3) Если i = 1, то стоп. Если нет, уменьшаем i на 1 и повторяем шаг 2). ♦

Приводимое ниже утверждение позволяет находить число путей фиксированной длины между любыми двумя вершинами.

Для графа G(V,E), $|V| = n$ определим матрицу смежности, т.е. (n×n) - матрицу $A = (a_{ij})$, i, j = 1, … , n, где

$$a_{ij} = \begin{cases} 1, \text{ если вершины } i, j \text{ соединены ребром} \\ 0, \text{ в противном случае.} \end{cases}$$

Теорема 2. Пусть $A^{\ell} = (a_{ij}^{(\ell)})$, i , j = 1, … , n, где ℓ - натуральное число. Тогда $a_{ij}^{(\ell)}$ равно числу путей длины ℓ, соединяющих вершины i и j.

При $\ell = 1$утверждение верно по определению. Пусть для ℓ-1 это выполняется. Тогда образуем $A^{\ell} = A^{\ell-1} * A$.

Имеем $a_{ij}^{(\ell)} = a_{i1}^{(\ell-1)} \cdot a_{1j} + a_{i2}^{(\ell-1)} \cdot a_{2j} + \ldots + a_{in}^{(\ell-1)} \cdot a_{nj}$.

Элемент $a_{ik}^{(\ell-1)} \cdot a_{kj} \neq 0$ в том и только в том случае, когда имеется путь длины (ℓ-1) из вершины i в вершину k, и вершины k и j соединены дугой. По индукции $a_{ik}^{(\ell-1)}$ - число путей длины ℓ-1 из i в k. Значит $a_{ik}^{(\ell-1)} \cdot a_{kj}$, - число путей длины ℓ из i в j, таких, что k - предыдущая вершина для j. Просуммировав по всем k, получаем общее число путей длины ℓ.

§ 5. Деревья.

1. Связный граф G(V, E), не имеющий циклов, называется деревом. Следующая теорема перечисляет некоторые основные свойства деревьев.

Теорема 1. Пусть граф G(V, E) имеет n вершин. Тогда следующие утверждения эквиваленты.

1) G является деревом;

2) G не содержит циклов и имеет n - 1 ребер;

3) G связен и имеет n - 1ребер;

4) G связен, но удаление любого ребра нарушает связность;

5) любые две вершины графа G соединены ровно одним путем;

6) G не имеет циклов, но добавление любого ребра порождает ровно один цикл.

♦ При n = 1 утверждение очевидно, поэтому считаем $n \geq 2$. 1) $\Rightarrow$ 2). По определению G не имеет циклов. Рассмотрим некоторое ребро $\ell = (v_1, v_2)$ и удалим его. Получим граф G′. В графе G′ нет пути из v_1 в v_2 , т.к. если бы такой путь был, то в графе G был бы цикл. Значит G′ не связен и не имеет циклов. Значит он состоит из двух компонент, являющихся деревьями с числом вершин n_1 и n_2 соответственно $(n_1 + n_2 = n)$. По индуктивному предположению G′ имеет $n_1 - 1 + n_2 - 1$ ребер. Следовательно, граф G имеет n - 1 ребер.

2) $\Rightarrow$ 3). Если бы G был несвязен, то каждая его компонента представляла бы собой связный граф без циклов. Из предыдущего имеем, что число ребер в каждой компоненте меньше на один числа ее вершин. Значит, общее число ребер меньше числа вершин по крайней мере на два, что противоречит тому, что G имеет n - 1ребер.

3) $\Rightarrow$ 4). Удаление любого ребра приводит к графу с n вершинами и n-2 ребрами, который не может быть связным в силу Факта 2 § 1.

4) $\Rightarrow$ 5). В силу связности G, каждая пара вершин соединена путем. Если бы данная пара была соединена более, чем одним путем, то они образовывали бы цикл. Но тогда удаление любого ребра в цикле не нарушает связности графа.

5) $\Rightarrow$ 6). Если бы G содержал цикл, то любые две вершины на цикле соединялись бы по крайней мере двумя путями. Добавим теперь к графу G ребро $\ell = (v_1, v_2)$. Тогда образуется цикл, т.к. вершины v_1 и v_2 уже соединены путем. Ясно, что цикл единственный.

6) $\Rightarrow$ 1). Если бы G был несвязен, то добавление ребер, соединяющих вершины из разных компонент, не приводит к образованию цикла. ♦

Следствие. Дерево с более чем одной вершиной имеет по крайней мере две вершины степени 1.

♦ Действительно, пусть $v_1, \dots, v_n$ - множество вершин, тогда имеем

$$\sum_{i=1}^{n} d(v_i) = 2(n-1)$$

В силу связности $d(v_i) \geq 1$, отсюда и следует утверждение. ♦

2. Для графа G(V, E) определим два полезные понятия.

Вершинный подграф $G(V', E')$ - это граф на множестве вершин $V' \subset V$ и ребрами $E' \subset E$, такими, что оба конца ребра $e' \in E'$ принадлежат V'.

Реберный подграф $G(V', E')$ - это граф, определяемый подмножеством ребер $E' \subset E$ и множеством вершин $V' \subset V$, состоящим из концевых вершин ребер из E'. Остовным (покрывающим) деревом графа G(V, E) называется его реберный подграф с множеством вершин V, являющийся деревом.

Факт 2. Граф G(V, E) имеет остовное дерево тогда и только тогда, когда он связен. ♦ Предложим процедуру построения остовного дерева. Ясно, что если граф G не связен, то он не может иметь остовного дерева.

Пусть граф связен. Если в графе нет ребра, удаление которого сохраняет связность графа, то G - дерево.

Если такое ребро есть, удалим его и продолжим процедуру. Когда процедура не может быть продолжена, полученный граф является деревом. ♦

Рассмотрим теперь известную проблему нахождения минимального остовного дерева. Пусть G(V, E) неориентированный граф и пусть каждому ребру $e \in E$ поставлено в соответствие положительное число $\ell(e)$, называемое его весом. Требуется найти связный реберный подграф $G'(V', E')$, такой, что $V' = V$, причем сумма

$$M(G') = \sum_{e' \in E'} \ell(e')$$

минимальна.

Ясно, что граф $G(V', E')$ должен быть деревом. Действительно, если $G(V', E')$ содержит цикл, то тогда любое ребро цикла можно удалить из графа и тем самым уменьшить суммарный вес ребер графа $G(V', E')$.

Факт 3. Пусть V - произвольная вершина связного графа G(V, E) и пусть e - смежное с ней ребро, для которого $\ell(e)$ минимально для всех ребер, смежных с V. Тогда существует минимальное остовное дерево для G(V, E), которое содержит ребро e.

♦ Пусть T - любое минимальное остовное дерево для G(V, E). Если e не является ребром T, добавим e к T. Поскольку T - дерево, то в силу теоремы, при этом образуется цикл. Возьмем ребро e′, лежащее на цикле и смежное с вершиной V, и удалим его. Поскольку $\ell(e') \geq \ell(e)$, то получившееся дерево также минимально. ♦

Следующая теорема дает алгоритм построения минимального остовного дерева, известный под названием алгоритма Краскала.

Теорема 4. Пусть G(V, E) связный граф с n вершинами. Тогда следующая процедура приводит к построению минимального остовного дерева.

1) Выберем ребро e_1, обладающее в G наименьшим весом.

2) Определим по индукции последовательность ребер $e_2, \ldots , e_{n-1}$ (∗) , выбирая на каждом шаге ребро, отличное от предыдущих, с наименьшим весом и не образующее цикла с уже выбранными ребрами. Полученный подграф T графа G, образованный ребрами $e_1, \ldots , e_{n-1}$, и есть искомое остовное дерево.

♦ Поскольку T не содержит циклов и имеет n - 1 ребер, то T - остовное дерево, в силу теоремы 1. Покажем, что сумма весов всех ребер T минимальна. Предположим, что в G существует некоторое другое остовное дерево T′, такое, что $M(T') < M(T)$. Пусть e_k - первое ребро из последовательности (∗) теоремы, которое не принадлежит T′. Добавим ребро e_k к T′ - тогда в T′ образуется цикл C, содержащий ребро e_k. Цикл C содержит ребро e, принадлежащее T′ и не принадлежащее T. Удалим из T′ ребро e и добавим ребро e_k. Полученный подграф T″ также является остовным деревом. По построению $\ell(e_k) \leq \ell(e)$, поэтому $M(T'') \leq M(T')$. При этом число общих ребер у T″ и T на одно больше, чем у T′ и T. Повторяя описанную процедуру, можно преобразовать T′ в T, причем сумма весов на каждом шаге не увеличивается. Значит, $M(T) \leq M(T')$, что противоречит допущению. ♦ Сделаем теперь несколько замечаний о применениях понятия остовного дерева.

Представим себе, что мы хотим построить сеть связи, которая бы соединяла n данных городов, причем так, чтобы каждый город имел связь с каждым, быть может транзитную. Если при этом из экономических соображений требуется, чтобы общая длина линий была минимальной, то ясно, что речь идет о минимальном остовном дереве графа, вершины которого соответствуют городам, а ребра - соединяющим их линиям связи. Поиск минимального остовного дерева можно искать с помощью алгоритма теоремы 4. Это замечание справедливо, если минимальное остовное дерево определяется как остовное дерево, доставляющее минимум некоторой монотонной симметрической функции от весов составляющих его ребер.

3. В этом пункте мы получим формулу Кирхгофа для числа остовных деревьев произвольного неориентированного графа и формулу Кэли для числа остовных деревьев полного графа. Получим сначала подготовительные результаты. Пусть G(V, E) ориентированный граф без петель, где $V = \{v_1, \dots, v_n\}$, $E = \{e_1, \dots, e_m\}$. Определим матрицу инцидентности A графа G следующим образом:

$A = (a_{ij})$, $i = 1, \dots, n$, $j = 1, \dots, m$, где

$$a_{ij} = \begin{cases} +1, \text{ если } v_i \text{ начальная вершина } e_j; \\ -1, \text{ если } v_i \text{ конечная вершина } e_j; \\ 0, \text{ если } v_i \text{ не инцидентна } e_j. \end{cases}$$

Напомним, что минором $A\begin{pmatrix} i_1 & i_2 & \dots & i_p \\ j_1 & j_2 & \dots & j_p \end{pmatrix}$ называется определитель подматрицы, полученный из A строками $i_1, \dots, i_p$ и столбцами $j_1, \dots, j_p$.

Факт 5. Миноры матрицы инциденций A равны + 1, - 1 или 0.

♦ По определению, каждый столбец матрицы A имеет один элемент +1 и один -1, остальные элементы 0. Рассмотрим произвольную подматрицу $A\begin{pmatrix} i_1 & i_2 & \dots & i_p \\ j_1 & j_2 & \dots & j_p \end{pmatrix}$.

Если имеется столбец из нулей, то ее определитель равен нулю. Если имеется столбец, содержащий один ненулевой элемент (+ 1 или - 1), то утверждение следует по индукции, т.к. оно верно для размера p = 1.

Если все столбцы содержат оба элемента + 1 и - 1, то суммированием всех строк получаем нулевую строку и, значит, определитель равен нулю.

Факт 6. Минор $A\begin{pmatrix} i_1 & i_2 & \dots & i_{n-1} \\ j_1 & j_2 & \dots & j_{n-1} \end{pmatrix}$ матрицы инциденций A ориентированного графа G(V, E) отличен от нуля (т.е. равен + 1 или - 1) тогда и только тогда, когда соответствующий скелетный граф $\tilde{G}$ реберного подграфа, определенного $E' = \{e_{j_1}, \dots, e_{j_{n-1}}\}$ является деревом.

♦ Пусть $\tilde{G}$ не является деревом. Тогда, поскольку число ребер равно n - 1, то по теореме 1 $\tilde{G}$ должен содержать цикл. Если взять сумму столбцов, которые соответствуют ребрам простого цикла в $\tilde{G}$, то получим нулевой столбец. Минор в этом случае равен нулю. Обратно, пусть $\tilde{G}$ дерево. Если n = 2, то $\tilde{G}$ состоит из одного ребра. Соответствующая матрица A имеет размер 2×1, а ее миноры равны + 1 и - 1. Предположим, что если $\tilde{G}$ дерево с k - 1 вершинами, то соответствующий минор ненулевой, и пусть $\tilde{G}$ имеет k вершин. Пусть $E' = \{e_{j1}, e_{j2}, \ldots, e_{jk-1}\}$- соответствующий ему набор ребер, а $\{v_{i_1}, v_{i_2}, \ldots, v_{i_{k-1}}, v_{i_k}\}$ - набор вершин. Поскольку каждое дерево имеет по крайней мере 2 конечные вершины, то среди k - 1 вершин $v_{i_1}, v_{i_2}, \ldots, v_{i_{k-1}}$ имеется одна конечная, скажем v_t. Разложим минор по строке t. Ясно, что эта строка содержит единственный, отличный от нуля элемент (+ 1 или - 1) и k - 2 нулей. Значит, с точностью до знака, минор равен минору, который соответствует дереву $\tilde{G}'$, полученному из $\tilde{G}$ удалением вершины v_t и всех ребер, смежных с ней. По индуктивному предположению данный минор отличен от нуля. ♦

Нам понадобится известная формула Бинэ-Коши из линейной алгебры.

Пусть A - (n × m)- матрица и B - (m × n)- матрица, где n ≤ m. Тогда справедливо следующее тождество

$$\det(A \cdot B) = \sum_{1 \le j_1 < j_2 < \ldots < j_n \le m} A\begin{pmatrix} 1 & 2 & \ldots & n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix} B\begin{pmatrix} j_1 & j_2 & \ldots & j_n \\ 1 & 2 & \ldots & n \end{pmatrix}$$

Теперь мы в состоянии доказать теорему Кирхгофа.

<u>Теорема 7.</u> Пусть M - ((n - 1) × m)-матрица, полученная из матрицы инциденций A ориентированного графа G(V, E) вычеркиванием некоторой строки. Тогда det(M·M′) равен числу остовных деревьев соответствующего скелетного графа. (Здесь M′ - транспонированная матрица M).

По формуле Бинэ-Коши имеем

$$\det(M \cdot M') = \sum_{1 \le j_1 < j_2 < \ldots < j_{n-1} \le m} M\begin{pmatrix} 1 & 2 & \ldots & n-1 \\ j_1 & j_2 & \ldots & j_{n-1} \end{pmatrix} M'\begin{pmatrix} j_1 & j_2 & \ldots & j_{n-1} \\ 1 & 2 & \ldots & n-1 \end{pmatrix} =$$

$$= \sum_{1 \le j_1 < j_2 < \ldots < j_{n-1} \le m} \left[M\begin{pmatrix} 1 & 2 & \ldots & n-1 \\ j_1 & j_2 & \ldots & j_{n-1} \end{pmatrix} \right]^2$$

поскольку

$$M\begin{pmatrix} 1 & 2 & \dots & n-1 \\ j_1 & j_2 & \dots & j_{n-1} \end{pmatrix} = M'\begin{pmatrix} j_1 & j_2 & \dots & j_{n-1} \\ 1 & 2 & \dots & n-1 \end{pmatrix}$$

Далее, на основе факта 6 скелетный граф реберного подграфа, определенного ребрами $E' = \{e_{j_1}, e_{j_2}, \dots, e_{j_{n-1}}\}$ является остовным деревом тогда и только тогда, когда $\left[M\begin{pmatrix} 1 & 2 & \dots & n-1 \\ j_1 & j_2 & \dots & j_{n-1} \end{pmatrix}\right]^2 = 1$. Суммирование распространено по всем E' и каждое E' появляется точно один раз. Каждое E', соответствующее дереву, дает 1, не соответствующее дереву, дает 0. ♦

Если дан произвольный неориентированный граф $G(V, E)$, то нет необходимости приписывать ребрам ориентацию, определять матрицы M и M' и перемножать их. Можно вычислить $M \cdot M'$ непосредственно, исходя из графа $G(V, E)$. Пусть $V = \{v_1, v_2, \dots, v_n\}$. Пусть вычеркиваемая строка в матрице инциденций A соответствует v_n . Нетрудно заметить, что элемент $(M \cdot M')_{ii}$ - это степень вершины v_i , а элемент $(M \cdot M')_{ij}$ при $i \neq j$- это число ребер, соединяющих v_i с v_j , взятое со знаком минус.

<u>Пример.</u> Рассмотрим граф G:

Тогда $$M \cdot M' = \begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix}$$

и значит $\det(M \cdot M') = 4$.

Значительный интерес имеет случай полного неориентированного графа на n вершинах. Число покрывающих деревьев такого графа найдено Кэли.

<u>Теорема 8.</u> Число остовных деревьев полного неориентированного графа на n вершинах равно n^{n-2} .

♦ Матрица $M \cdot M'$ в этом случае имеет вид:

$$\begin{pmatrix} n-1 & -1 & \dots & -1 \\ -1 & n-1 & \dots & -1 \\ & & \dots & \\ -1 & -1 & \dots & n-1 \end{pmatrix}$$

Отнимем первый столбец от остальных и получим

$$\begin{pmatrix} n-1 & -n & \dots & -n \\ -1 & n & \dots & 0 \\ & & \dots & \\ -1 & 0 & \dots & n \end{pmatrix}$$

Теперь прибавим все строки к первой строке, получаем

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ -1 & n & \dots & 0 \\ & & \dots & \\ -1 & 0 & \dots & n \end{pmatrix}$$

Ясно, что определитель последней матрицы есть n^{n-2}. ♦

4. Вернемся еще раз к вопросу о порождении подстановок транспозициями, рассмотренному в главе I. Пусть S_n - группа всех подстановок степени n, T_n - множество всех транспозиций. Напомним, что некоторое множество элементов M из группы G является системой образующих для G или порождает G, если множество $\langle M\rangle$ произведений с конечным числом сомножителей элементов из M, взятых с положительными и отрицательными степенями, совпадают с группой G.

Поставим теперь вопрос, когда произвольное множество транспозиций R_n из T_n является системой образующих для S_n? Пусть $R_n = \{t_1, ... , t_r\}$. Поставим множеству R_n в соответствие граф $\Gamma(R_n)$, называемый графом Пойа и определяемый следующим образом:

Вершинами графа $\Gamma(R_n)$ являются элементы 1, 2, … , n. Каждой $t_i \in R_n$, если $t_i = (p, q)$ в $\Gamma(R_n)$ соответствует ребро, инцидентное вершинам p и q. Может быть доказана

<u>Теорема 9.</u> Множество транспозиций $R_n = \{t_1, \dots , t_r\}$, $(r \geq n - 1)$ тогда и только тогда порождает симметрическую группу S_n, когда соответствующий граф Пойа $\Gamma(R_n)$ связен.

<u>Следствие 1.</u> Множество из n - 1 транспозиций R_n порождает S_n тогда и только тогда, когда соответствующий граф Пойа $\Gamma(R_n)$ является деревом.

Следствие 2. Число систем образующих симметрической группы S_n, состоящих из $n - 1$ транспозиций, равно n^{n-2}.

§ 6. Планарные графы

1. В некоторых случаях требуется, чтобы изображение графа удовлетворяло определенным условиям. Будем изображать графы так, что его вершинам соответствуют точки плоскости, а ребрам непрерывные, спрямляемые линии без самопересечений, причем ребра не должны иметь общих точек кроме инцидентных им вершин.

Такое изображение будем называть плоским графом, а граф, изоморфный плоскому, назовем планарным. Легко указываются примеры планарных графов. Например, $K_{2,\,3}$, K_4. В то же время не удается установить планарность графов $K_{3,\,3}$, K_5. Ниже будет доказано, что графы $K_{3,\,3}$, K_5 не являются планарными. Отметим, что справедлив факт, приводимый без доказательства.

<u>Теорема 1.</u> Почти все графы не являются планарными.

Рассмотрим сначала укладку графов в действительном трехмерном пространстве R_3.

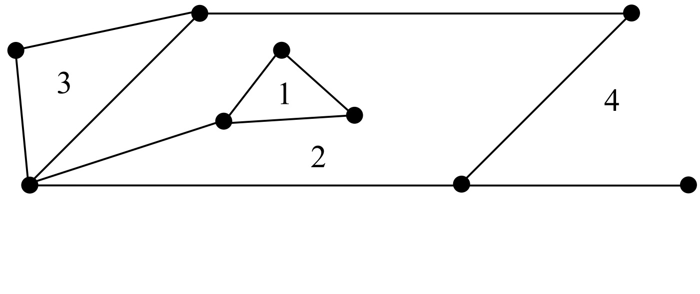
<u>Теорема 2.</u> Каждый граф укладывается в R_3.

▸ Все вершины произвольного графа G помещаем в различных точках координатной оси x. Рассмотрим пучок плоскостей, проходящих через ось x, и зафиксируем |E| различных таких плоскостей. Теперь каждое ребро (u, v) изобразим полуокружностью, проходящей в соответствующей плоскости через вершины u, v. Ясно, что различные ребра не будут пересекаться кроме как в общих вершинах. ◂

2. Пусть G – плоский граф. Определим отношение эквивалентности на множестве точек плоскости: объявим две точки u и v эквивалентными, если их можно соединить непрерывной, спрямляемой, без самопересечений кривой, не пересекающей ребра графа.

Легко проверить данное отношение есть отношение эквивалентности. Поэтому вся плоскость разбивается на классы эквивалентных точек. Класс эквивалентных точек плоскости называется гранью плоского графа.

<u>Пример.</u> Приведенный ниже граф имеет 4 грани.



Пусть $G = (V, E)$ – плоский граф, такой, что $n = |V|$, $m = |E|$, f – число граней.

Теорема 3 (Эйлер). Для всякого плоского связного графа G справедливо соотношение

$$n - m + f = 2$$

▸ Доказываем индукцией по m при фиксированном n. Поскольку G связен, то $m \geq n - 1$. Пусть $m = n - 1$. В силу связности G он является деревом. Значит в G нет циклов и потому $f = 1$ и теорема справедлива для этого случая.

Пусть она справедлива для всех m, таких, что $n - 1 \leq m < m_1$. Докажем ее для m_1.

Пусть G – связный граф, плоский с n вершинами и m_1 ребрами, имеющий f граней.

Поскольку $m_1 > n - 1$, то G содержит цикл C. Пусть e – ребро, принадлежащее циклу. Тогда e принадлежит разным граням. Удалим ребро e из графа G. Тогда эти две грани сливаются в одну, при этом граф G_1^1 полученный из G удалением e, связен, поскольку e лежит на цикле.

Граф G^1 имеет n вершин, $m_1 - 1$ ребер, $f - 1$ граней. По предположению индукции справедливо соотношение

$$n - (m_1 - 1) + (f - 1) = 2$$

Отсюда $n - m_1 + f = 2$, что и доказывает утверждение. ◂

Следовательно, число граней планарного графа определяется соотношением

$$f = m - n + 2$$

3. Используя теорему Эйлера можно доказывать непланарность конкретных графов.

Пусть G – планарный граф. Обозначим через φ_k – число граней, ограниченных k ребрами.

Поскольку рассматриваются графы без петель и параллельных ребер, то $\varphi_0 = \varphi_1 = \varphi_2 = 0$.

Справедливы следующие соотношения:

$$f = \varphi_3 + \varphi_4 + \ldots$$

$$2m = 3 \cdot \varphi_3 + 4\varphi_1 + \ldots$$

В первом соотношении просуммированы все грани, во втором – ребра, ограничивающие каждую грань, при этом каждое ребро учитывается дважды.

Рассмотрим граф $K_{3,3}$. Для него $n = 6$, $m = 9$. Пусть $K_{3,3}$ – плоский граф. Тогда должно быть $f = 9 - 6 + 2 = 5$ граней.

Для графа $K_{3,3}$ нет циклов длины 3, поэтому $\varphi_3 = 0$. Следовательно, должно быть выполнено

$$5 = \varphi_4+\varphi_5+ \ldots$$

$$18 = 4\cdot\varphi_4+5\varphi_5+ \ldots$$

Отсюда получаем (т.к. $\varphi_k \geq 0$), что $-2 \geq 0$ – противоречие.

Рассмотрим теперь граф K_5. Для него $n = 5$, $m = 10$. Если бы граф K_5 был плоским, то должно быть $f = 10 - 5+2 = 7$. Следовательно, должно быть выполнено

$$7 = \varphi_4+\varphi_5+ \ldots$$

$$20 = 4\cdot\varphi_4+5\varphi_5+ \ldots$$

Отсюда следует, что $-1 \geq 0$ – противоречие.

В качестве упражнения предлагается доказать, что граф E_4 – (четырехмерный куб) – не является планарным.

4. Имеется несколько критериев планарности графа. Приведем без доказательства критерий Понтрягина-Куратовского. Для этого определим понятие гомеоморфизма графа. Операцией разбиения ребра $e = (u, v)$ называют операцию замены ребра e двумя ребрами $e_1 = (u, w)$ и $e_2 = (w, v)$, где w – новая вершина. Два графа называют гомеоморфными, если они могут быть получены из одного графа с помощью операций разбиения ребер.

Справедлива

<u>Теорема</u> (Понтрягин-Куратовский). Граф планарен тогда и только тогда, когда он не содержит подграфов, гомеоморфных $K_{3,3}$ или K_5.

5. Для характеристики непланарных графов используются различные меры, из которых укажем две. <u>Толщина</u> графа G есть число $t(G)$ – наименьшее число его планарных подграфов, объединение которых дает граф G. Очевидно, что толщина планарного графа есть 1.

Приведем значение толщины некоторых графов:

$$t(K_n) = \left[\frac{n+7}{6}\right]$$

$$t(E_n) = \left]\frac{n+1}{4}\right[$$

$$t(K_{m,n}) = \left]\frac{mn}{2(m+n-2)}\right[$$

Здесь $[x]$, $]x[$ – ближайшие целые для x, удовлетворяющие $[x] \leq x \leq]x[$.

Род графа G определяется как минимальное число ручек $\gamma(G)$, которые надо прикрепить к сфере, чтобы уложить граф G. Ясно, что для плоского графа G $\gamma(G) = 0$ поскольку укладка на плоскости равносильна укладке на сфере.

Приведем значения рода некоторых графов.

$$\gamma(E_n) = 1 + (n-4)2^{n-3}$$

$$\gamma(K_n) = \left]\frac{(n-3)(n-4)}{12}\right[$$

$$\gamma(K_{m,n}) = \left]\frac{(m-2)(n-2)}{4}\right[$$

§ 7. Раскраска графов

Пусть $G = (V, E)$ – некоторый граф. Пусть $\{1, 2, ..., k\}$ – множество "цветов". Отображение $f: V \to \{1, 2, ..., k\}$ называют k-раскраской вершин графа G. К-раскраска называется правильной, если

$$\forall(v_1, v_2) \qquad (v_1, v_2) \in E \Rightarrow f(v_1) \neq f(v_2).$$

т.е. смежные вершины получают различную окраску. Граф G называется k-раскрашиваемым, если для него существует правильная k-раскраска. Наименьшее k, для которого граф G является k-раскрашиваемым, называется хроматическим числом графа G (обозначение: $x(G)$). Если $x(G) = k$, то граф G называется k-хроматическим.

Существует ряд задач кибернетики, которые приводят к раскраске графа (задачи составления расписаний, обслуживания и др.).

Заметим сначала, что для любого натурального n существует граф G, такой, что $x(G) = n$. Примером такого графа является K_n. Очевидно, что $x(K_n) = n$.

Ясно, что 1-хроматические графы это графы, состоящие из изолированных вершин. 2-хроматические графы – это двудольные графы и только они.

В настоящее время нет описания k-хроматических графов при $k \geq 3$. Нет также эффективных алгоритмов нахождения хроматического числа графа. Однако, имеются хорошие оценки хроматического числа.

Теорема 1. Пусть p – максимальная степень вершин графа $G = (V, E)$. Тогда справедливо неравенство

$$x(G) \leq p+1$$

▸ Индукция по $n = |V|$. Выберем произвольную вершину $v \in V$ и удалим ее вместе с инцидентными ей ребрами. Получим граф G', у которого максимальная степень вершин p', причем $p' \leq p$. Число вершин у G' равно $n - 1$ и по индукции для G' имеется $(p'+1)$-раскраска, а значит и $(p+1)$-раскраска. Тогда $(p+1)$ – раскраску для G можно получить так: окрасим v в цвет, отличный от цветов вершин, смежных с ней, число которых не больше p. ◂

Для планарных графов данную оценку можно уточнить (используем обозначения предыдущего параграфа).

Теорема 2. Любой планарный граф 6-раскрашиваем.

▸ Заметим сначала, что для связного планарного графа $G = (V, E)$ выполнено

$$2m - 3f \geq 0.$$

Это следует из равенств:

$f = \varphi_3+\varphi_4+ ...$

$2m = 3\varphi_3+4\varphi_4+ ...$

По теореме Эйлера должно выполняться $n - m+f = 2$. Отсюда получаем $3n - m \geq 6$.

Покажем теперь, что в планарном графе существует вершина степени не выше 5.

Пусть напротив, все вершины имеют степень не меньшую, чем 6. Поскольку $\sum \deg(v) = 2m$, то отсюда следует, что должно быть $2m \geq 6n$ или $m \geq 3n$.

Два последние неравенства приводят к противоречию.

Теперь доказываем утверждение теоремы индукцией по $n = |V|$.

Пусть для всех планарных графов $G = (V, E)$ с $|V| < n_0$ утверждение верно. Пусть G – граф с $|V| = n_0$. По предыдущему, в G есть вершина v степени не выше 5. Удалим v вместе со смежными ей ребрами и получим граф G' с $n_0 - 1$ вершинами, планарный. По предположению индукции $x(G') \leq G$. Пусть $v_1, ..., v_k$ – вершины G', смежные с v. Имеем $k \leq 5$. Для раскраски G используем для v цвет, отличный от цветов $v_1, ..., v_k$. Следовательно, $x(G) \leq G$. ◄

Усложнив рассуждения, можно доказать, что $x(G) \leq 5$ для всякого планарного графа. Гипотеза 4^x красок для планарного графа была сформулирована А. Кэли в 1878 году и утверждала, что $x(G) = 4$.

Данная гипотеза была подтверждена в 1978 году Аппелем Т. и Хакеном М. Соответствующее доказательство использовало ЭВМ и пока оно не имеет проверки в традиционном понимании.

§ 8. Потоки в сетях.

В этом пункте будут рассмотрены основы важного направления, связанного с изучением потоков в сетях. На практике постоянно приходится сталкиваться с различного рода сетями - например, транспортные сети, сети связи, электрические сети и т.п., поэтому математическое изучение таких сетей имеет важное прикладное значение. В теории сетей большую роль играют графические методы. Предварительно рассмотрим пример.

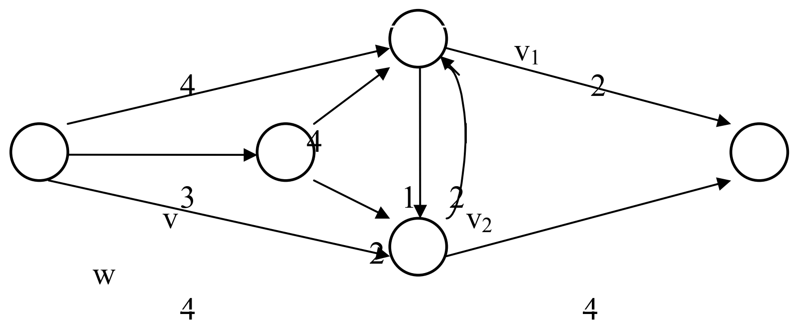


Рис. 1.

Пусть отправитель v хотел бы послать получателю w несколько предметов. Числа на дугах графа на рис. 1 обозначают максимальное число предметов, которое можно послать по соответствующим каналам. Для отправителя v представляет существенный интерес знать, какое максимальное количество предметов он может послать, не превышая допустимую пропускную способность каждого канала.

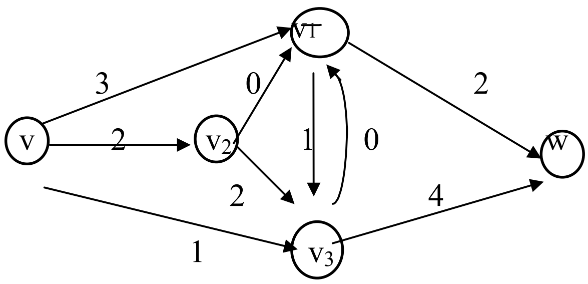
Будем называть <u>сетью</u> N ориентированный граф, каждой дуге которого e приписано неотрицательное действительное число ω(e), называемое ее пропускной способностью. Другими словами, сеть N есть пара (Γ, ω), где - Γ - ориентированный граф, а ω - функция, отображающая множество дуг графа Γ в множество неотрицательных действительных чисел. По аналогии с терминологией для ориентированных графов можно определить <u>полустепень исхода</u> вершины v для сети N как сумму пропускных способностей дуг вида (v, x). Аналогично определяется <u>полустепень захода</u> вершины. Ясно, что сумма полустепеней исхода всех вершин в сети равна сумме полустепеней захода.

Будем предполагать, что ориентированный граф Γ содержит точно одну вершину v, у которой полустепень захода равна нулю, и точно одну вершину ω, у которой полустепень исхода равна нулю. Эти вершины называются <u>источником</u> и <u>стоком</u> соответственно.

Пусть дана сеть N = (Г, ω). Определим поток через сеть как функцию φ, сопоставляющую каждой дуге e из Г неотрицательное действительное число φ(e), которое называется потоком через e, причем функция φ удовлетворяет условиям:

1) φ(e) ≤ ω(e) для любой дуги e.

2) В сети (Г, φ) полустепень исхода равна полустепени захода для любой вершины, отличной от источника и стока. Данные условия означают, что поток через любую дугу не превышает ее пропускной способности и что поток “входящий” в любую вершину (отличную от источника и стока) равен “исходящему” из нее потоку. Ясно, что сумма потоков через дуги, инцидентные источнику, равна сумме потоков через дуги, инцидентные стоку. Эта сумма называется величиной потока. Нас будут интересовать потоки, имеющие наибольшее значение, эти потоки называются максимальными. Например, для сети на рис. 2 максимальным потоком будет поток, равный 6. Он изображен на рис. 2 ниже.



Для сети N = (Г,ω) определим понятие разреза, как такого множества A дуг графа Г, что любая ориентированная простая цепь из v в ω содержит дугу из A. Пропускной способностью разреза A называется сумма пропускных способностей принадлежащих A дуг. Минимальным называется такой разрез, у которого пропускная способность принимает наименьшее значение. Например, для сети на рис. 1 множество дуг (v_1, ω), (v_3, ω) является разрезом. Его пропускная способность равна 6, т.е. совпадает с величиной максимального потока. Дуга e, для которой φ(e) = ω(e), называется насыщенной. Поток, при котором φ(e) = 0 для всех дуг e, называется нулевым.

Заметим, что величина любого потока не превышает пропускной способности любого разреза и, значит, величина максимального потока не превосходит пропускной способности минимального разреза. Оказывается, что эти два числа равны между собой. Соответствующий результат известен, как теорема Форда-Фалкерсона.

Теорема 1. Во всякой сети величина минимального разреза потока равна пропускной способности любого минимального разреза.

♦ В силу замечания о том, что величина любого максимального потока не превышает пропускной способности любого минимального разреза, достаточно доказать, что существует разрез, пропускная способность которого равна величине данного максимального потока. Действительно, путь φ - максимальный поток. Определим два множества вершин сети V и W следующим образом: пусть G - скелетный граф для графа Г. Тогда вершину z сети N включаем в множество V тогда и только тогда, когда в G существует простая цепь из v в z: $v = v_0, v_1, \dots, v_{m-1}, v_m = z$, обладающая тем свойством, что любое ее ребро $\{v_i, v_{i+1}\}$ соответствует либо не насыщенной дуге (v_i, v_{i+1}), либо дуге (v_{i+1}, v_i), через которую проходит не нулевой поток. Очевидно, что множество V содержит вершину v. Пусть множество W есть дополнение множества V в множестве вершин сети N. Покажем, что множество W содержит вершину w. Если это не так, то w принадлежит множеству V. Значит существует простая цепь $v, v_1, \dots, v_{m-1}, w$ такая, что ребро $\{v_i, v_{i+1}\}$ соответствует либо ненасыщенной дуге (v_i, v_{i+1}), либо дуге (v_{i+1}, v_i) с ненулевым потоком. Определим положительное число ε, удовлетворяющее условиям:

а) Для дуг первого типа число ε не превышает величину разности пропускной способности каждой дуги и соответствующего ей потока.

б) Для дуг второго типа число ε не превышает величины потока через каждую из них.

Теперь заметим, что если потоки через дуги первого типа увеличить на ε, а потоки через дуги второго типа уменьшить на ε, то величина потока φ увеличится и станет равной $\varphi + \varepsilon$. Однако это противоречит предположению о максимальности потока φ. Значит w содержится в множестве W.

Обозначим теперь через R множество дуг вида (x, y), где $x \in V$, $y \in W$. Ясно, что R является разрезом. Далее, каждая дуга (x, y) из R является насыщенной, поскольку в противном случае y должна принадлежать множеству V. Значит сумма потоков дуг по разрезу R равна его пропускной способности, а с другой стороны, равна величине потока. Значит R и есть искомый разрез. ♦

Данная теорема еще не дает алгоритма построения максимального потока через сеть. Приведем такой алгоритм для целочисленного потока. Алгоритм построения максимального потока состоит из трех этапов.

1. Отыскание какого-нибудь потока. Строим произвольный поток φ, удовлетворяющий условиям сохранения потока в каждой внутренней вершине и условиям на пропускную способность дуг. За φ можно взять нулевой поток.

2. Отыскание полного потока, т.е. такого потока, у которого любой ориентированный путь из v в w содержит насыщенную дугу. Если поток φ не полный, то существует путь из v в w, все дуги которого не насыщены. Увеличивая поток по этому пути до насыщения одной из дуг получаем новый поток φ', величина которого превосходит исходный поток.

3. Отыскание максимального потока. Для этого применяем следующую процедуру.

3.1. Помечаем вершину v символом o. Если вершина v_i помечена, то помечаем символом + i все непомеченные вершины, в которое из v_i идут не насыщенные дуги, и символом - i все непомеченные вершины, из которых идут дуги в вершину v_i с ненулевым потоком.

3.2. Если продолжая таким образом, вершина w оказалась помеченной, то это означает, что существует цепь из v в w, все вершины которой помечены. Увеличивая поток во всех дугах цепи на 1, у которых направление совпадает с прохождением пути, и уменьшая поток на 1 во всех дугах, направление которых обратно прохождению пути. Ясно, что поток в сети увеличивается на 1. Повторяем шаги 3.1. и 3.2. до тех пор, пока вершину w удается пометить.

Если при некотором потоке φ, вершину w не удается пометить, то поток φ будет максимальным. Действительно, если через V обозначить множество помеченных вершин, а через W - множество непомеченных, причем

$x \in V$, $w \in W$, то множество дуг R вида (x, y), где $x \in V$, $y \in W$ будет разрезом. При этом все такие дуги (x, y) будут насыщенными, в противном случае y была бы помечена. Значит φ - максимальный поток. Рассмотрим одно приложение данных результатов. Паросочетанием в неориентированном графе G(V, E) называется произвольное множество ребер $M \subseteq E$, такое, что никакие два ребра из M не имеют общей вершины. Особый интерес представляет нахождение паросочетаний для двудольных графов, поскольку этот вопрос возникает в задачах теории связи. Покажем, как задача нахождения наибольшего паросочетания в двудольном графе сводится к построению максимального потока в некоторой сети. Пусть $H = (V_1, V_2, E)$ - произвольный двудольный граф. Это означает, что $V_1 \bigcap V_2 = \varnothing$ и каждое ребро $e \in E$ имеет вид (x, y), $x \in V_1$, $y \in V_2$.

Построим сеть S(H) следующим образом:

1. Добавим вершины s (источник) и t (сток).

2. Добавим дуги от s к каждой вершине $x \in V_1$ и дуги от каждой вершины $y \in V_2$ к t.

3. Ориентируем ребра $e \in E$, $e=(x,y)$ от x к y.

4. Припишем всем дугам пропускную способность 1.

Согласно изложенному выше, для сети S(H) существует максимальный поток φ.

Теорема 2. Существует взаимно однозначное соответствие между паросочетаниями в H и потоками в S(H), при котором паросочетанию M мощности k соответствует поток величины k, причем соответствие устанавливается так:

Паросочетание $M = \{(x_1, y_1), \dots , (x_k, y_k)\}$ мощности k	$\Rightarrow$	Поток $\varphi(s, x_i) = \varphi(x_i, y_i) = \varphi(y_i, t) = 1$ величины k $\varphi(e) = 0$ (1) для остальных дуг
Поток φ величины k	$\Rightarrow$	Паросочетание $M= \{(x, y)\}$, $x\in V_1, y \in V_2$ мощности k $\varphi(x, y) = 1$ (2)

♦ Пусть $M = \{(x_1, y_1), \dots , (x_k, y_k)\}$ - паросочетание мощности k. Тогда вершины $x_1, \dots , x_k$ и вершины $y_1, \dots , y_k$ попарно различны. Отсюда следует, что функция φ, определенная (1), является потоком из s в t. Далее, разным паросочетаниям M соответствуют разные потоки φ. С другой стороны, если φ - поток в сети S(H), то количество потока, прибывающего (а значит, убывающего) в каждую вершину $x \in V_1$ не превосходит единицы, т.к. единственная дуга, входящая в x - это дуга (s, x) с пропускной способностью, равной 1. Отсюда следует, что в множестве M, определенном (2) нет ребер вида (x, y_1), (x, y_2),
$y_1 \neq y_2$. Аналогично в M нет ребер вида (x_1, y), (x_2, y), $x_1 \neq x_2$. Следовательно, M - паросочетание в H. Легко заметить, что отображения, определенные (1) и (2), являются обратными друг к другу. ♦

Таким образом, для построения максимального паросочетания можно использовать алгоритм построения максимального потока.

Упражнения.

1. Доказать, что если число ребер графа с вершинами ($n > 2$) больше, чем $\binom{n-1}{2}$, то он связен.

2. Доказать, что если степень каждой вершины G не меньше двух, то G содержит цикл.

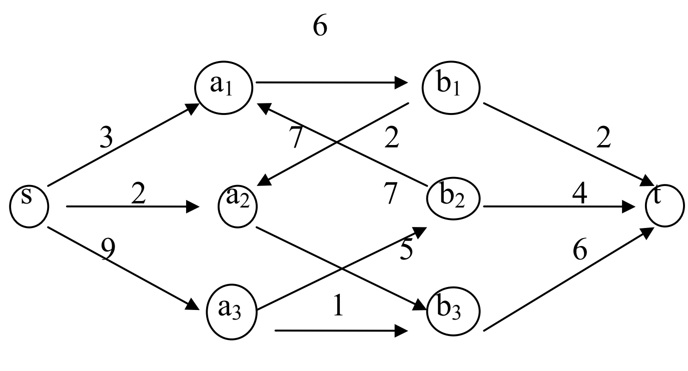
3. Выяснить, при каких m, n графы $K_{m,n}$ (полный двудольный граф с m и n вершинами в долях), K_n (полный граф на n вершинах), B_n (граф единичного куба) являются эйлеровыми.

4. Доказать, что графы K_n , $K_{n,n}$, B_n являются гамильтоновыми.

5. Индукцией по n доказать, что каждое дерево с $n \geq 2$ вершинами является двудольным графом.

6. Найти число остовных деревьев графа де Брейна с $n = 3$.

7. Найти максимальный поток в графе



ЛИТЕРАТУРА

[1] Холл. М. Комбинаторика. М., Мир, 1970.

[2] Райзер Г.Дж. Комбинаторная математика, М., Мир, 1966.

[3] Рыбников К.А. Введение в комбинаторный анализ. М., МГУ, 1985.

[4] Айгнер М. Комбинаторная теория. М., Мир, 1982.

[5] Липский В. Комбинаторика для программистов, М., Мир, 1988.

[6] Оре О. Теория графов. М., Наука, 1968.

[7] Харари Ф. Теория графов. М., Мир, 1973.

[8] Форд Л.Р., Фалкерсон Д.Р. Потоки в сетях, М., Мир, 1963.

[9] Уилсон Р. Введение в теорию графов, М., 1977.

[10] Кофман А. Введение в прикладную комбинаторику. М., 1975.

[11] Комбинаторный анализ. Задачи и упражнения. Под ред. Рыбникова К.А., М., 1982

[12] Гаврилов Г.П., Сапоженко А.А. Задачи и упражнения по курсу дискретной математики, М., Наука, 1992.