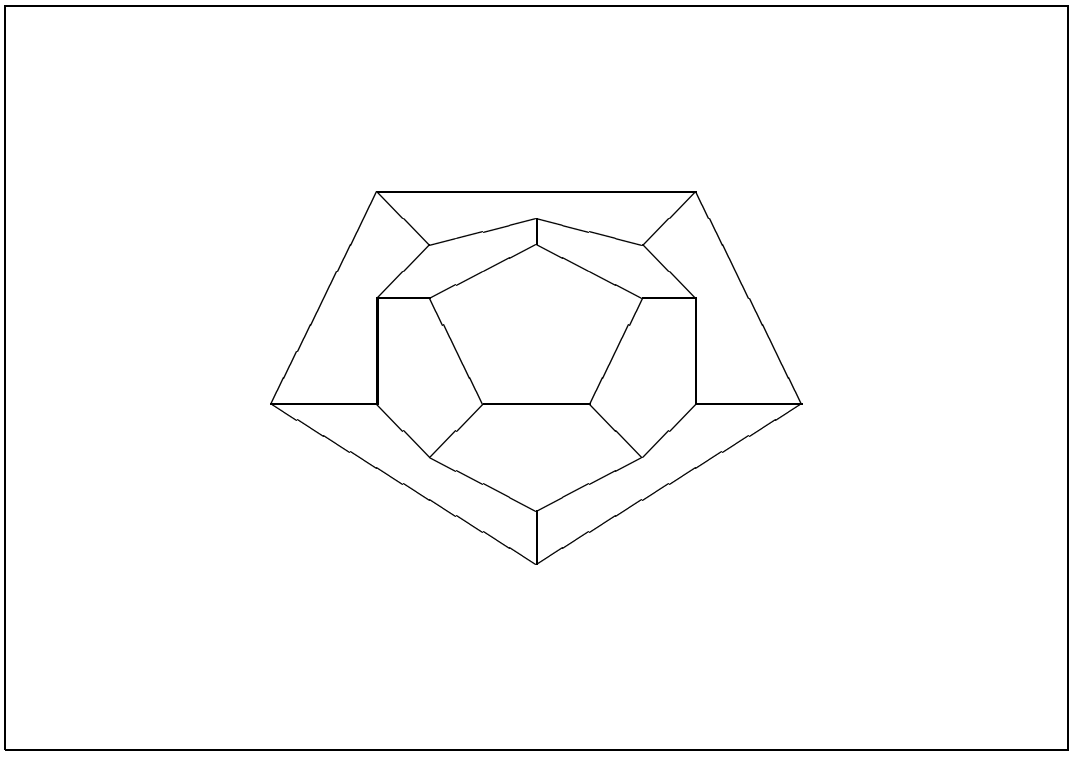
Ю.Н.Мальцев, Е.П.Петров

ВВЕДЕНИЕ В ДИСКРЕТНУЮ МАТЕМАТИКУ

ЭЛЕМЕНТЫ КОМБИНАТОРИКИ, ТЕОРИИ ГРАФОВ И ТЕОРИИ КОДИРОВАНИЯ



Барнаул · 1997

МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО
ОБРАЗОВАНИЯ РФ
АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Ю.Н.МАЛЬЦЕВ, Е.П.ПЕТРОВ

ВВЕДЕНИЕ В ДИСКРЕТНУЮ МАТЕМАТИКУ

ЭЛЕМЕНТЫ КОМБИНАТОРИКИ, ТЕОРИИ ГРАФОВ И ТЕОРИИ КОДИРОВАНИЯ

Издательство Алтайского
государственного университета
Барнаул – 1997

УДК 510.51

Введение в дискретную математику (элементы комбинаторики, теории графов и теории кодирования): Учебное пособие. // Ю.Н.Мальцев, Е.П.Петров. Барнаул: Изд-во Алт. ун-та, 1997. 135 с.

Цель данного пособия – изложить студентам математического факультета основные разделы дискретной математики в соответствии с новой программой. В пособии приведено большое количество примеров и задач, многие из которых снабжены указаниями к решению.

Авторы выражают благодарность генеральному директору фирмы "Байт" А.М.Стрыгину за финансовую помощь.

Табл. 9. Ил. 80. Библиогр. 29 назв.

ОГЛАВЛЕНИЕ

Глава 1

ЭЛЕМЕНТЫ КОМБИНАТОРИКИ

Комбинаторика – раздел математики, посвященный решению задач выбора и расположения элементов некоторого множества в соответствии с заданными условиями. Элементы комбинаторики встречались в трудах математиков Древнего Востока (число сочетаний, бином Ньютона). Б.Паскаль и П.Ферма являлись основоположниками комбинаторики как раздела математики. Большой вклад в развитие комбинаторики внесли Г.Лейбниц, Я.Бернулли, Л.Эйлер, Ф.Холл, Г.Пойа, Р.Дилуорс.

1.1 Перестановки, сочетания, полиномиальная теорема

Рассмотрим конечное множество $M = \{a_1, \ldots, a_n\}$, содержащее n элементов. Сочетание – подмножество M, т.е. некоторая неупорядоченная выборка различных элементов из M. Обозначим через C_n^k (или через $\binom{n}{k}$) число всех сочетаний, содержащих k элементов. Другими словами, C_n^k – число всех k-элементных подмножеств n-элементного множества M.

Утверждение 1. $C_n^k = \frac{n!}{k!(n-k)!}$.

Доказательство проведем индукцией по числу $n \geq k$.

Если $n = k$, то $C_k^k = 1 = \frac{k!}{k!0!}$. Предположим истинность нашей формулы для n-элементных множеств. Докажем ее справедливость для множества $A = \{a_1, \ldots, a_n, a_{n+1}\}$, содержащего $(n+1)$ элементов. Каждое k-элементное

подмножество A либо содержит a_{n+1}, либо не содержит a_{n+1}. Число подмножеств первого типа равно C_n^{k-1}, т.к. каждое такое подмножество однозначно определяется сочетанием из $(k-1)$ элемента в $\{a_1, \ldots, a_n\}$. Число подмножеств второго типа равно, очевидно, C_n^k. Следовательно, $C_{n+1}^k = C_n^k + C_n^{k-1} = \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} = \frac{n!}{(k-1)!(n-k)!}[\frac{1}{k} + \frac{1}{n-k+1}] = \frac{(n+1)!}{k!(n+1-k)!}$. Обозначим, далее, через P_n число всех упорядоченных n-ок $\{(a_{i_1}, \ldots, a_{i_n});\, a_{i_j} \in M, a_{i_s} \neq a_{i_t}\}$ множества M. Такие n-ки мы будем называть перестановками. Докажем, что $P_n = n!$. Воспользуемся методом математической индукции. Если $n = 1$, то $P_1 = 1 = 1!$. Предположим истинность искомого равенства для n-элементных множеств и докажем его справедливость для $(n+1)$-элементного множества $A = \{a_1, \ldots, a_{n+1}\}$. Множество всех перестановок элементов A можно разбить на $(n+1)$ непересекающихся классов $C_1, \ldots, C_{n+1}$. Именно, отнесем в класс C_i те (и только те) перестановки, которые содержат a_{n+1} на i-м месте

$$(a_{j_1}, a_{j_2}, \ldots, a_{j_{i-1}}, a_{n+1}, a_{j_{i+1}}, a_{j_{i+2}}, \ldots, a_{j_{n+1}}).$$

Ясно, что $|C_i| = n!$ и $P_{n+1} = |C_1| + |C_2| + \cdots + |C_{n+1}| = (n+1) \cdot n! = (n+1)!$. Обозначим через P_n^r число всех упорядоченных выборок, содержащих r различных элементов множества M (иногда это число обозначается как $P(n,r), A_n^r$ или ${}_nP_r$). Число всех r-элементных подмножеств M равно C_n^r и каждое такое подмножество порождает $r!$ упорядоченных искомых выборок, т.е. $P_n^r = C_n^r \cdot r! = \frac{n!}{(n-r)!}$. Подсчитаем число всех упорядоченных r-множеств $\{(a_1, \ldots, a_r);\, a_i \in M\}$. Каждая координата (независимо) пробегает все множество M. Поэтому число всех таких r-выборок равно n^r.

Замечание. Из предыдущего следует, что число всех подмножеств n-множества (т.е. n-элементного множества) равно $(C_n^0 + C_n^1 + \cdots + C_n^n)$. Неупорядоченная совокупность из r элементов $\{a_1, a_2, \ldots, a_r\}$ множества M (не обязательно различных) называется r-выборкой из M. Две r-выборки равны, если каждый элемент входит в обе выборки одинаковое число раз. r-выборка, содержащая каждый элемент один раз является r-подмножеством

или r-сочетанием.

Утверждение 2. *Число r-выборок из n-множества равно C^r_{n+r-1}.*

ДОКАЗАТЕЛЬСТВО.

Пусть $M = \{1, 2, \ldots, n\}$ и $M^* = \{1, 2, \ldots, n, n+1, \ldots, n+r-1\}$. Соответствие $\{a_1, a_2, \ldots, a_r\} \longleftrightarrow \{a_1+0, a_2+1, \ldots, a_r+(r-1)\}$, где $a_1 \le a_2 \le \cdots \le a_r$, является биективным соответствием между множеством всех r-выборок из M и r-сочетаний из M^*. По утверждению 1, искомое число равно C^r_{n+r-1}.

Подсчитаем число различных перестановок символов

$$\underbrace{a, \ldots, a}_{\alpha_1}, \underbrace{b, \ldots, b}_{\alpha_2}, \ldots, \underbrace{c, \ldots, c}_{\alpha_k} \quad ,$$

где $\sum\limits_{i=1}^{k} \alpha_i = n$. Число всех перестановок символов

$$a_1, \ldots, a_{\alpha_1}, b_1, \ldots, b_{\alpha_2}, \ldots, c_1, \ldots, c_{\alpha_k}$$

равно $n!$. Отождествляя $a_1 = \cdots = a_{\alpha_1} = a$, мы уменьшаем это число в $\alpha_1!$ раз; отождествляя, далее, $b_1 = \cdots = b_{\alpha_2} = b$, мы уменьшаем предыдущее число еще в $\alpha_2!$ раз и т.д. Поэтому искомым числом будет

$$P^n(\alpha_1, \ldots, \alpha_k) = \frac{n!}{\alpha_1! \alpha_2! \ldots \alpha_k!}.$$

Утверждение 3 (полиномиальная теорема). *Справедливо следующее равенство многочленов*

$$(x_1 + \cdots + x_k)^n = \sum_{\alpha_1 + \cdots + \alpha_k = n} \frac{n!}{\alpha_1! \ldots \alpha_k!} x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k}.$$

ДОКАЗАТЕЛЬСТВО. Рассмотрим левую часть равенства

$$(x_1 + \cdots + x_k)^n = \underbrace{(x_1 + \cdots + x_k) \ldots (x_1 + \cdots + x_k)}_{n} =$$

$$= \sum_{\alpha_1 + \cdots + \alpha_k = n} A(\alpha_1, \ldots, \alpha_k) x_1^{\alpha_1} \cdots x_k^{\alpha_k},$$

где коэффициент $A(\alpha_1, \ldots, \alpha_k)$ равен числу всех таких наборов

$(\alpha_1, \ldots, \alpha_k)$, что $\alpha_1 + \cdots + \alpha_k = n$. Подсчитаем это число. Переменную x_1 можно выбрать в α_1 множителях (из n возможных!), т.е. $C_n^{\alpha_1}$ способами. Переменную x_2 можно (независимо) выбрать в α_2 в оставшихся $(n - \alpha_1)$ множителях и т.д. Таким образом,

$$A(\alpha_1, \ldots, \alpha_k) = C_n^{\alpha_1} \cdot C_{n-\alpha_1}^{\alpha_2} \cdot \cdots \cdot C_{n-(\alpha_1+\cdots+\alpha_{k-1})}^{\alpha_k} = \\ = \frac{n!}{\alpha_1!(n-\alpha_1)!} \cdot \frac{(n-\alpha_1)!}{\alpha_2!(n-\alpha_1-\alpha_2)!} \cdot \cdots \cdot \frac{(n-(\alpha_1+\cdots+\alpha_{k-1}))!}{\alpha_k!0!} = \frac{n!}{\alpha_1!\alpha_2!\ldots\alpha_k!}.$$

В частности, $(x_1 + x_2)^n = \sum\limits_{k=0}^{n} C_n^k x_1^k x_2^{n-k}$ – классическая формула бинома Ньютона.

ЗАДАЧИ

1). Число всех подмножеств n-множества равно 2^n.

УКАЗАНИЕ. Воспользоваться равенством

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

2). Доказать, что

$$C_n^0 + C_n^2 + C_n^4 + \cdots = C_n^1 + C_n^3 + C_n^5 + \cdots \ .$$

УКАЗАНИЕ. Рассмотреть бином $(1-1)^n = 0$.

3). Доказать равенство $C_{r+s}^m = \sum\limits_{i=0}^{m} C_r^i C_s^{m-i}$.

УКАЗАНИЕ 1. Рассмотреть тождество

$$(1+x)^r(1+x)^s = (1+x)^{r+s}.$$

УКАЗАНИЕ 2. Рассмотреть число способов выбора комиссии из m человек в группе, состоящей из r женщин и s мужчин.

4). Сколько различных пятизначных чисел можно составить при помощи цифр 1,2,3 ?

ОТВЕТ: 3^5.

5). Сколько различных семизначных чисел можно составить из цифр

2,2,3,3,3,0,4?

ОТВЕТ: $\frac{7!}{2!3!} - \frac{6!}{2!3!} = 360$.

6). В оранжерее имеются цвета 10 наименований. Сколькими способами можно составить букет из 20 цветов?

ОТВЕТ: $C^{20}_{10+20-1} = 10015005$.

7). Из группы, состоящей из 7 мужщин и 4 женщин, надо выбрать 6 человек так, чтобы среди них было не менее 2-х женщин. Сколькими способами это можно сделать?

ОТВЕТ: $C^2_4 \cdot C^4_7 + C^3_4 \cdot C^3_7 + C^4_4 \cdot C^2_7 = 371$.

8). Найти число всех натуральных делителей числа $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, где $p_1, \ldots, p_s$ – различные простые числа.

ОТВЕТ: $(\alpha_1 + 1) \cdots (\alpha_s + 1)$.

9). Доказать, что $\sum\limits_{k=1}^{n} C^k_n \cdot k = 2^{n-1} \cdot n$.

УКАЗАНИЕ. Рассмотреть $f(x) = (1+x)^n$ и ее производную $f'(x)$.

10). Доказать равенство

$$4 \cdot \sum_k C^{4k}_n = 2^n + 2^{\frac{n}{2}+1} \cdot cos\frac{\pi n}{4}.$$

УКАЗАНИЕ. Рассмотреть равенство

$$(1+1)^n + (1+i^2)^n + (1+i)^n + (1+i^3)^n = 4 \cdot \sum_k C^{4k}_n.$$

11). Из колоды, содержащей 52 карты, вынули 10 карт. В скольких случаях среди этих карт окажется:

а) хотя бы один туз;

б) ровно один туз;

в) не менее 2-х тузов;

г) ровно 2 туза.

ОТВЕТ:

а) $C^1_4 \cdot C^9_{48} + C^2_4 \cdot C^8_{48} + C^3_4\ C^7_{48} + C^4_4 \cdot C^6_{48}$; б) $C^1_4 \cdot C^9_{48}$ и т.д.

1.2 Рекуррентные соотношения и производящие функции

Пусть F – некоторое поле и $\{u_0, u_1, \dots\}$ – последовательность чисел из F. Скажем, что эта последовательность является рекуррентной порядка r, если существуют числа $a_1, \dots, a_r \in F$ такие, что

$$u_r = a_1 u_{r-1} + a_2 u_{r-2} + \cdots + a_r \cdot u_0,$$

$$u_{r+1} = a_1 u_r + a_2 u_{r-1} + \cdots + a_r \cdot u_1,$$

$$\cdots\cdots\cdots$$

$$u_{n+r} = a_1 \cdot u_{n+r-1} + \cdots + a_r \cdot u_n,$$

$$\cdots\cdots\cdots$$

где $n = 0, 1, 2, \dots$. Для рекуррентной последовательности $\{u_n\}$ многочлен $f(x) = x^r - a_1 x^{r-1} - \cdots - a_r = (x - \alpha_1)^{e_1} \dots (x - \alpha_s)^{e_s}$, где $\sum\limits_{i=1}^{s} e_i = r$, $\alpha_1, \dots, \alpha_s \in \bar{F}$, называется характеристическим ($\bar{F}$ - алгебраическое замыкание поля F; например, $\bar{\mathbf{C}} = \mathbf{C}, \bar{\mathbf{R}} = \mathbf{C}$). Рассмотрим, далее, множество $F\langle\langle x\rangle\rangle = \{\sum\limits_{i=0}^{\infty} v_i x^i; v_i \in F\}$ всех формальных степенных рядов от переменной x с коэффициентами из поля F. Определим на этом множестве следующие операции:

$$(\sum_{i=0}^{\infty} v_i x^i) + (\sum_{i=0}^{\infty} w_i x^i) \doteq \sum_{i=0}^{\infty} (v_i + w_i) x^i,$$

$$(\sum_{i=0}^{\infty} v_i x^i)(\sum_{i=0}^{\infty} w_i x^i) = \sum_{i=0}^{\infty} q_i x^i,$$

где $q_i = \sum\limits_{t=0}^{i} v_t w_{i-t}$. Легко видеть, что $\langle F\langle\langle x\rangle\rangle, +, .\rangle$ является ассоциативным и коммутативным кольцом с единицей $1 = 1 + 0 \cdot x + 0 \cdot x^2 + \cdots$, не содержащим делителей нуля (т.е. если $\alpha \cdot \beta = 0$, где $\alpha, \beta \in F\langle\langle x\rangle\rangle$, либо $\alpha = 0$, либо $\beta = 0$). При этом ряд $\sum\limits_{i=0}^{\infty} v_i x^i$ является обратимым в том и только том случае, если $v_0 \neq 0$. С каждой последовательностью $\{u_n\}$ свяжем ряд

$$g(x) = u_0 + u_1 x + u_2 x^2 + \dots,$$

который назовем производящей функцией для $\{u_n\}$. Предположим, что последовательность $\{u_n\}$ является рекуррентной. Положим

$$\varphi(x) = x^r f(\frac{1}{x}) = 1 - a_1 x - a_2 x^2 - \cdots - a_r x^r$$

и рассмотрим произведение $g(x) \cdot \varphi(x) = (\sum\limits_{i=0}^{\infty} u_i x^i)\ (1 - a_1 x - \cdots - a_r x^r) =$
$= u_0 + (u_1 - a_1 u_0)x + (u_2 - a_1 u_1 - a_2 u_0)x^2 + \cdots + (u_{r-1} - a_1 u_{r-2} - \cdots -$
$\cdots - a_{r-1} u_0)x^{r-1} + (u_r - a_1 u_{r-1} - \cdots - a_r \cdot u_0)x^r + \cdots + (u_{n+r} - a_1 u_{n+r-1} - \cdots -$
$-a_r \cdot u_n)x^{n+r} + \cdots = b_0 + b_1 x + \cdots + b_{r-1} x^{r-1} = \psi(x)$. Следовательно,
$g(x) = \frac{\psi(x)}{\varphi(x)} = \frac{\psi(x)}{(1-\alpha_1 x)^{e_1} \cdots (1-\alpha_s x)^{e_s}}$. Правая часть этого равенства является правильной дробью в $\bar{F}(x)$ и, следовательно, разложима в сумму конечного числа простейших дробей, т.е. дробей вида $\frac{A}{(1-\alpha_i x)^t}$, где $A \in \bar{F}, t \le e_i$. Итак,

$$\begin{gathered} g(x) = \frac{\beta_{11}}{(1-\alpha_1 x)} + \frac{\beta_{12}}{(1-\alpha_1 x)^2} + \cdots + \frac{\beta_1 e_1}{(1-\alpha_1 x)^{e_1}} + \\ + \frac{\beta_{21}}{(1-\alpha_2 x)} + \frac{\beta_{22}}{(1-\alpha_2 x)^2} + \cdots + \frac{\beta_2 e_2}{(1-\alpha_2 x)^{e_2}} + \cdots + \\ + \frac{\beta_{s1}}{(1-\alpha_s x)} + \frac{\beta_{s2}}{(1-\alpha_s x)^2} + \cdots + \frac{\beta_{ses}}{(1-\alpha_s x)^{e_s}}. \end{gathered} \tag{1.1}$$

Так как
$\frac{1}{(1+x)^k} = 1 - k \cdot x + \cdots + \frac{(-k)(-k-1)\cdots(-k-(n-1))\cdot x^n}{n!} + \cdots =$
$= 1 - C_k^{k-1} x + C_{k+1}^{k-1} x^2 - \cdots + (-1)^n \cdot C_{n+k-1}^{k-1} x^n + \cdots$,
то $\frac{\beta}{(1-\alpha x)^k} = \beta + \sum\limits_{n=1}^{\infty} C_{n+k-1}^{k-1} \cdot \beta \cdot \alpha^n \cdot x^n$. Приравнивая коэффициенты при x^n в левой и правой части равенства (1), имеем, что

$$u_n = q_1(n)\alpha_1^n + q_2(n)\alpha_2^n + \cdots + q_s(n)\alpha_s^n,$$

где $q_i(n)$ – многочлен от n степени $\le e_i - 1$, коэффициенты которых определяются начальными значениями $u_0, u_1, \ldots, u_{r-1}$ нашей последовательности. Таким образом, мы указали алгоритм вычисления членов рекуррентной последовательности с помощью производящих функций. Приведем примеры работы этого алгоритма.

Пример 1. Пусть $u_0 = 1,\ u_1 = 1,\ u_n = u_{n-1} + u_{n-2}$, где $n \ge 2$ (последовательность Фибоначчи). Характеристический многочлен $f(x) = x^2 - x - 1$

имеет корни $\alpha = \frac{1+\sqrt{5}}{2}$ и $\beta = \frac{1-\sqrt{5}}{2}$. Следовательно,

$k(x) = (1-\alpha x)(1-\beta x)$ и $g(x)\cdot k(x) = (\sum\limits_{n=0}^{\infty} u_n x^n)(1-x-x^2) =$

$$= u_0 + (u_1 - u_0)x + (u_2 - u_1 - u)x^2 + \cdots = 1.$$

Таким образом,

$g(x) = \frac{1}{(1-\alpha x)(1-\beta x)} = \frac{\alpha/(\alpha-\beta)}{(1-\alpha x)} + \frac{\beta/(\beta-\alpha)}{(1-\beta x)} = \frac{1}{\sqrt{5}}\big[\frac{\alpha}{1-\alpha x} - \frac{\beta}{(1-\beta x)}\big] =$

$= \frac{1}{\sqrt{5}}\big[\alpha(1+\alpha x+\alpha^2x^2+\alpha^3x^3+\cdots) - \beta(1+\beta x+\beta^2x^2+\cdots)\big] =$

$= \frac{1}{\sqrt{5}}\big\{(\alpha-\beta) + (\alpha^2-\beta^2)x + \cdots + (\alpha^{n+1}-\beta^{n+1})x^n + \cdots\big\}$. Следовательно,

$u_n = \frac{1}{\sqrt{5}}(\alpha^{n+1}-\beta^{n+1}) = \frac{1}{\sqrt{5}}\big\{(\frac{\sqrt{5}+1}{2})^{n+1} - (\frac{1-\sqrt{5}}{2})^{n+1}\big\}$ (формула Бине).

Замечание. Укажем идею другого метода вычисления общего члена рекуррентной последовательности порядка два на примере последовательности

$$u_0 = 1,\ u_1 = 2,\ u_{n+1} = 8u_n - 15u_{n-1},\ n \geq 1.$$

Найдем числа α, β такие, что $8 = \alpha + \beta,\ 15 = \alpha\beta$ (ясно, что $\alpha = 3,\ \beta = 5$). Перепишем равенство $u_{n+1} = 8u_n - 15u_{n-1}$ в виде

$$u_{n+1} - 5u_n = 3(u_n - 5u_{n-1}),$$

$$u_{n+1} - 3u_n = 5(u_n - 3u_{n-1}).$$

Из последних равенств следует, что

$u_{n+1} - 5u_n = 3\{3(u_{n-1} - 5u_{n-2})\} = 3^2(u_{n-1} - 5u_{n-2}) = \cdots =$

$$= 3^{n-1}(u_2 - 5u_1) = 3^n(u_1 - 5u_0) = -3^{n+1},$$

$u_{n+1} - 3u_n = 5\{5(u_{n-1} - 3u_{n-2})\} = 5^2(u_{n-1} - 3u_{n-2}) = \cdots =$

$$= 5^n(u_1 - 3u_0) = -5^n.$$

Откуда следует, что $u_n = \frac{3^{n+1}-5^n}{2}$.

Пример 2. Рассмотрим рекуррентную последовательность порядка 3:

$$u_0 = +1,\ u_1 = 5,\ u_2 = 10,$$

$$u_{n+3} = u_{n+2} + 5u_{n+1} + 3u_n,\ n \geq 0.$$

Найдем формулу n-ого члена этой последовательности. Заметим, что характеристический многочлен $f(x) = x^3 - x^2 - 5x - 3$ имеет корни $3, -1, -1$.

Поэтому $(u_0 + u_1x + u_2x^2 + \dots)(1 - x - 5x^2 - 3x^3) = u_0 + (u_1 - u_0)x + +(u_2 - u_1 - 5u_0)x^2 + 0 \cdot x^3 + 0 \cdot x^4 + \dots = 1 + 4x$. Следовательно, производящая функция $g(x)$ равна дроби $\frac{1+4x}{(1-3x)(1+x)^2}$. Разложим эту правильную дробь в сумму простейших

$$\frac{1+4x}{(1-3x)(1+x)^2} = \frac{A}{(1-3x)} + \frac{B}{(1+x)} + \frac{C}{(1+x)^2}.$$

Приводя к общему знаменателю в правой части и приравнивая коэффициенты при соответствующих степенях числителей, мы получим систему уравнений

$$A + B + C = 1$$

$$A - 3B = 0$$

$$2A - 2B - 3C = 4,$$

из которой следует, что $A = 21/16, B = 7/16, C = -3/4$. Следовательно, $g(x) = 1 + 5x + \dots + (\frac{21}{16} \cdot 3^n + \frac{7}{16}(-1)^n + \frac{3}{4}(n+1)(-1)^{n+1})x^n + \dots$. Поэтому $u_n = \frac{21}{16} \cdot 3^n + \frac{7}{16}(-1)^n + \frac{3}{4}(n+1)(-1)^{n+1}$, где $n \geq 0$.

ЗАДАЧИ

1). Найти общий член следующих рекуррентных последовательностей

а) $u_0 = -2,\ u_1 = 3,\ u_{n+1} = 10u_n - 9u_{n-1},\ n \geq 1$;

б) $u_0 = 1,\ u_1 = 2,\ u_2 = 0,\ u_3 = -1,$

$$u_{n+4} = 3u_{n+3} + 3u_{n+2} - 7u_{n+1} - 6u_n,\ n \geq 0.$$

2). Сколькими способами можно расставить скобки в (неассоциативном) слове $a_1a_2 \dots a_n$?

УКАЗАНИЕ. Обозначим через u_n число таких способов. Положим $u_0 = 0,\ u_1 = 1$. Тогда $u_2 = 1,\ u_3 = 2,\ u_4 = 5$, так как имеем следующие расстановки скобок

$$(a_1a_2)a_3, a_1(a_2a_3),$$

$$((a_1a_2)a_3)a_4, (a_1a_2)(a_3a_4), a_1(a_2(a_3a_4)),$$

$$(a_1(a_2a_3))a_4, a_1((a_2a_3)a_4).$$

Заметим, что $u_n = u_1u_{n-1} + u_2u_{n-2} + \cdots + u_{n-1}u_1,\ n \geq 2$. Из этого равенства следует следующее соотношение для производящей функции $f(x) = \sum\limits_{i=0}^{\infty} u_i x^i :\ f(x)^2 = f(x) - x$. Откуда следует, что $f(x) = \frac{1-\sqrt{1-4x}}{2}$ (ряд $f(x)$ удовлетворяет условию $f(0) = 0$). Следовательно, $u_n = \frac{(2n-2)!}{n!(n-1)!},\ n \geq 2$.

3). (Задача о встречах). Некто написал n писем и запечатал их в конверты, не надписав предварительно адресов. После этого он уже не знал, в каком конверте лежит какое письмо, и поэтому n адресов на конвертах написал наугад. Какова вероятность того, что хотя бы один из адресатов получит предназначенное для него письмо?

УКАЗАНИЕ. Обозначим через A_n число исходов, при которых ни один конверт не будет подписан правильно. Тогда искомая вероятность равна $(1 - \frac{A_n}{n!})$. Вычислим число A_n. Для этого заметим, что

$$A_n = (n-1)(A_{n-1} + A_{n-2}).$$

При неблагоприятном исходе на 1-м конверте (т.е. в нем находится письмо, отправлемое по первому адресу) может быть написан 2-й, 3-й, $\ldots, n$-й адрес. Пусть, например, написан 2-й адрес. Если на 2-м конверте написан 1-й адрес, то для остальных $(n-2)$ конвертов мы имеем A_{n-2} неблагоприятных возможностей. Если же на 2-м конверте разрешается писать только 3-й, 4-й, ..., n-й адреса, то таких возможностей у нас A_{n-1}. Итак, общее число неблагоприятных возможностей, при которых на первом конверте подписывается второй адрес, равно $(A_{n-1}+A_{n-2})$. Такие же числа мы получим, подписывая первый конверт 3-м, 4-м,..., n-м адресами. Следовательно,

$$A_n = (n-1)(A_{n-1} + A_{n-2}).$$

Откуда следует, что $A_n - nA_{n-1} = -(A_{n-1} - (n-1)A_{n-2}) =$
$= A_{n-2} - (n-2)A_{n-3} = \cdots = (-1)^{n-2}(A_2 - 2A_1) = (-1)^n$, т.к. $A_1 = 0, A_2 = 1$.

Рассмотрим равенства:

$$A_n = nA_{n-1} + (-1)^n$$

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

$$\dots \quad \dots \quad \dots$$

$$A_3 = 3A_2 + (-1)^3$$

Умножим второе равенство на n, третье – на $n(n-1), \dots$ и сложим. Получим следующее равенство:

$$A_n = \left[\frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \dots + \frac{(-1)^n}{n!}\right] \cdot n!$$

Искомая вероятность равна

$$1 - \frac{A_n}{n!} = 1 - \frac{1}{2!} + \frac{1}{3!} - \dots - \frac{(-1)^n}{n!} \to (1 - e^{-1}) \approx 0,6.$$

4). Найти производящие функции следующих последовательностей:

а)

$$u_n = \begin{cases} 1, & n = 0, 1, \dots, N, \\ 0, & n > N. \end{cases}$$

ОТВЕТ: $g(x) = 1 + x + \dots + x^N$.

б)

$$u_n = \begin{cases} 0, & n - \text{ четное }, \\ \alpha^n/n!, & n - \text{ нечетное }. \end{cases}$$

УКАЗАНИЕ. $g(x) = \frac{\alpha}{1!} \cdot x + \frac{\alpha^3}{3!}x^3 + \dots = \frac{e^{\alpha x} - e^{-\alpha x}}{2}$.

в) $v_n = n \cdot u_n$, если $g(x)$ – известная производящая функция последовательности $\{u_n\}$.

УКАЗАНИЕ. $H(x) = \sum\limits_{n=0}^{\infty} v_n x^n = 0 + u_1 x + 2u_2 x^2 + \dots =$

$$= x \cdot (u_1 + 2u_2 x + 3u_3 x^2 + \dots) = x \cdot (g(x)').$$

г) $v_n = u_{n+1} - u_n$, если $g(x)$ – известная производящая функция последовательности $\{u_n\}$.

УКАЗАНИЕ.

$H(x) = (u_1 - u_0) + (u_2 - u_1)x + (u_3 - u_2)x^2 + \dots = \dots \frac{g(x) - g(0)}{x} - g(x)$.

5). Пусть $\{u_n\}$ такая последовательность элементов поля F, что производящая функция $g(x)$ является правильной дробью вида

$$\frac{b_0 + b_1 x + \cdots + b_{r-1}x^{r-1}}{1 + a_1 x + \cdots + a_r x^r}.$$

Доказать, что $\{u_n\}$ – рекуррентная последовательность порядка r.

УКАЗАНИЕ. Из равенства

$g(x)(1 + a_1 x + \cdots + a_r x^r) = (b_0 + b_1 + \cdots + b_{r-1}x^{r-1})$ следует, что $u_{n+r} + a_1 u_{n+r-1} + \cdots + a_r \cdot u_n = 0, n \geq 0.$

6). Найти общие решения рекуррентных соотношений:

а) $a_{n+2} - 4a_{n+1} + 3a_n = 0;$

б) $a_{n+3} + 3a_{n+2} + 3a_{n+1} + a_n = 0;$

в) $a_{n+3} - 3a_{n+2} + a_{n+1} - 3a_n = 0,$

$a_1 = 3,\ a_2 = 7,\ a_3 = 27;$

г) $a_{n+2} - 2cos\alpha \cdot a_{n+1} + a_n = 0,\ a_1 = cos\alpha,\ a_2 = cos2\alpha.$

7). Решить рекуррентные соотношения:

а) $a_{n+1} - a_n = n,\ a_1 = 7;$

б) $a_{n+2} + 2a_{n+1} - 8a_n = 27 \cdot 5^n,\ a_1 = -9,\ a_2 = 45.$

8). Найти последовательность $\{a_n\}$, члены которой удовлетворяют соотношениям:

а) $a_0 a_n + a_1 a_{n-1} + \cdots + a_n a_0 = 2^n a_n,\ a_0 = a_1 = 1;$

б) $a_{n+2} \cdot (n+2)^2 + a_n = 0,\ a_0 = 1,\ a_1 = 0.$

УКАЗАНИЕ для а). Рассмотрим ряд $f(x) = \sum\limits_{i=0}^{\infty} a_i x^i$. Тогда $f(x)^2 = f(2x)$. Из соотношений а) следует, что если решение существует, то оно единственное. Положим $f(x) = e^{\lambda x}$. Тогда $(e^{\lambda x})^2 = e^{\lambda(2x)}$. Так как

$e^{\lambda x} = \sum\limits_{n=0}^{\infty} \frac{(\lambda x)^n}{n!}$, то положим $\frac{\lambda}{1!} = a_1 = 1,\ a_n = \frac{1}{n!}$.

ОТВЕТ для б): $a_{2n+1} = 0,\ a_{2n} = \frac{(-1)^n \cdot 4^{-n}}{(n!)^2}$.

9). Пусть a_n – число решений в целых неотрицательных числах уравнения

$2x + 5y + 7z = n$. Доказать, что

$$\sum_{n=0}^{\infty} a_n x^n = (1-x^2)^{-1}(1-x^5)^{-1}(1-x^7)^{-1}.$$

1.3 Принцип включения и исключения

Пусть $M = \{m_1, \ldots, m_n\}$ – некоторое множество, элементы которого могут удовлетворять одному из следующих свойств: $p_1, \ldots, p_k$. Обозначим через A_i множество тех элементов M, которые удовлетворяют свойству p_i. Обозначим также через $A_{i_1 i_2 \ldots i_r} = A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_r}$.

Утверждение. *Число элементов M, не удовлетворяющих ни одному из свойств $p_1, \ldots, p_k$, равно*

$$M(0) = n - \sum_{i=1}^{k} |A_i| + \sum_{i<j} |A_{ij}| - \sum_{i<j<k} |A_{ijk}| + \cdots + (-1)^k |A_{12\ldots k}|.$$

ДОКАЗАТЕЛЬСТВО следует из равенства

$$|A_1 \cup \cdots \cup A_k| = \sum_{i=1}^{k} |A_i| - \sum_{i<j} |A_i \cap A_j| + \cdots + (-1)^{k-1} |A_1 \cap \cdots \cap A_k|,$$

которое, в свою очередь, доказывается индукцией по числу k.
Если $k = 2$, то $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$. Предположим, что наше равенство истинно для k множеств. Докажем его для $(k+1)$ множеств. Имеем $|A_1 \cup \cdots \cup A_k \cup A_{k+1}| = |A_1 \cup \cdots \cup A_k| + |A_{k+1}| - |(A_1 \cup \cdots \cup A_k) \cap A_{k+1}| =$
$= \sum\limits_{1 \le i \le k} |A_i| - \sum\limits_{1 \le i < j \le k} |A_{ij}| + \sum\limits_{1 \le i < j < k} |A_{ijk}| - \cdots + (-1)^{k-1} |A_{12\ldots k}| +$
$+ |A_{k+1}| - |(A_1 \cap A_{k+1}) \cup \cdots \cup (A_k \cap A_{k+1})| =$
$= \sum\limits_{i \le k+1} |A_i| - \sum\limits_{1 \le i < j \le k+1} |A_{ij}| + \cdots + (-1)^k |A_{12\ldots k k+1}|$. Утверждение доказано.

Обозначим через $M(r)$ число элементов M, удовлетворяющих точно r свойствам. Фиксируем свойства $p_1, \ldots, p_r (r \le k)$ и обозначим через

$$A = A_{12\ldots r},\ B_{r+1} = A \cap A_{r+1}, \ldots, B_k = A \cap A_k.$$

Число элементов M, удовлетворяющих точно свойствам $p_1, \ldots, p_r$, равно
$A(0) = |A_{12\ldots r}| - \sum\limits_{r+1\le i\le k} |B_i| + \sum\limits_{1\le i<j\le k} |B_i \cap B_j| - \ldots$
$+(-1)^{n-r}|B_{r+1} \cap \cdots \cap B_k| = |A_{12\ldots r}| - \sum\limits_{r+1\le i\le k} |A_{12\ldots ri}| + (-1)^{n-r}|A_{12\ldots k}|.$

Следовательно,

$$M(r) = \sum_{i_1<\cdots<i_r} |A_{i_1 i_2 \ldots i_r}| - C_{r+1}^r \sum_{i_1<\cdots<i_{r+1}} |A_{i_1 i_2 \ldots i_{r+1}}| +$$
$$+C_{r+2}^r \sum_{i_1<\cdots<i_{r+2}} |A_{i_1 \ldots i_{r+2}}| - \cdots + (-1)^j C_{r+j}^r \sum_{i_1<\cdots<r+j} |A_{i_1 \ldots i_{r+j}}| + \ldots.$$

Эта формула обобщает утверждение 1 ($r = 0$) и называется формулой (принципом) включения и исключения.

Применим доказанный принцип к решению задачи о встречах. Подсчитаем число тех перестановок $a_1, \ldots, a_n$ чисел $1, 2, \ldots, n$, для которых $a_i \ne i, i \le n$. Обозначим через $A_{i_1 \ldots i_r}$ множество тех перестановок, для которых $a_{i_j} = i_j, j \le r$. Тогда $|A_{i_1 \ldots i_r}| = (n-r)!$ Из утверждения 1 следует, что искомое число равно

$n! - (n-1)!n + (n-2)!C_n^2 - (n-3)!C_n^3 + \cdots + (-1)^n \frac{n!}{n!} =$
$= \frac{n!}{2!} - \frac{n!}{3!} + \cdots + (-1)^n \frac{n!}{n!} = n!\left(\frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}\right).$

Пример. На одной из кафедр университета работают тринадцать человек, причем каждый из них знает хотя бы один иностранный язык. Девять человек знают английский, восемь – немецкий, пять – французский. Пятеро знают английский и немецкий, трое – английский и французский и двое немецкий и французский. Можем ли мы ответить на следующие вопросы:

1) Сколько человек знают все три языка?

2) Сколько человек знают ровно два языка?

3) Сколько человек знают только английский?

Обозначим через K множество сотрудников кафедры, через K_x – множество сотрудников, знающих язык x. Тогда

$13 = |K_a| + |K_{\text{н}}| + |K_{\text{ф}}| - |K_{\text{а,н}}| - |K_{\text{а,ф}}| - |K_{\text{н,ф}}| + |K_{\text{а,н,ф}}| =$
$= 9 + 8 + 5 - 5 - 3 - 2 + |K_{\text{а,н,ф}}| = 12 + |K_{\text{а,н,ф}}|$. Следовательно, только один человек знает все три языка.

Подсчитаем число людей, знающих только английский язык. Имеем, $|K_{\text{а}}| - |K_{\text{а,н}}| - |K_{\text{а,ф}}| + |K_{\text{а,н,ф}}| = 9 - 5 - 3 + 1 = 2$. И, наконец, число сотрудников, знающих ровно 2 языка, равно сумме следующих чисел

$$|K_{\text{а,н}}| - |K_{\text{а,н,ф}}|,$$

$$|K_{\text{а,ф}}| - |K_{\text{а,н,ф}}|,$$

$$|K_{\text{н,ф}}| - |K_{\text{а,н,ф}}|.$$

Т.е. искомое число равно 4+2+1=7.

ЗАДАЧИ

1). Доказать, что число целых чисел в сегменте $[1, n]$ взаимно простых с n равно $\varphi(n) = n \cdot \prod_{p|n}(1 - \frac{1}{p})$.

УКАЗАНИЕ. Число m не является взаимно простым с $n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ тогда и только тогда, когда существует простой делитель $p_i|n$ такой, что $p_i|m$. Пусть $A_i = \{m \in [1, n]; p_i|m\}$. Тогда $\varphi(n)$ – число элементов в разности

$$[1, n] \setminus (A_1 \cup A_2 \cup \dots \cup A_s),$$

т.е. $\varphi(n) = n - \sum_{i=1}^{s} |A_i| + \sum_{i<j} |A_i \cap A_j| - \sum_{i<j<k} |A_i \cap A_j \cap A_k| + \dots +$
$+(-1)^s |A_1 \cap \dots \cap A_s|$. Так как $p_i \neq p_j$ при $i \neq j$, то $A_{i_1} \cap \dots \cap A_{i_t} =$
$= \{m \in [1, n]; (p_{i_1} \dots p_{i_t})|m\}$. Заметим, наконец, что число элементов в $[1, n]$, делящихся на $d (d \leq n)$ равно $[\frac{n}{d}]$. Поэтому $\varphi(n) = n - \sum_{i=1}^{s} \frac{n}{p_i} +$
$+ \sum_{i<j} \frac{n}{p_i p_j} - \sum_{i<j<k} \frac{n}{p_i p_j p_k} + \dots + (-1)^s \frac{n}{p_1 p_2 \dots p_s} = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_s})$.

2). Сколько из $n!$ членов определителя

$$\begin{pmatrix} 0 & a_{12} & \dots & \dots & a_{1n} \\ a_{21} & 0 & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & 0 & a_{n-1,n} \\ a_{n1} & \dots & \dots & a_{n,n-1} & 0 \end{pmatrix}$$

рано нулю?

ОТВЕТ: $(n-1)!n - C_n^2(n-2)! + C_n^3(n-3)! - \cdots = n! - \frac{n!}{2} + \frac{n!}{3!} - \frac{n!}{4!} + \cdots =$
$= n(1 - \frac{1}{2!} + \frac{1}{3!} - \cdots + \frac{(-1)^{n-1}}{n!})$.

3). Пусть дано n объектов ($n > 1$) и пусть свойством α обладают все, кроме первого, свойством β – все, кроме второго,..., свойством λ – все, кроме последнего. Определить число объектов, не обладающих ни одним из этих свойств.

ОТВЕТ: $n(1 - (n-1) + \frac{(n-1)(n-2)}{2} \dots) = n(1-1)^{n-1} = 0$.

4). Найти число целых положительных чисел, не превосходящих 1000 и не делящихся ни на одно из чисел 3, 5 и 7.

УКАЗАНИЕ. Искомое число равно $1000 - [\frac{1000}{3}] - [\frac{1000}{5}] - [\frac{1000}{7}] + [\frac{1000}{15}] +$
$+[\frac{1000}{21}] + [\frac{1000}{35}] - [\frac{1000}{105}]$.

5). При обследовании читательских вкусов студентов оказалось, что 60% студентов читает газету "Правда", 50% – газету "Алтайская Правда", 50% – газету "Комсомольская Правда", 30% – газеты "Правда" и "Алтайская Правда", 20% – газеты "Алтайская Правда" и "Комсомольская Правда", 40% – газеты "Правда" и "Комсомольская Правда", 10% – все газеты. Сколько процентов студентов

1)не читает ни одной из газет;

2) читает точно две газеты;

3) читает не менее двух газет?

6). (Задача мажордома). К обеду за круглым столом приглашены n пар враждующих рыцарей ($n \geq 2$). Доказать, что существует ровно

$$\sum_{k=0}^{n} (-1)^k C_n^k \cdot 2^k \cdot (2n-k)!$$

способов рассаживания их так, чтобы никакие два врага не сидели рядом.

1.4 Теорема Холла (о представителях)

Рассмотрим следующую "задачу о сватовстве":

Пусть n юношей дружат с девушками, и пусть для каждой группы из k юношей $(k = 1, 2, \cdots, n)$ имеется по крайней мере k девушек, имеющих друзей среди этих юношей. Верно ли, что каждого юношу можно женить на девушке, с которой он дружит?

Ответ на этот вопрос положительный и составляет содержание т.н. теоремы Ф.Холла о представителях (1935 г.).

Теорема 1. *Пусть $S_1, S_2, \ldots S_n$ – подмножества S (не обязательно различные). Необходимым и достаточным условием существования системы различных представителей (с.р.п.) для семейства*

$$S_1, S_2, \ldots, S_n,$$

т.е. таких элементов $x_1, \ldots, x_n \in S$, что $x_i \in S_i, i \leq n$ и $x_i \neq x$; при $i \neq j$, является условие $(*)$: для любых различных индексов $i_1, \ldots, i_k$ множество

$$S_{i_1} \cup S_{i_2} \cup \cdots \cup S_{i_k}$$

содержит не менее k различных элементов.

ДОКАЗАТЕЛЬСТВО. Если такие представители существуют, то, очевидно, наше условие выполнено. Докажем обратное утверждение. Для этого рассмотрим сначала примеры. Пусть $S = \{1, 2, 3, 4, 5, 6\}$ и $S_1 = \{1, 2, 3\}, S_2 = \{1, 2, 4\}, S_3 = \{1, 2, 5\}, S_4 = \{2, 5, 6\}, S_5 = \{2, 5, 6\}$. Элементы $1 \in S_1, 4 \in S_2, 5 \in S_3, 2 \in S_4, 6 \in S_5$ составляют с.р.п. для нашего семейства множеств. Если же мы возьмем семейство подмножеств $T_1 = \{1, 1, 3\}, T_2 = \{1, 1, 3\}, T_3 = \{3, 3, 1\}, T_4 = \{1, 2, 3, 3\}$, то для него не существует с.р.п., т.к. $|T_1 \cup T_2 \cup T_3| = 2$.

Доказательство теоремы проведем методом математической индукции по числу множеств n. Теорема очевидна при $n = 1$. Сделаем предположение индукции об истинности теоремы для семейств, содержащих менее чем n

элементов. Докажем теорему для семейства из n элементов (доказательство принадлежит М.Холлу). Если $|S_1| = |S_2| = \cdots = |S_n| = 1$, то условие $(*)$ означает, что $S_1 = \{x_1\}, \ldots, S_n = \{x_n\}$, где $x_i \neq x_j; i \neq j$. Следовательно, теорема доказана. Если некоторое S_i содержит более, чем n элементов, то, оставляя в нем n элементов, мы, очевидно, сохраним условие $(*)$. Семейство $\{S_{i_1}, \ldots, S_{i_r}\} = B_{r,s}$, где $s = |S_{i_1} \cup \cdots \cup S_{i_r}| \geq r$, назовем блоком (условие $s \geq r$ следует из условия $(*)$). Если $s = r$, то блок назовем критическим. Пусть $\{A_1, \ldots, A_u, C_{u+1}, \ldots, C_r\} = B_{r,s}$ и $\{A_1, \ldots, A_u, D_{u+1}, \ldots, D_t\} = B_{t,v}$ – два блока $(A_i, B_j, D_e \in \{S_1, \ldots, S_n\})$, в которых множества $A_1, \ldots, A_u$ являются общими для этих блоков. Положим $B_{r,s} \cap B_{t,v} = \{A_1, \ldots, A_u\} = B_{u,w}$ и $B_{r,s} \cup B_{t,v} = \{A_1, \ldots, A_u, C_{u+1}, \ldots, C_r, D_{u+1}, \ldots, D_t\} = B_{(r+t-u),z}$. Ясно, что $w \geq u$ и $z \geq r + t - u$.

Лемма 1. *Объединение и пересечение двух критических блоков (в смысле вышеприведенных определений) являются снова критическими блоками.*

ДОКАЗАТЕЛЬСТВО. Пусть $B_{r,r} \cap B_{t,t} = B_{u,w}$ и $B_{r,r} \cup B_{t,t} = B_{r+t-u,z}$. Заметим, что $z \leq r + t - w$ и $z \geq r + t - u, w \geq u$. Следовательно, $r + t - w \geq$ $\geq z \geq r + t - u, u \geq w, u = w, z = r + t - u$.

Лемма доказана.

Пусть $B_{r,s} = \{A_1, \ldots, A_u, C_{u+1}, \ldots, C_r\}$ – произвольный блок и

$B_{k,k} = \{A_1, \ldots, A_u, D_{u+1}, \ldots, D_k\}$ – критический блок, в котором $A_1, \ldots, A_u$ – все множества, общие для обоих блоков. Тогда $B_{r,s} \cap B_{k,k} = B_{u,v}$, где $v \geq u$ и $B_{r,s} \cup B_{k,k} = \{A_1, \ldots, A_u, C_{u+1}, \ldots, C_r, D_{u+1}, \ldots, D_k\} = B_{r+k-u,z}$, где $z \geq r + k - u$. С блоком $B_{r,s}$ свяжем блок $B'_{r,s'}$, полученный из $B_{r,s}$ вычеркиванием элементов $B_{k,k}$ из множеств $C_{u+1}, \ldots, C_r$. Этот блок имеет вид

$$\{A_1, \ldots, A_u, C'_{u+1}, \ldots, C'_r\} = B'_{r,s'}.$$

Покажем, что $s' \geq r$, т.е. операция вычеркивания не нарушает условия $(*)$. Заметим, что $|(C_{u+1} \cup \cdots \cup C_r) \setminus B_{k,k}| = z - k$ и, следовательно, $s' =$ $= v + z - k \geq v + (r + k - u) - k \geq r$. Итак, нами доказана следующая

Лемма 2. *Если $B_{k,k}$ – критический блок, то вычеркивание элементов $B_{k,k}$ из множеств, не принадлежащих $B_{k,k}$, не нарушает условия* $(*)$.

Если, далее, система наших множеств $\{S_1, \ldots, S_n\}$ содержит критический блок $B_{k,k}$, где $k \leq n-1$, то, вычеркнув элементы $B_{k,k}$ из остальных множеств, мы можем считать, что наше семейство $\{S_1, \ldots, S_n\}$ состоит из двух блоков $B_{k,k}$ и $B_{n-k,v}$. Эти блоки не имеют общих элементов, и для них выполнимо условие $(*)$. По предположению индукции, оба имеют с.р.п. и, следовательно, существует с.р.п. и для семейства $\{S_1, \ldots, S_n\}$.

Пусть наше семейство не содержит критических блоков $B_{k,k}$, где $1 \leq k < n$. Пусть $a \in S_1$. Вычеркнем a в $S_2, S_3, \ldots, S_n$. Произвольный блок $B_{r,s}(r < n)$ семейства $\{S_2, \ldots, S_n\}$ не является критическим, т.е. $s \geq r+1$. Следовательно, после вычеркивания мы получим блок $B'_{r,s'}$ семейства $\{S'_2, \ldots, S'_n\}$, в котором s' равно либо s, либо $s-1$. Т.е. $s' \geq r$. Это означает, что семейство $\{S'_2, \ldots, S'_n\}$ удовлетворяет условию $(*)$. По предположению индукции семейство $\{S'_2, \ldots, S'_n\}$ имеет с.р.п. Следовательно, $\{S_2, \ldots, S_n\}$ имеет с.р.п. (все они не равны a). Беря элемент a в качестве представителя S_1, мы получим доказательство теоремы.

Замечание 1. Лемма 1 не использовалась в доказательстве теоремы. Но из нее следует, что существует наибольший и наименьший критические блоки.

Замечание 2. Из доказанной теоремы можно вывести, в качестве следствия, что если $H \leq G$ – конечная подгруппа группы G, то существуют элементы $\{a_i\} \subseteq G$, являющиеся одновременно представителями для правых смежных классов по H и левых смежных классов по H.

1.5 Некоторые комбинаторные задачи на плоскости

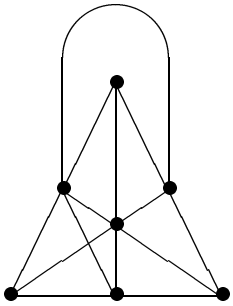
Задача 1. Показать, что можно так организовать автобусное движение в городе, что

1) каждый автобусный маршрут имел ровно 3 остановки;

2) каждые два маршрута имели единственную общую остановку;

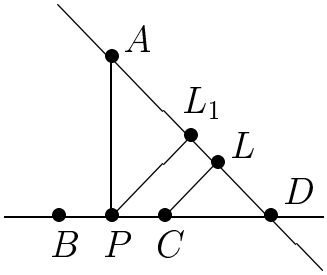
3) с любой из остановок можно проехать на любую другую без пересадки.

УКАЗАНИЕ. Рассмотреть граф



Задача 2. На плоскости дано n точек, расположенных так, что на каждой прямой, соединяющей любые две из этих точек, лежит по крайней мере еще одна из них. Доказать, что все эти точки лежат на одной прямой.

УКАЗАНИЕ. Допустим противное и выберем среди данных точек такие три точки A, B, C, что расстояние от точки A до прямой BC не равно нулю и является наименьшим из всех возможных.

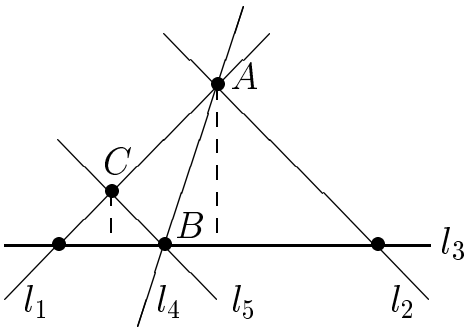


Пусть D – третья точка нашего множества, принадлежащая прямой BC. Ясно, что длины перпендикуляров CL, PL, AP удовлетворяют неравенствам: $AP > PL_1 > CL$. Противоречие.

Задача 3. На плоскости дано некоторое конечное число попарно пересекающихся прямых, причем через точку пересечения любых двух прямых

нашего множества проходит некоторая третья прямая из этого же множества. Доказать, что все прямые пересекаются в одной точке.

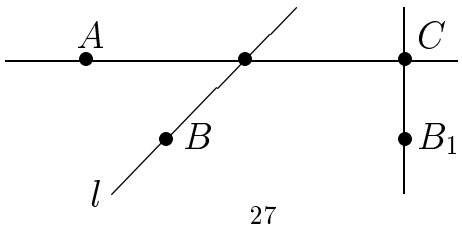
УКАЗАНИЕ. Допустим противное. Тогда существуют прямые l_1, l_2, l_3 из нашего множества такие, что они не пересекаются в одной точке и расстояние от точки A пересечения прямых l_1 и l_2 до l_3 является наименьшим из возможных:



Через точку A проходит некоторая прямая l_4 из нашего множества, а через точку $B = l_3 \cap l_4$ прямая l_5, пересекающая l_1 в точке C. Ясно, что расстояние от точки C до l_3 меньше расстояния от точки A до l_3. Противоречие.

Задача 4. Можно ли спланировать автобусную сеть в некотором городе, состоящую из $n(n \geq 3)$ маршрутов так, чтобы после закрытия любого из этих маршрутов оставалась бы возможность проехать с каждой из имеющихся остановок на любую другую, используя пересадки, а после закрытия каких угодно двух маршрутов нашлись бы две остановки, с одной из которых уже нельзя проехать на другую?

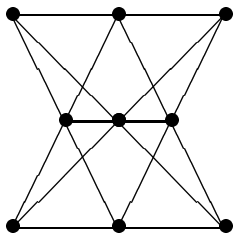
УКАЗАНИЕ. Такая планировка существует. Действительно, рассмотрим n попарно пересекающихся прямых, никакие три из которых не пересекаются в одной точке. Каждую прямую будем считать автобусным маршрутом, а каждую точку пересечения – остановкой. Выбросим некоторую прямую l :



Если наши остановки A и B_1 лежат на одной прямой, не совпадающей с l, то доехать можно без пересадки. Если же они принадлежат разным прямым (не совпадающими с l), то доехать можно, сделав пересадку в точке пересечения этих прямых. Если же одна или обе остановки принадлежат вычеркнутому маршруту l, то рассуждение аналогично. В случае удаления 2-х маршрутов, то остановка, расположенная на их пересечении, была бы недосягаемой.

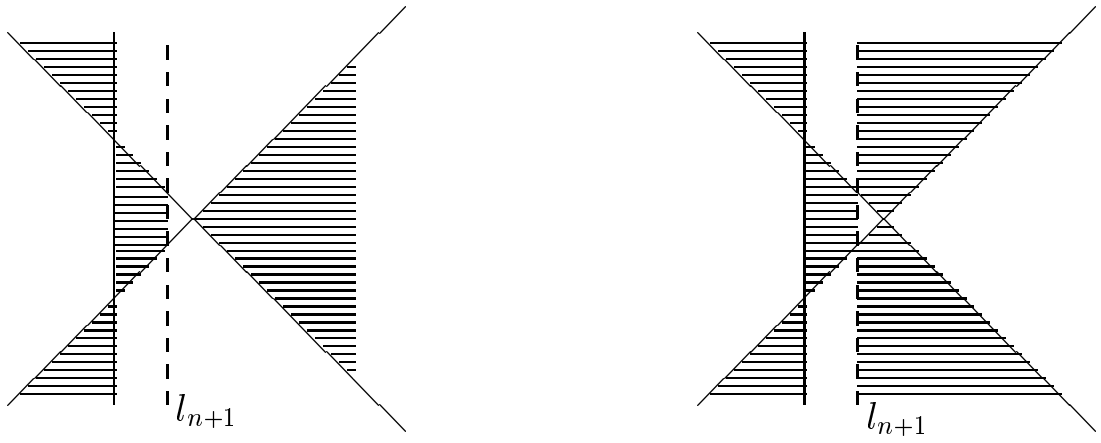
Задача 5. Расположить на плоскости девять прямых и девять точек так, чтобы через каждую точку проходили ровно 3 прямые и на каждой прямой лежали ровно 3 точки.

УКАЗАНИЕ.



Задача 6. На плоскости проведено n прямых линий. Доказать, что области, на которые эти прямые разбивают плоскость, можно закрыть 2 красками так, что никакие две соседние области не будут закрашены одним цветом.

УКАЗАНИЕ. Воспользоваться индукцией по числу n. Еслми $n = 1$, то решение очевидно. Предположим, что задача имеет решение для n прямых. Рассмотрим разбиение плоскости $(n + 1)$ прямыми $l_1, \ldots, l_{n+1}$. По предположению индукции существует искомая раскраска областей плоскости, на которые она разбивается прямыми $l_1, \ldots, l_n$.

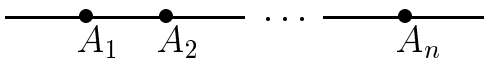


Алгоритм новой раскраски: с одной стороны от l_{n+1} раскраска не меняется, а с другой – меняется на противоположную.

Задача 7. Доказать, что число точек пересечения диагоналей выпуклого n-угольника не превосходит C_n^4.

Задача 8. На прямой отмечены n различных точек $A_1, \ldots, A_n (n \geq 4)$. Каждая из этих точек покрашена в один из 4-х цветов, причем все 4 цвета присутствуют. Доказать, что существует отрезок прямой, содержащий ровно по одной точке двух цветов и по крайней мере по одной точке двух оставшихся цветов.

УКАЗАНИЕ. Можно считать, что наши точки расположены слева направо.



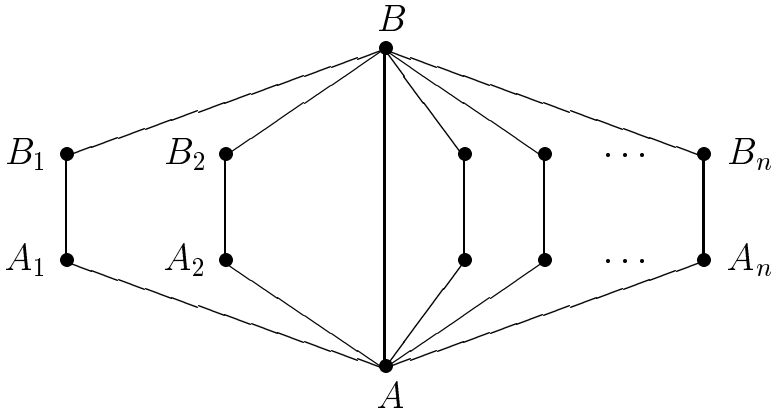
Пусть $m = min\{i;$ среди точек $A_1, \ldots, A_i$ присутствуют точки всех 4-х цветов $\}$. Тогда цвет A_m отличен от цветов $A_1, \ldots, A_{m-1}$. Пусть $k = max\{j; j \leq m-1,$ среди точек $A_j, A_{j+1}, \ldots, A_m$ присутствуют точки всех 4-х цветов $\}$. Тогда цвет A_k отличается от цветов $A_{k+1}, \ldots, A_m$, и отрезок $[A_k, A_m]$ является искомым.

Задача 9. В некотором обществе любые два знакомых не имеют общих знакомых, а любые два незнакомых имеют ровно двух общих знакомых. Доказать, что в этом обществе все имеют одинаковое число знакомых.

УКАЗАНИЕ. Сначала докажем следующую лемму.

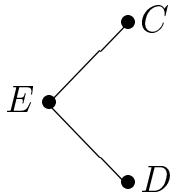
Лемма. *Если A и B знакомы, то они имеют одинаковое число знакомых.*

ДОКАЗАТЕЛЬСТВО. Пусть $A_1, \ldots, A_n$ – все знакомые A. Будем изображать членов общества точками и соединять любые два ребром, если они знакомы. Тогда среди $B, A_1, \ldots, A_n$ нет знакомых и существуют $B_1, \ldots, B_n$ такие, что B_i – общий знакомый A_i и B :



Таким образом, число знакомых B больше или равно n. Аналогично доказывается, что число знакомых A не меньше числа знакомых B. Лемма доказана.

Пусть C и D незнакомы. Тогда существует E такой, что

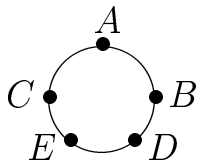


По лемме число знакомых E равно числу знакомых C и равно числу знакомых D.

Задача 10. В компании, состоящей из 5 человек, среди любых трех человек найдутся двое, которые знают друг друга, и двое, незнакомых друг с другом. Доказать, что компанию можно рассадить за круглым столом так, чтобы по обе стороны от каждого человека сидели его знакомые.

УКАЗАНИЕ. Докажем, что каждый человек знает ровно двоих. Если A знает трех B, C, D, то среди $\{B, C, D\}$ нет знакомых. Противоречие.

Если A не знаком с тремя членами компании B, C, D, то B, C и D попарно знакомы друг с другом. Итак, каждый член компании знаком ровно с двумя другими. Пусть A знаком, например, с B и C. Тогда B и C не знакомы между собой. Пусть D – знакомый B и E – оставшийся член компании. Тогда E – знакомый C и D – незнакомый C. Укажем искомую рассадку

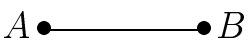


Задача 11. В каждой из 3-х студенческих групп учится по n студентов. Любой студент имеет $(n+1)$ знакомых студентов в двух других группах. Доказать, что в каждой группе можно выбрать по одному студенту так, чтобы все трое выбранных студентов были знакомы друг с другом.

УКАЗАНИЕ. Пусть A такой студент одной из групп, который имеет наибольшее число k знакомых в одной из групп $(k \leq n)$. Так как
$(n+1-k) \geq 1$, то пусть B – знакомый A из оставшейся третьей группы. Если B знаком с кем-либо из знакомых A во второй группе, то задача решена. Иначе, он знаком с не более чем k студентами в первой группе и с не более чем $(n-k)$ студентами во второй группе. Т.е. общее число его знакомых не превосходит n. Противоречие.

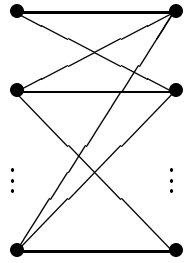
Задача 12. Доказать, что если в графе с $2n$ вершинами никакие три ребра не образуют треугольника, то число ребер не превосходит n^2.

УКАЗАНИЕ. Воспользуемся методом математической индукции. Выберем две вершины A и B, соединенные ребром:



Оставшиеся вершины соединены не более чем n^2 ребрами и каждая из них соединена с A и B не более чем одним ребром.

Таким образом, общее число ребер не превосходит числа $n^2 + 2n + 1 = (n + 1)^2$. Примером графа с $2n$ вершинами и n^2 ребрами является двудольный граф:



Глава 2

Элементы теории графов

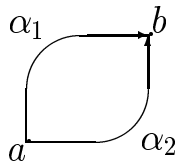
В 1736 г. Л.Эйлер опубликовал статью, посвященную решению задачи о Кенигсбергских мостах. С этого времени идет отсчет теории графов как математической дисциплины. Первые исследования в теории графов были связаны с попытками решения т.н. задачи о четырех красках (впервые сформулированной в Великобритании А.Де Морганом и А.Кэли во второй половине XIX века), а также с задачами о перевозках и о электрических схемах (Г.Кирхгоф). В настоящее время теория графов является самостоятельной математической дисциплиной, имеющей приложения как в самой математике, так и в экономике, физике, биологии. Это связано с универсальностью языка теории графов и эффективностью ее методов в решении различных задач.

2.1 Основные понятия теории графов и способы представления графов

Граф G – упорядоченная пара (V, E), где V – множество и E семейство неупорядоченных пар элементов из V. Элементы множества V называются вершинами графа G, а элементы E – его ребрами. Вершины a, b ребра $\{a, b\} \in E$ называются его концами. Говорят, что ребро $\alpha = \{a, b\}$ инцидентно своим концам a и b, а концы, в свою очередь, инцидентны ребру

α. Граф $G = (V, E)$ называется простым, если V – конечное множество и семейство E тоже является множеством, т.е. каждую пару вершин графа может соединять не более чем одно ребро. Часто рассматривают ориентированные графы $G = (V, E)$, представляющие собой пару (V, E), где V – некоторое множество, а E – семейство упорядоченных пар элементов из V, т.е. E – семейство элементов декартова квадрата $V \times V$. При этом в ребре $\alpha = (a, b) \in E$ вершину a называют началом, а b – концом ребра α и изображают следующим образом

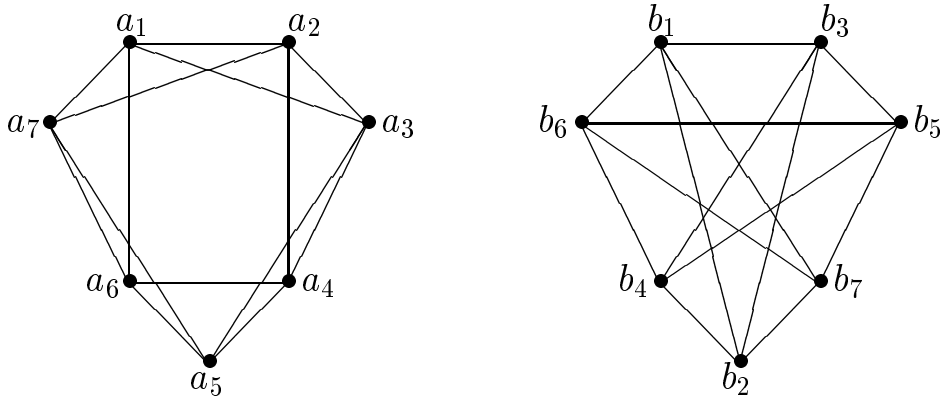
Иногда рассматривают смешанные графы, которые имеют как ориентированные, так и неориентированные ребра. Например, план города можно рассматривать как смешанный граф, в котором вершины – перекрестки, а ребра – улицы с односторонним или с двусторонним движением. Из определения графа следует, что допускаются ребра вида (a, a), называемые петлями (обычно, петля считается неориентированной), а также кратные ребра, соединяющие две вершины $\alpha_1 = (a, b)_1,\ \alpha_2 = (a, b)_2$:



Два графа $G_1 = (V_1, E_1)$ и $G_2 = (V_2, E_2)$ назовем изоморфными, если существует биекция V_1 на V_2, $\varphi : V_1 \to V_2$, такая, что

$\{x, y\} \in E_1 \Leftrightarrow \{\varphi(x),\ \varphi(y)\} \in E_2$ (если ребра ориентированы, то ориентация сохраняется). Если G_1 изоморфен G_2, то будем писать $G_1 \cong G_2$.

Пример 1. Следующие графы являются изоморными

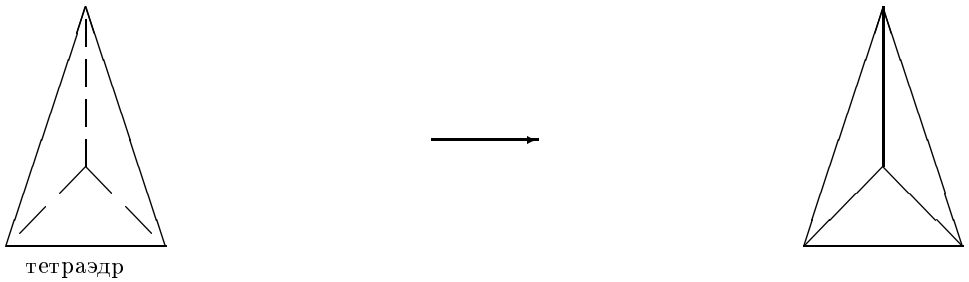


относительно биекции $a_i \to b_i,\ i \leq 7$.

Вершина, не инцидентная никакому ребру, называется изолированной. Граф, состоящий только из изолированных вершин называется нуль-графом и обозначается E^n, где n – число вершин. Граф, содержащий n вершин, в котором любые две различные вершины соединены одним ребром, называется полным графом и обозначается K^n (граф $K_1 = E^1$ называется тривиальным). Заметим также, что простой граф порядка n (т.е. содержащий n вершин) имеет не более C_n^2 ребер. Число ребер простого графа называется его размером и обозначается $\nu_e(G)$.

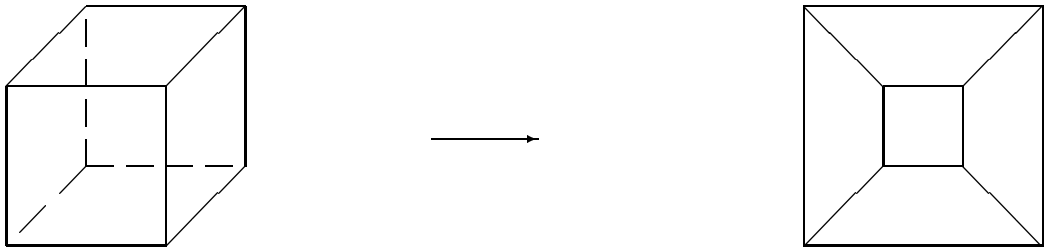
Пример 2. Следующие "пространственные" графы допускают изоморфное изображение на плоскости:

1)



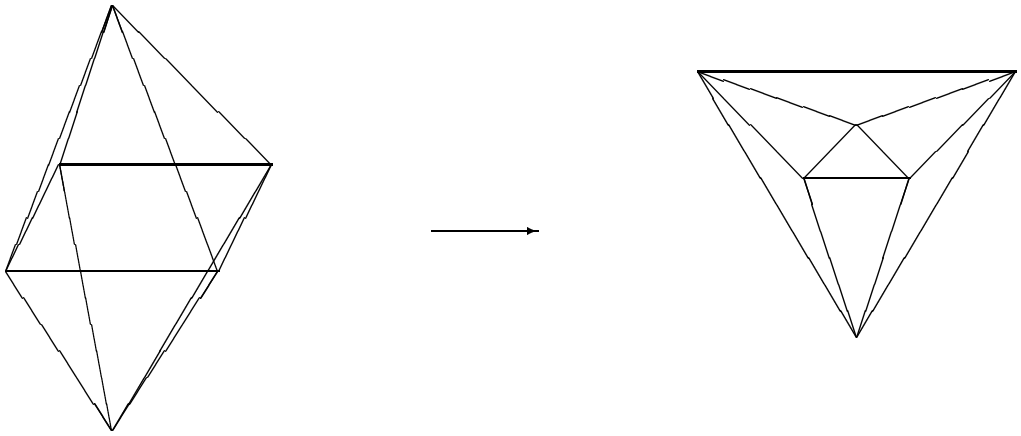
тетраэдр

2)



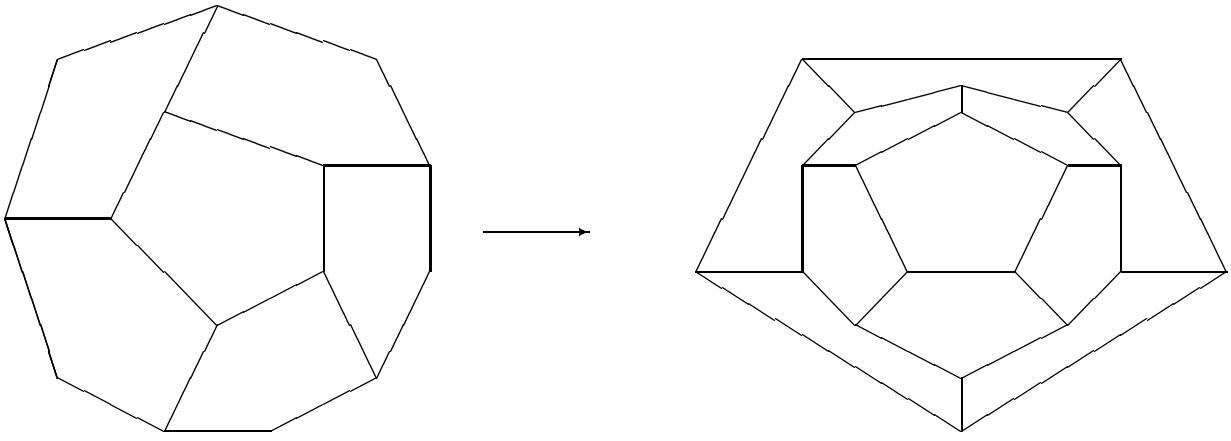
куб

3)



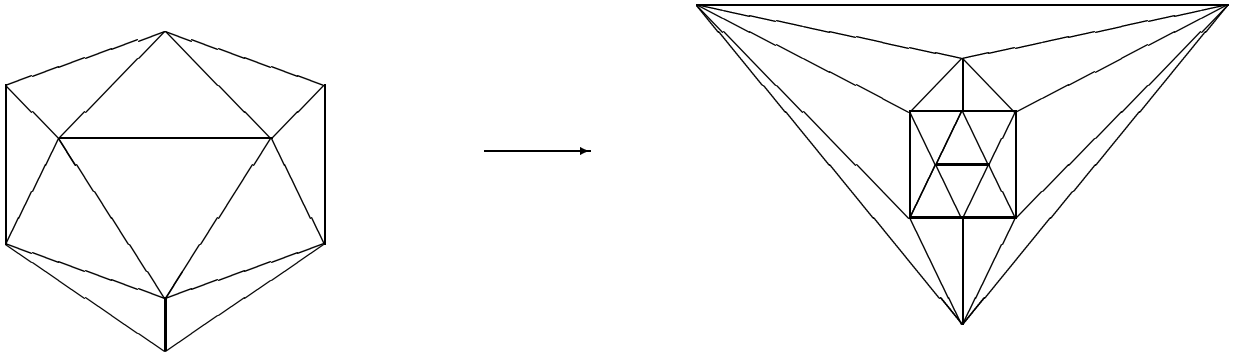
октаэдр

4)



додекаэдр

5)



икосаэдр

Степенью вершины a неориентированного графа назовем число ребер, инцидентных a (в обозначении $\rho(a)$). Граф называется однородным (регулярным) степени k, если степень каждой вершины $\rho(a)$ равна k. Например, графы правильных многогранников (платоновых тел) являются регулярными (см. пример 2).

Утверждение 1. *Пусть $\nu_e = \nu_e(G)$ – число всех ребер графа $G = (V, E)$. Тогда*

$$2\nu_e = \sum_{a \in V} \rho(a).$$

В частности, в конечном графе число вершин, имеющих нечетную степень, является четным.

Доказательство следует из того, что в сумме $\sum\limits_{a \in V} \rho(a)$ каждое ребро $\{a, b\}$ учитывается два раза.

Иногда число всех ребер графа G обозначается символом $e(G)$.

Следствие 1. *В однородном степени k конечном графе порядка n справедливо равенство*

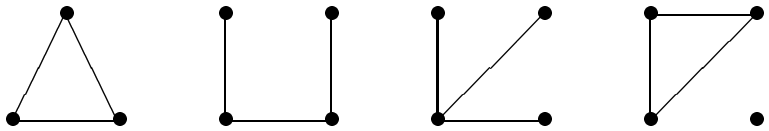
$$\nu_e = \frac{k \cdot n}{2}.$$

В частности, если k – нечетное число, то число вершин является четным.

Как уже отмечалось, число всех вершин графа G называется порядком графа и обозначается символом $|G| = n = |V(G)|$. Произвольный граф

порядка n записывается в виде G^n, а произвольный простой граф порядка n с m ребрами записывается в виде $G(n, m)$.

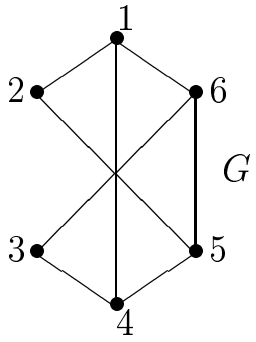
Пример 3. Следующие графы имеют порядок не превосходящий 4 и размер 3:



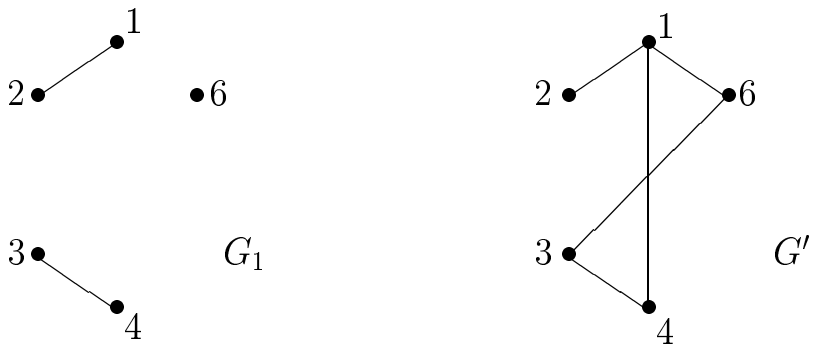
Граф $G' = (V', E')$ является подграфом графа $G = (V, E)$, если $V' \subseteq V$ и $E' \subseteq E$ (в обозначении, $G' \subseteq G$). Если подграф G' содержит все ребра графа G, соединяющие любые две вершины из G', то он называется натянутым (или индуцированным) на V'.

Пример 4. Рассмотрим граф

$$G = (\{1,2,3,4,5,6\},\ \{\{1,2\},\ \{1,4\},\ \{1,6\},\ \{2,5\},\ \{3,4\},\ \{3,6\},\ \{4,5\},\{5,6\}\}).$$

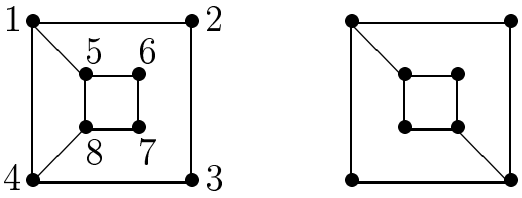


Тогда нижеследующие графы G_1 и G' являются соответственно подграфом G и подграфом G, натянутым на $\{1, 2, 3, 4, 6\}$:



Подграф G', натянутый на множество $V' \subseteq V$, обозначают $G' = G[V']$. Если $W \subseteq V(G)$, то $G \setminus W = G[V \setminus W]$ – подграф G, полученный из G вычеркиванием всех вершин из W и всех ребер, инцидентных этим вершинам. Аналогично, если $E' \subseteq E(G)$, то $G \setminus E' = (V(G), E(G) \setminus E')$.

Задача 1. Доказать, что следующие графы не являются изоморфными



УКАЗАНИЕ. В первом графе есть последовательность инцидентных ребер, возвращающаяся к исходной вершине (цикл):

$$\{1,2\},\{2,3\},\{3,4\},\{4,8\},\{8,7\},\{7,6\},\{6,5\},\{5,1\}.$$

Во втором графе такой последовательности нет.

Если имеется простой граф без петель $G = (V, E)$, $|G| = n$, то его можно дополнить до полного графа K^n, проведя недостающие ребра. Граф, образованный множеством вершин $V(G)$ и вновь проведенными ребрами, называется дополнением G и обозначается через $\bar{G}$.

Пример 5.

Пусть $G = (V(G), E(G))$ и $H(V(H), E(H))$ – два графа. Назовем их объединением следующий граф:

$$G \cup H = (V(G) \cup V(H), E(G) \cup E(H)).$$

Суммой $G + H$ называется граф, полученный из $G \cup H$ добавлением всех ребер, соединящих вершины из $V(G)$ с вершинами из $V(H)$. Граф называется конечным, если число его ребер конечно. Т.е., если в конечном графе

имеется бесконечное число вершин, то все они, за исключением конечного числа, являются изолированными. Система ребер графа $= (V, E)$

$$A_{a_i a_j} = \{\{a_{i_1}, a_{i_2}\}, \{a_{i_2}, a_{i_3}\}, \ldots, \{a_{i_{s-1}}, a_{i_s}\}\},$$

где $a_i = a_{i_1},\ a_{i_s} = a_j$ и $\{a_{i_t},\ a_{i_{t+1}}\} \in E, 1 \leq t \leq s-1,\ a_t \in V$ называется путем (или маршрутом), соединяющим вершины a_i и a_j. Если $a_i = a_j$, то путь $A_{a_i a_i}$ называется циклическим. Граф G называется связным, если для любых двух различных вершин a_i и a_j графа G существует путь, соединяющий эти вершины. Ясно, что каждый граф конечного порядка является объединением конечного числа связных непересекающихся (т.е. не имеющих общих вершин) подграфов, называемых связными компонентами графа.

Путь $A_{a_i a_j}$, в котором каждое ребро встречается не более одного раза, называется цепью. Циклический путь, являющийся цепью, называется циклом. Цикл с концом a называется простым циклом: если a не является в нем промежуточной вершиной и никакие другие вершины не повторяются. Аналогично, назовем нециклическую цепь простой цепью, если в ней никакая вершина не повторяется. Фигура $S \subseteq \mathbf{R}^{(3)}$, состоящее из точек $b_1, b_2, \ldots$ и кривых (отрезков), их соединяющих (в обозначении $\{b_i, b_j\}$; заметим также, что никакая внутренняя точка кривой не является вершиной или внутренней точкой другой кривой), называется геометрической реализацией графа $G = (V, E)$, где $V = \{a_1, a_2, \ldots\}$, если существуют биекции V на $\{b_1, \ldots\}$ и E на $\{\{b_i, b_j\}\}$ такие, что $\{b_{n_i}, b_{n_j}\} \leftrightarrow (a_i, a_j)$ тогда и только тогда, когда $b_{n_i} \leftrightarrow a_i,\ b_{n_j} \leftrightarrow a_j$ (т.е. $S \cong G$).

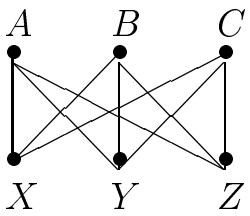
Утверждение 2. *Каждый конечный граф $G = (V, E)$ можно реализовать в $\mathbf{R}^{(3)}$.*

ДОКАЗАТЕЛЬСТВО. Без ограничения общности можно считать, что $|G| = n < \infty$. Возьмем прямую в $\mathbf{R}^{(3)}$ и проведем через нее связку из m плоскостей, где m – число ребер G. Выберем на прямой n точек $b_1, \ldots,\ b_n$ и рассмотрим биекцию $b_i \to a_i, i \leq n$, где $V = \{a_1, \ldots, a_n\}$. Каждому ребру

$\{a_i, a_j\} \in E$ поставим в соответствие некоторую плоскость из пучка и в ней дугу окружности, соединяющую b_i и b_j. В результате получаем искомую геометрическую реализацию S нашего графа G в $\mathbf{R}^{(3)}$.

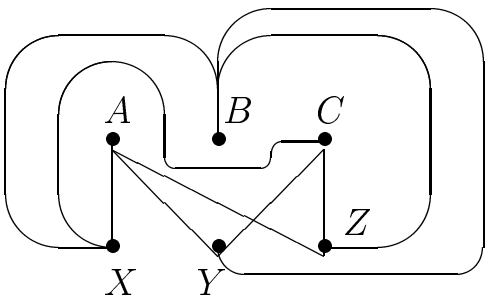
Вопрос о реализации произвольного конечного графа в $\mathbf{R}^{(2)}$ является не простым, хотя и имеет полное решение (см. ниже теорему Понтрягина-Куратовского).

Задача 2. (о трех домах и трех колодцах)

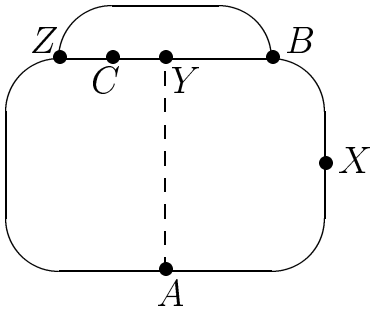


На участке земли были построены три дома A, B, C и вырыты три колодца X, Y, Z. От каждого из домов имелась тропа к каждому из трех колодцев. Спустя некоторое время обитатели домов A, B, C поссорились друг с другом и решили проложить дорожки к колодцам X, Y, Z так, чтобы по пути к колодцам им не приходилось встречаться друг с другом. Спрашивается, можно ли это сделать?

Попытки решить эту задачу приводят нас к убеждению, что это невозможно, хотя число точек пересечения ребер можно свести к 1:



Предположим, что наш граф допускает плоскую реализацию. Начертим на плоскости непересекающиеся ребра AX, BX, YB, YC, CZ, ZA :



Можно считать, что полученный замкнутый контур описывается непрерывной кривой. Проводя непересекающиеся непрерывные линии AY и BZ, можно считать, что одна из них лежит внутри контура, а вторая вне его. Но тогда дуга CX обязательно пересечет одну из дуг. В доказательстве есть элементы интуитивности. Строгость достигается, если пользоваться теоремой Жордана:

Пусть K – непрерывная замкнутая линия на плоскости. Линия K делит плоскость на внешнюю и внутреннюю области так, что любая непрерывная кривая, соединяющая любую точку внутренней области с некоторой точкой внешней области, пересекает K.

Другое доказательство основано на следующей теореме Л.Эйлера (1752), справедливой для любого конечного плоского связанного графа:
$b + r = p + 2$, где b – порядок графа, p – число его ребер и r – число его граней.

В нашем графе $b = 6,\ p = 9$. Если бы граф был бы плоским, то
$r = 11-6 = 5$. Обозначим через φ_k – число k-угольных граней графа. Тогда $r = \varphi_2 + \varphi_3 + \ldots$ и $2p = 2\varphi_2 + 3\varphi_3 + \ldots$, так как каждое ребро принадлежит двум граням. Следовательно,

$$5 = \varphi_2 + \varphi_3 + \ldots,$$

$$2p = 18 = 2\varphi_2 + 3\varphi_3 + \ldots.$$

Так как $\varphi_2 = \varphi_3 = 0$, то

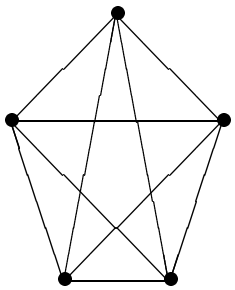
$$5 = \varphi_4 + \varphi_5 + \ldots,$$

$$18 = 4\varphi_4 + 5\varphi_5 + 6\varphi_6 + \ldots,$$

$$20 = 4\varphi_4 + 4\varphi_5 + 4\varphi_6 + \dots .$$

Откуда следует, что $18 > 20$. Противоречие.

Задача 3. Доказать, что полный граф K^5 не является плоским.



K^5

РЕШЕНИЕ. Действительно, допустив противное, имеем

$$b = 5,\ p = 10,\ r = p + 2 - b = 7.$$

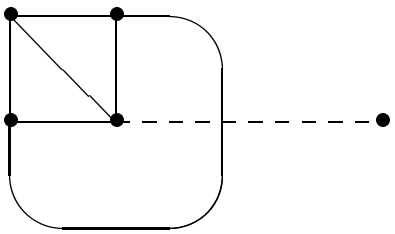
Следовательно,

$$7 = \varphi_2 + \varphi_3 + \dots ,$$

$$20 = 2\varphi_2 + 3\varphi_3 + \dots .$$

Так как $\varphi_2 = 0$, то $21 = 3\varphi_3 + 3\varphi_4 + 3\varphi_5 + \dots > 20 = 3\varphi_3 + 4\varphi_4 + 5\varphi_5 + \dots$. Противоречие.

Задача 4. Каждый из 4-х соседей соединил свой дом с тремя другими домами при помощи непересекающихся дорожек.



Пятый человек построил свой дом поблизости. Доказать, что его нельзя соединить с другими домами непересекающимися дорожками.

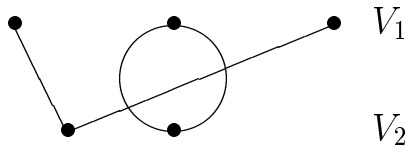
УКАЗАНИЕ 1. Воспользоваться теоремой Жордана.

УКАЗАНИЕ 2. Воспользоваться теоремой Эйлера.

Имеем $b = 5,\ p = 10,\ r = p + 2 - b = 7$. Далее рассуждаем аналогично решению задачи 2.

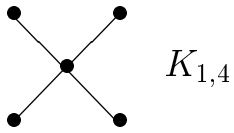
Двудольные графы

Граф $G = (V, E)$ называется двудольным, если $V = V_1 \cup V_2, V_1 \cap V_2 = \emptyset$ и каждое ребро соединяет какую-нибудь вершину из V_1 с какой-либо вершиной из V_2. Например,



Если двудольный граф является простым и каждая вершина из V_1 соединена с каждой вершиной из V_2, то он называется полным двудольным и обозначается $K_{m,n}$, где $m = |V_1|, n = |V_2|$. Ясно, что $K_{m,n} = E^m + E^n$. Граф $K_{1,n}$ называется звездным.

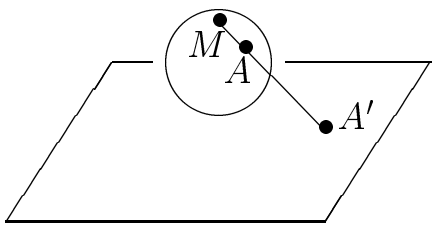
Пример 6.



Пример 7. Граф, возникающий в задаче о трех колодцах, изоморфен $K_{3,3}$.

Утверждение 3. *Граф планарен, т.е. изоморфен плоскому графу, тогда и только тогда, когда он укладывается на поверхности сферы.*

ДОКАЗАТЕЛЬСТВО. Пусть граф уложен на поверхности сферы. Выберем точку M на сфере, не совпадающей ни с одной вершиной графа и не лежащей ни на одном его ребре. Плоское представление графа получается применением стереографической проекции из т. M на плоскость, диаметрально противоположную точке M.



Обратное утверждение доказывается аналогично.

Определение. Два графа называются гомеоморфными, если они оба получаются из одного и того же графа включением в его ребра новых вершин степени 2.

Пример 8. Графы

являются гомеоморфными.

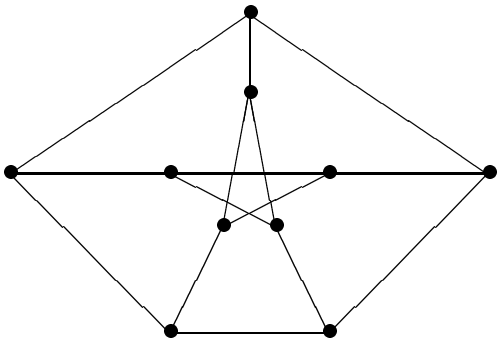
Утверждение 4 (теорема Понтрягина-Куратовского).

Граф планарен тогда и только тогда, когда он не содержит подграфов, гомеоморфных K^5 *или* $K_{3,3}$.

Замечание. Л.С.Понтрягин доказал ее в 1927 г., но не опубликовал; К.Куратовский доказал ее независимо в 1930 г.

ДОКАЗАТЕЛЬСТВО см. в [22].

Задача 5. Доказать, что регулярный граф Петерсена



не является планарным.

УКАЗАНИЕ. Если $\alpha = \{a, b\} \in E(G)$, то операция удаления ребра α в G и отождествление вершин a и b называется стягиванием. Справедлива теорема о том, что граф является планарным тогда и только тогда, когда

в нем нет подграфов, стягиваемых к K^5 или $K_{3,3}$. Примените эту теорему для решения данной задачи.

Матрицей смежности графа $G = (V, E)$ называется матрица $A = (a_{ij})$ размера $n \times n$, в которой a_{ij} равно числу ребер, соединяющих вершину v_i с v_j, где $V = \{v_1, \ldots, v_n\}$.

Задача 6.

а) Построить матрицы смежности графов: $K^4, K_{3,2}$.

ОТВЕТЫ: $\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}$,

б) Пусть G_n – граф с множеством вершин $\{v_1, \ldots, v_n\}$, в котором v_i и v_j инцидентны $\leftrightarrow (i, j) = 1$. Изобразить G_4, G_8 и найти их матрицы смежности. Доказать, что если $m < n$, то G_m – подграф G_n.

Задача 7. Пусть G – простой конечный граф (т.е. в нем нет петель и кратных ребер). Тогда G содержит две вершины с одинаковыми степенями ($n = |G| \geq 2$).

УКАЗАНИЕ. Достаточно считать, что граф является связным. Пусть $V = \{v_1, \ldots, v_n\}$. Если $1 \leq \rho(v_1) < \rho(v_2) \cdots < \rho(v_n)$, то из неравенств $\rho(v_i) \leq n - 1,\ i \leq n - 1$ и принципа Дирихле следует, что найдутся $\alpha, \beta \leq n$ такие, что

$$\rho(v_\alpha) = \rho(v_\beta),\ (\alpha \neq \beta).$$

Задача 8. Докажите, что среди 6 человек всегда найдутся трое таких, которые либо попарно знакомы, либо ни один из них не знает двух других.

Задача 9. Приведите примеры (когда это возможно):

а) двудольного регулярного графа;

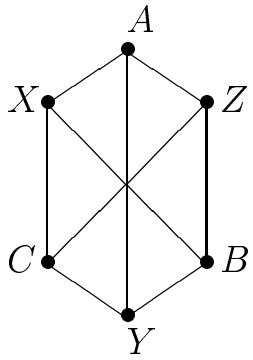
б) кубического графа порядка 9;

в) платонова двудольного графа;

г) простого графа порядка n, имеющего $(n-1)(n-1)/2$ ребер.

ОТВЕТ на вопрос г): $K^{n-1} \cup E^1$.

Замечание. При решении задач полезно иметь в виду следующее изображение графа $K_{3,3}$:

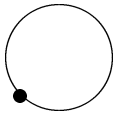


2.2 Теорема Л.Эйлера о плоских графах

В предыдущем параграфе мы сформулировали теорему Эйлера для плоских связных графов и убедились в ее важности. Прежде чем строго формулировать теорему, определим понятие грани графа $G = (V, E)$. Пусть x – точка плоскости, не принадлежащая V и не лежащая ни на одном ребре E. Грань графа G, содержащая x, это множество таких точек плоскости, которые можно соединить с x жордановыми кривыми, целиком состоящими из точек, не принадлежащих V и ребрам графа. Одна грань в графе является неограниченной.

Теорема. (Эйлер Л., 1752) *Пусть G – плоский связный граф; пусть $b = |G|$, $p = v(G)$, r – число граней G. Тогда $p + 2 = b + r$.*

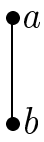
ДОКАЗАТЕЛЬСТВО. Доказательство проведем индукцией по p. Если $p = 0$, то $b = 1$ и $r = 1$. Теорема доказана. Предположим, что теорема верна для графов с числом ребер $\leq p - 1$. Рассмотрим плоский граф G с $v(G) = p$. Если он содержит петлю



,

то ее удаление уменьшает число ребер на 1 и число граней тоже на 1, т.е.

искомое равенство является верным. Если G содержит ребро вида



где $\rho(a) = 1$, то удаляя из G вершину a и это ребро, мы докажем искомое равенство в силу предположения индукции. Итак, можно считать, что G – плоский связный граф, в котором степень каждой вершины ≥ 2 и среди ребер нет петель (и кратных ребер).

Лемма. *Если степень каждой вершины графа G_1 не меньше двух, то G_1 содержит цикл.*

ДОКАЗАТЕЛЬСТВО. Если в G_1 есть петли или кратные ребра, то лемма доказана. Иначе, G_1 – простой граф. Пусть $v \in V(G_1)$. Пусть v_1 – смежная вершина с v, v_2 – смежная вершина с v_1 и отличная от v, v_3 – смежная вершина с v_2 и отличная от v_1 и т.д. Так как $|G_1| < \infty$, то в последовательности $v, v_1, v_2, \ldots$ встретится вершина v_k, которая встречалась раньше. Выбирая k минимальным с этим свойством, мы получим искомый цикл.

Следовательно граф G содержит цикл. Удалим в этом цикле одно ребро. Полученный граф является снова связным, но число его ребер $p_1 = p - 1$ и число его граней $r_1 = r - 1$. Ввиду предположения индукции $p_1 + 2 = b_1 + r_1$. Следовательно, $p + 2 = b + r$ и теорема доказана.

Если мы рассмотрим выпуклый многогранник в $\mathbf{R}^{(3)}$ и спроектируем его на поверхности сферы, описанной около него, а затем воспользуемся стереографической проекцией, то мы получим плоский связный граф многогранника, для которого справедлива формула Эйлера

$$p + 2 = b + r.$$

Следствие 1. *Если $G = (V, E)$ – связный простой планарный граф порядка $n = |V| \geq 3$ и размера $m = |E|$, то $m \leq 3n - 6$.*

ДОКАЗАТЕЛЬСТВО. Подсчитывая ребра в графе, имеем $3r \leq 2m$. Следовательно,

$$m + 2 = n + r \leq n + \frac{2}{3}m, \qquad m \leq 3(n-2).$$

Следствие 2. *В любом простом планарном графе существует вершина, степень которой не превосходит 5.*

ДОКАЗАТЕЛЬСТВО.Для доказательства достаточно считать, что граф является связным. Если степень каждой вершины ≥ 6, то $6 \cdot n \leq 2m$, где n – число всех вершин и m – число всех ребер. Откуда следует, что $3n \leq m \leq 3n - 6$. Противоречие.

Следствие 3. *Пусть G – плоский граф порядка n, с m ребрами, r гранями и k компонентами связности. Тогда $n + r = m + (k + 1)$.*

Доказательство следует из теоремы и того, что бесконечная грань считается только один раз.

Задача 10. Пусть $G = (V, E)$ – планарный граф порядка $n \geq 3$, в котором все циклы содержат $\geq g \geq 3$ ребер. Доказать, что число ребер

$$m = |E| \leq max\{(n-1),\ \frac{g}{(g-2)}(n-2)\}.$$

УКАЗАНИЕ. Можно считать, что $g \leq n$ и G – связный граф. Если в G каждое ребро принадлежит двум граням, то

$$2m = \sum_i f_i \cdot i \geq \sum_{i \geq g} f_i \cdot i \geq g(\sum_i f_i) = g \cdot r,$$

где r – число всех граней и f_i – число граней с i ребрами на своих границах. Следовательно,

$$m + 2 = n + r \leq n + \frac{2}{g}m,$$

$$m \leq \frac{g}{g-2}(n-2).$$

Если ребро $\{a, b\} \in E$ принадлежит одной грани, то $G \setminus \{a, b\}$ – объединение двух непересекающихся графов G_1 и G_2. Полагая $m_i = |E(G_i)|$, $n_i = |G_i|, i \leq 2$, имеем, что

$m = m_1 + m_2 + 1 \leq max\{\frac{g}{g-2}(n_1 - 2), n_1 - 1\}+$
$+max\{\frac{g}{g-2}(n_2 - 2),\ n_2 - 1\} + 1 \leq max\{\frac{g}{g-2}(n - 2), n - 1\}.$

В частности, если бы граф K^5 был бы плоским, то
$g = 3,\ v(K^5) = 10 < \frac{3}{1} \cdot (5 - 2)$. Противоречие.

2.3 Оценка числа графов

Обозначим через H_n^m – число всех сочетаний с повторениями из n элементов по m, т.е. число всех таких семейств, содержащих m элементов из данных n и различных элементов, что один и тот же элемент может входить в семейство несколько раз. Следующее утверждение доказано в 1.1. Здесь мы приведем второе доказательство.

Утверждение 5. $H_n^m = C_{m+n-1}^m$.

Пример. $H_2^3 = 4$, т.к. на базе $\{a, b\}$ существуют только следующие семейства из 3-х элементов:

$$\{a, a, a\}, \qquad \{a, a, b\}, \qquad \{a, b, b\}, \qquad \{b, b, b\}.$$

ДОКАЗАТЕЛЬСТВО. Рассмотрим основное множество $M = \{a_1, \ldots, a_n\}$. Если $n = 1$, то $H_1^m = 1 = C_m^m$ и все доказано. Сделаем предположение индукции об истинности нашего утверждения для n элементного множества и докажем его для множества, содержащего $(n + 1)$ элементов:

$$N = \{a_1, \ldots, a_{n+1}\}.$$

Число сочетаний с повторениями из $(n+1)$ элементов по m, не содержащих a_{n+1}, равно H_n^m; число сочетаний с повторениями из $(n + 1)$ элементов по m, содержащих a_{n+1} ровно один раз, равно H_n^{m-1}; число сочетаний с повторениями из $(n + 1)$ элементов по m, содержащих a_{n+1} ровно 2 раза, равно H_n^{m-2} и т.д. Следовательно,

$H_{n+1}^m = H_n^m + H_n^{m-2} + \cdots + H_n^1 + 1 = C_{n+m-1}^m + C_{n+m-2}^{m-1} + \cdots + C_n^1 + 1.$

Докажем индукцией по m, что

$$C_{n+m}^m = 1 + C_n^1 + C_{n+1}^2 + \cdots + C_{n+m-1}^m.$$

Если $m = 1$, то $C_{n+1}^1 = n + 1 = 1 + C_n^1$. Пусть искомое равенство верно для m. Докажем его для $m + 1$. Имеем

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

Утверждение доказано.

Утверждение 6. $(\frac{n}{e})^n < n!$

ДОКАЗАТЕЛЬСТВО. Так как $(1 + \frac{1}{n})^n < e$, то $\frac{(n+1)^n}{e} < n^n$.

Предположим истинность нашего неравенства для n и докажем его для $(n + 1)$. Имеем

$$(n+1)! = n! \cdot (n+1) > (\frac{n}{e})^n \cdot (n+1) > \frac{(n+1)^n}{e \cdot e^n} \cdot (n+1) = (\frac{n+1}{e})^{n+1}.$$

Теорема 2. *Максимальное число $\gamma(m)$ попарно неизоморфных графов без изолированных вершин с m ребрами удовлетворяет неравенству*

$$\gamma(m) < c_1(c_2 m)^m,$$

где c_1, c_2 – некоторые константы.

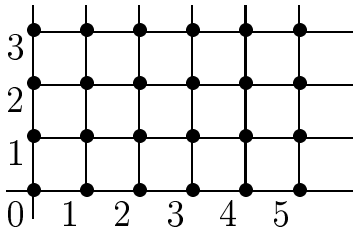
ДОКАЗАТЕЛЬСТВО. Каждый граф с m ребрами имеет не более $2m$ вершин. На множестве из $2m$ вершин число пар вершин, которые могут связываться ребрами, не превосходит числа $r = H_{2m}^2 = C_{2m+1}^2 = m(2m + 1)$. Тогда искомое число графов с m ребрами $\gamma(m)$ не превосходит

$H_r{}^m = C_{r+m-1}^m \le \frac{(r+m-1)^m}{m!} < \frac{(2m^2+2m)^m}{(\frac{m}{e})^m} = (1 + \frac{1}{m})^m \cdot (2em)^m < e \cdot (2em)^m.$

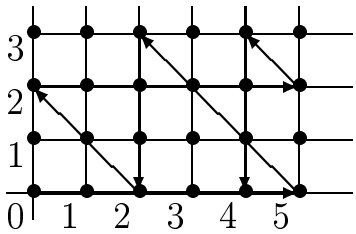
Теорема доказана.

Задача 11. У Вас имеется 3 кувшина A, B, C объемом соответственно 8, 5 и 3 литров. Кувшин A наполнен водой. Вам необходимо разделить воду на 2 равные части, используя пустые кувшины B, C. Можно ли это сделать?

РЕШЕНИЕ. Предлагается следующее решение, использующее язык теории графов. Рассмотрим целочисленную решетку плоскости



Каждому распределению воды по кувшинам B и C сопоставим точку (a, b) нашей решетки, где b – количество воды в B и c – количество воды в C. Так как $b \in \{0, 1, 2, 3, 4, 5\}, c \in \{0, 1, 2, 3\}$, то множество возможных узловых точек решетки состоит из 6 х 4=24 точек. Будем считать точки вершинами графа. Две вершины (b_1, c_1) и (b_2, c_2) соединены (ориентированным) ребром, если за одно переливание из состояния (b_1, c_1) можно перейти к состоянию (b_2, c_2). Наша задача заключается в существовании пути (маршрута) от вершины (0,0) к вершине (4,0). Укажем такой путь: $(0, 0) \to (5, 0) \to (2, 3) \to (2, 0) \to (0, 2) \to (5, 2) \to (4, 3) \to (4, 0)$. Проиллюстрируем этот путь графически:



Задача 12. Решить аналогичную задачу для кувшинов A, B, C, объемы которых соответственно равны 12, 7, 4.

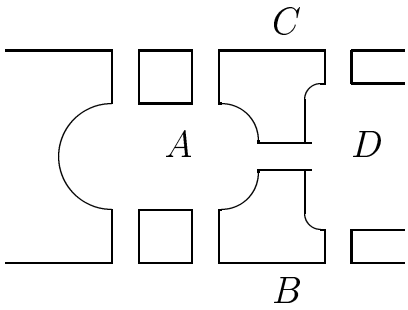
ОТВЕТ: (7, 0), (3, 4), (3, 0),(0, 3), (7, 3), (6, 4), (6, 0).

2.4 Эйлеровы и гамильтоновы графы

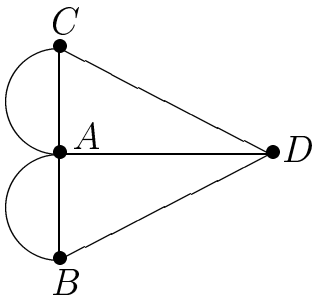
Как уже отмечалось, теория графов своим рождением обязана следующей задаче, возникшей в первой половине XVIII столетия и решенной петербургским математиком Л.Эйлером (см. рис.).

Город Кенигсберг (Калининград) расположен на берегах реки Прегель и двух островах. Различные части города были соединены 7 мостами. Можно

ли совершить прогулку по городу таким образом, чтобы, выйдя из дома, вернуться обратно, пройдя по каждому мосту только один раз?



Изобразим карту рисунка в виде графа



Л.Эйлер доказал, что не существует маршрута, включающего в себя каждое ребро только один раз. Л.Эйлер поставил более общий вопрос: для каких графов существует цикл (т.е. замкнутая цепь), содержащий все ребра графа, причем каждое ребро в точности по одному разу?

Графы, обладающие таким циклом (эйлеровой линией), называются эйлеровыми. Такой граф, очевидно, связный и степень каждой его вершины является четной.

Теорема 3. *Конечный граф $G = (V, E)$ является эйлеровым тогда и только тогда, когда он связный и степень каждой его вершины является четной.*

ДОКАЗАТЕЛЬСТВО. Если G – эйлеров граф, то, как было отмечено, он связный и степень каждой его вершины четная. Обратно, пусть G – связный граф и степени всех его вершин являются четными числами. Возьмем некоторую вершину $a \in V$ и рассмотрим максимальную цепь T, исходящую из a. Так как граф G связный и степень каждой вершины четная, то T проходит через каждую вершину G и заканчивается в a. В частности, T

является циклом. Если этот цикл не является эйлеровым, то T содержит вершину b, инцидентную ребру, не входящему в T. Исходя из вершины b, построим новую цепь, используя ребра, не принадлежащие T. Это возможно, т.к. степень каждой вершины является четной. Новая цепь L должна оканчиваться в вершине b. Но тогда мы можем построить больший чем T цикл, исходящий из вершины a. Действительно, сначала следуем по T от a к b, затем по L делаем цикл и возвращаемся в b, а затем продолжаем путь по T. Это противоречит максимальности пути T.

Итак, T – эйлеров цикл. Теорема доказана.

Если же на связном конечном графе $G = (V, E)$ имеется цепь, начинающаяся в вершине a и оканчивающаяся в вершине $b \neq a$, то предполагая, что она проходит по всем ребрам в точности по одному разу, мы видим, что a, b – единственные вершины нечетной степени. Обратно, если в связном конечном графе $G = (V, E)$ вершины a и b $(a \neq b)$ являются единственными нечетными, то, добавляя к E новое ребро $\{a, b\}$, мы получим (согласно теореме 3) эйлеров граф, обладающий эйлеровым циклом T. Удалив из T ребро $\{a, b\}$, мы получим цепь, начинающуюся в a, заканчивающуюся в b и проходящую каждое ребро ровно один раз. Итак, доказана

Теорема 4. *Конечный связный граф $G = (V, E)$ содержит цепь, начинающуюся в вершине a и оканчивающуюся в вершине b, а также содержащую все ребра ровно по одному разу тогда и только тогда, когда a, b – единственные нечетные вершины этого графа.*

Задача 13. Пусть $G = (V, E)$ – конечный связный граф с $2k$ нечетными вершинами. Доказать, что G имеет семейство из k цепей, которые в совокупности содержат все ребра графа ровно по одному разу.

УКАЗАНИЕ. Пусть $\{a_1, \ldots, a_k, b_1, \ldots, b_k\}$ – нечетные вершины. Добавим к E новые ребра $\{a_1, b_1\}, \ldots, \{a_k, b_k\}$. Мы получим эйлеров граф, содержащий эйлеров цикл T. Удалим из T новые ребра. Получим искомое семейство из k цепей.

Задача 14. Конечный связный граф является эйлеровым тогда и только тогда, когда семейство его ребер можно разбить на непересекающиеся циклы.

Алгоритм Флери построения эйлеровой цепи в эйлеровом графе G

Выходя из произвольной вершины a, идем по ребрам графа, соблюдая правила:

1) стираем ребра по мере их прохождения и стираем изолированные вершины, которые при этом образуются;

2) на каждом этапе идем по мосту (ребро называется мостом, если его удаление нарушает связность графа) только тогда, когда нет других возможностей.

Указанный алгоритм действительно работает при прохождении каждой вершины b. Если $b \neq a$, то оставшийся подграф H связен и содержит ровно 2 вершины нечетной степени $\{a, b\}$. По теореме 4 существует эйлерова цепь T из b в a. Удалим первое ребро этой цепи T. Граф H останется связным и данное рассуждение можно продолжить. Если же $b = a$, то рассуждаем аналогично.

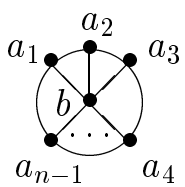
Задача 15:

а) найти все платоновы эйлеровы графы;

б) для каких чисел m, n следующие графы будут эйлеровыми: K^n, $K_{m,n}$?

ОТВЕТЫ: а) октаэдр; б) n – нечетное число; $m \equiv n \equiv 0 (mod\ 2)$.

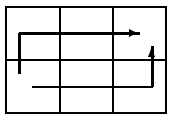
Задача 16. Пусть C_{n-1} – циклический граф порядка $n-1$. Тогда $W_n = E^1 + C_{n-1}$ (колесо с n вершинами):



W_n

При каких n граф W_n является эйлеровым?

Задача 17. Можно ли ходом шахматного коня обойти всю шахматную доску (8 x 8) так, чтобы каждый ход встречался ровно один раз? При этом ходы



мы отождествляем.

УКАЗАНИЕ. Рассмотрим граф порядка 64; две вершины его инцидентны, если возможен ход конем из одной в другую; заметить, что он связный и применить теорему Эйлера.

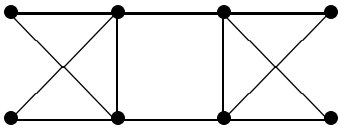
Задача 18. Можно ли ходом шахматного коня попасть из левого нижнего угла доски в правый верхний угол, побывав в каждом поле ровно один раз?

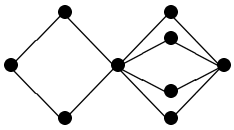
УКАЗАНИЕ. Предположим противное. Тогда необходимо сделать 63 хода. При каждом ходе меняется цвет клетки на противоположный. Так как диагональ одноцветна, то получаем противоречие.

Задача 19:

а) доказать, что K^5 имеет 264 эйлеровы цепи;

б) найти эйлеровы цепи графов





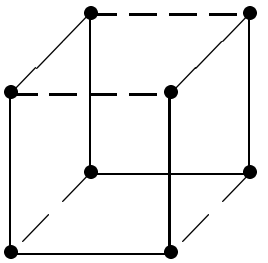
Определение. Пусть G – конечный связный граф. G называется гамильтоновым графом, если существует цикл (гамильтоновый), проходящий через каждую вершину ровно один раз. Цепь графа называется гамильтоновой, если это простая цепь (т.е. без петель и кратных ребер), проходящая через все вершины по одному разу.

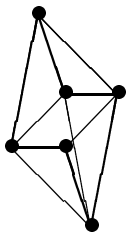
ИСТОРИЧЕСКАЯ СПРАВКА. Сэр У.Р.Гамильтон (*W.R.Hamilton*) – ирланский математик (1805-1865), профессор Дублинского университета. Доказал т.н. теорему Гамильтона-Кэли для матриц, ввел в рассмотрение тело кватернионов (первый пример некоммутативной алгебры с делением).

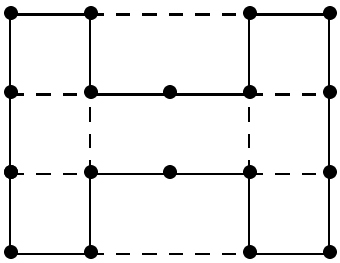
Примером гамильтонова графа является граф порядка 64 из задачи 17. Укажем один из гамильтоновых циклов в нем (задача Л.Эйлера о рыцарях, 1759):

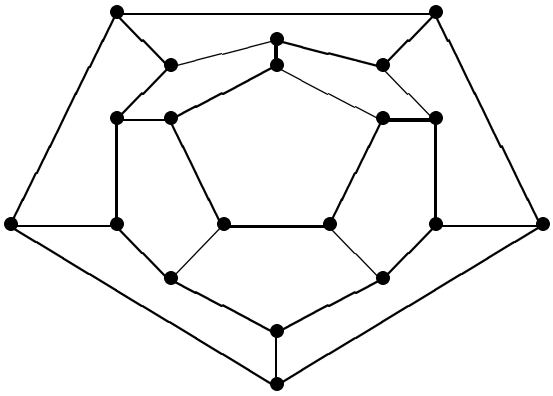
56	41	58	35	50	39	60	33
47	44	55	40	59	34	51	38
42	57	46	49	36	53	32	61
45	48	43	54	31	62	37	52
20	5	30	63	22	11	16	13
29	64	21	4	17	14	25	10
6	19	2	27	8	23	12	15
1	28	7	18	3	26	9	24

Другими примерами являются следующие графы:





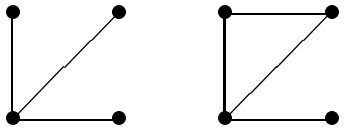




додекаэдр, пример У. Гамильтона, 1857

Граф называется полугамильтоновым, если в нем существует гамильтонова цепь. Примерами негамильтонова графа и полугамильтонова графа

являются графы:



С гамильтоновыми графами связана и следующая задача о коммивояжере ("о бродячем торговце"). Торговый агент должен посетить какое-то количество городов, побывав в каждом городе ровно один раз. Расстояния (стоимость билета) между городами известны. Необходимо выбрать кратчайший (самый дешевый) путь (с возвратом в исходный город).

Задача 20:

а) какие из платоновых графов имеют гамильтоновы цепи (циклы)?

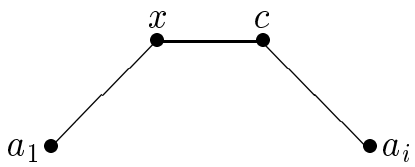
б) имеют ли решения задачи о рыцарях на шахматной доске $n \times n$ при $n = 3, 4, 5, 6, 7$?

в) для каких чисел m, n графы $K_{m,n}, W_n, K^n$ являются гамильтоновыми?

К сожалению, в отличие от эйлеровых графов, для гамильтоновых графов нет теоремы, претендующей на полное описание таких графов. Приведем, однако, следующий результат.

Теорема 5. (Г.Дирак, 1952). *Пусть $G = (V, E)$ – простой конечный граф порядка $n \geq 3$ такой, что степень каждой вершины $\geq n/2$. Тогда G – гамильтонов граф.*

ДОКАЗАТЕЛЬСТВО. Если граф G не является гамильтоновым, то его можно достроить до гамильтонова графа G_1, добавив некоторое конечное число вершин $b_1, b_2, \ldots, b_k$ и соединив их со всеми вершинами $\{a_1, \ldots, a_n\}$ графа G. При этом можно считать, что $k > 0$ и k является минимальным с этим свойством. Пусть $a_1 \to b_1 \to a_i \to \cdots \to a_1$ – гамильтонов цикл в G_1. Вершина a_i не является смежной с a_1 в графе G_1, иначе бы мы не использовали вершину b_1 (а это противоречило бы минимальности k). Предположим, что существует вершина c смежная с a_i, которая следует (в нашем цикле) за вершиной x, смежной с a_1 :



$$a_1 \to b_1 \to \underline{a_i \to \cdots \to x} \to c \to \cdots \to a_1.$$

Тогда заменим последний цикл на цикл

$$a_1 \to \underline{x \to \cdots \to a_i} \to c \to \cdots \to a_1,$$

который отличается от предыдущего обратной ориентацией прохода в выделенной части. Противоречие с минимальностью k (мы не использовали b_1!). Число вершин графа G_1, не являющихся смежными с a_i, не меньше числа вершин, смежных с a_1 (т.е. $\geq n/2+k$), т.к. в нашем цикле за каждой смежной с a_1 следует некоторая вершина, не являющаяся смежной с a_i. С другой стороны, число вершин смежных с $a_i \geq \frac{n}{2} + k$. Поэтому порядок графа G_1 не меньше числа $n + 2k$. Противоречие доказывает теорему.

Задача 21. В полном графе K^{2n+1} найти n гамильтоновых циклов, каждые два из которых не имеют общих ребер.

2.5 Деревья

Сделаем сначала несколько замечаний.

1. Пусть x – некоторая вершина графа $G = (V, E)$ и W – множество всех вершин связной компоненты G, содержащей x. Тогда

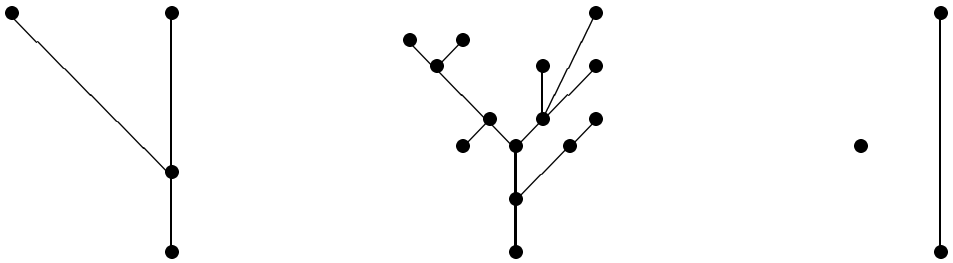
$W = \{y \in V; G$ содержит маршрут $A_{xy}\}$.

2. Граф $G = (V, E)$ является двудольным тогда и только тогда, когда он не содержит нечетных циклов. Действительно, если G – двудольный граф и $V = V_1 \cup V_2$, где $V_1 \cap V_2 = \emptyset$, то для любого цикла $x_1x_2 \ldots x_e$ имеем $x_1 \in V_1$ (например), $x_2 \in V_2, x_3 \in V_1$ и т.д.. Так как $x_2 \in V_2$, то e – четное число. Обратно, пусть G не содержит нечетных циклов. Заметим, что G – двудольный граф тогда и только тогда, когда все его связные компоненты

являются двудольными, т.е. мы можем считать, что G – связный граф. Пусть $x \in V$. Пусть $V_1 = \{y \in V;$ минимальная длина $d(x,y)$ пути $A_{x,y}$ является нечетной $\}$ и $V_2 = V \setminus V_1$. Если какие-нибудь вершины из V_i, $i = 1, 2$, соединены ребром, то G содержит нечетный цикл.

Определение. Граф, не содержащий циклов, называется лесом или ациклическим графом. Связный лес называется деревом.

Примеры деревьев:



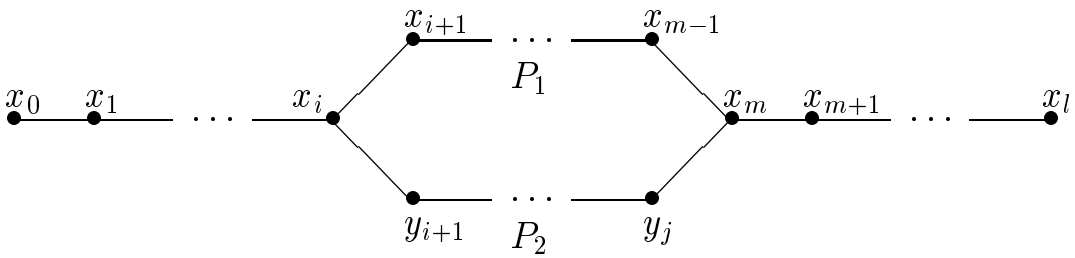
Ясно, что лес является объединением непересекающихся деревьев.

Утверждение 6. *Граф G является деревом тогда и только тогда, когда для любых двух различных вершин x, y существует не более одного пути $A_{x,y}$.*

ДОКАЗАТЕЛЬСТВО. Действительно, если G не является деревом и $x_1 \dots x_e$ – цикл, то $x_1 x_2 \dots x_e$ и $\{x_1, x_e\}$ – два пути A_{x_1,x_e}. Обратно, пусть G – дерево и

$$P_1 = x_0 x_1 \dots x_e\,, \qquad P_2 = x_0 y_1 \dots y_k x_e$$

два пути A_{x_1,x_e}. Пусть $i+1$ – минимальный индекс такой, что $x_{i+1} \neq y_{i+1}$ (т.е. $x_1 = y_1, \dots, x_i = y_i$) и j – минимальное число такое, что $j \geq i$ и y_{j+1} – вершина P_1, скажем $y_{j+1} = x_m$. Тогда



и $x_i x_{i+1} \dots x_m y_j \dots y_{i+1}$ – цикл G. Противоречие.

Утверждение 7. *Следующие утверждения эквивалентны для графа G:*

а) G – дерево;

б) G – минимальный связный граф, т.е. G – связный граф и для любого ребра $\{a,b\} \in E(G)$ граф $G \setminus \{a,b\}$ является несвязным (другими словами, каждое ребро является мостом);

в) G – максимальный ациклический граф, т.е. G – ациклический граф и если x, y – несмежные вершины G, то $G + \{x,y\}$ содержит цикл.

ДОКАЗАТЕЛЬСТВО. а) $\Rightarrow$ б). Пусть G – дерево и $\{x,y\} \in E(G)$. Граф $G \setminus \{x,y\}$ не содержит $A_{x,y}$ пути $x z_1 \dots z_k y$, т.к. иначе G содержит цикл. Таким образом, $G \setminus \{x,y\}$ – несвязный граф. Докажем, что б) $\Rightarrow$ в). Пусть G – минимальный связный граф и $x z_1 \dots z_k y$ – цикл в нем. Тогда $G \setminus \{x,y\}$ – связный граф, т.к. в любом пути $A_{u,v}$ ребро $\{x,y\}$ заменяется на путь $x z_1 \dots z_k y$. Противоречие. Т.е. G – дерево. Если a, b – две несмежные вершины его, то существует путь $a z_1 \dots z_k b$ в G. Следовательно, граф $G + \{a,b\}$ содержит цикл $a z_1 \dots z_k b$. Это доказывает, что G – максимальный ациклический граф. Докажем, что в) $\Rightarrow$ а). Предположим, что G – несвязный граф и a, b – вершины его, принадлежащие разным компонентам связности. Рассмотрим граф $G + \{a,b\}$. Он должен содержать цикл $a z_1 \dots z_k b$. Но это означает, что G содержит $A_{a,b}$ путь. Противоречие.

Утверждение 8. *Каждый конечный связный граф G содержит дерево, содержащее все вершины графа.*

ДОКАЗАТЕЛЬСТВО. Пусть $n = |G|$ – порядок графа G и $x \in V(G)$. Положим T_1 – подграф, состоящий из одной вершины x. Предположим, что мы построили цепь деревьев

$$T_1 \subset T_2 \subset \dots \subset T_k \subset G$$

такую, что $|T_i| = i$. Если $k < n$, то, ввиду связности, существует вершина $y \in V(G) \setminus V(T_k)$, инцидентная некоторой вершине $z \in V(T_k)$. Пусть T_{k+1} – подграф, полученный из T_k присоединением этой вершины z и ребра $\{y,z\}$.

Тогда T_{k+1} является снова связным графом, в котором ребро $\{y, z\}$ не является ребром никакого цикла, т.е. T_{k+1} – ациклический граф. Продолжая этот процесс, мы построим искомое дерево T_n.

Следствие 1. *Пусть G – дерево порядка n. Тогда $|E(G)| = n - 1$.*

ДОКАЗАТЕЛЬСТВО. Действительно, из утверждения 8 следует, что G содержит подграф, являющийся деревом, и в котором $|E(T_n)| = n - 1$. Если $G \neq T_n$, то получаем противоречие с утверждением 7 (точнее, с минимальностью связного графа G.).

Следствие 2. *Пусть G – лес порядка n, имеющий k связных компонент. Тогда $|E(G)| = (n - k)$.*

Доказательство следует из следствия 1.

Следствие 3. *Пусть G – дерево порядка $n \geq 2$. Тогда G содержит (по меньшей мере) две вершины степени 1.*

ДОКАЗАТЕЛЬСТВО. Действительно, пусть $d_1 \leq d_2 \leq \cdots \leq d_n$ – неубывающая последовательность степеней вершин дерева G. Допустим противное. Тогда $d_2 \geq 2$ и $2|E(G)| = 2(n-1) = d_1 + d_2 + \cdots + d_n \geq 1 + 2(n-1)$. Противоречие.

Вернемся к предложению 8. Из него следует, что в любом связном графе (порядка n) есть дерево, содержащее все вершины графа. Оно называется основным (каркасным) деревом графа. Вернемся еще раз к построению этого остова. Если исходный граф G не содержит циклов, то он сам и является деревом. Иначе, возьмем любой цикл и удалим любое ребро из него. Мы не нарушим связность этого нового графа, но уменьшим в нем число циклов. Продолжая этот алгоритм, мы получим остовное дерево графа. Число удаленных ребер при применении этого алгоритма называется циклическим рангом (или цикломатическим числом) графа G и обозначается через $\gamma(G)$. Ясно, что $\gamma(G) = m - n + 1$, где $m = |E(G)|, n = |G|$. Применяя этот алгоритм к произвольному (не обязательно связному графу G), мы получим остовное дерево, циклический ранг $\gamma(G)$ которого ра-

вен $\gamma(G) = |E(G)| - |G| + k$, где k – число связных компонент. Число $x(G) = |G| - k$ (число ребер в остовном лесе) называется коциклическим рангом.

Задача 22. Найти число всех неизоморфных деревьев T порядка n, где $n \leq 7$.

ОТВЕТ: а) при $n = 6$ их число равно 6; б) при $n = 7$ их число равно 11.

Задача 23. Доказать, что каждое дерево является двудольным графом. Какие деревья являются полными двудольными графами?

УКАЗАНИЕ. Воспользоваться замечанием 2 в начале 2.5.

Задача 24. Найти циклические и коциклические ранги графов K^n, $K_{m,n}$, E^n, W_n, платоновых графов, графа Петерсена.

Задача 25. Пусть G – граф порядка n. Доказать эквивалентность следующих утверждений:

1) G – дерево;

2) G – связный и $|E(G)| = n - 1$;

3) G – ациклический и $|E(G)| = n - 1$;

4) если $n = 1$ или 2, то $G = K^n$; если $n \geq 3$, то $G \neq K^n$ и добавление одного ребра к G приводит к появлению ровно одного цикла.

УКАЗАНИЕ. Импликация 1) $\Rightarrow$ 2) следует из определения и следствия 1. Импликация 2) $\Rightarrow$ 3) следует из утверждения 8. Импликация 3) $\Rightarrow$ 4) при $n \leq 2$ очевидна. Если же $n \geq 3$, то ясно, что $G \neq K^n$. Докажем, что G – связный граф. Иначе, каждая из его k связных компонент является деревом и $|E(G)| = n - k = n - 1$. Т.к. $k = 1$. Остальное следует из утверждения 7.

Конечный граф $G = (V, E)$ порядка n назовем помеченным, если все его вершины "помечены" целыми числами от 1 до n, т.е. существует биекция $\varphi : \{v_1, \ldots, v_n\} \longrightarrow \{1, 2, \ldots, n\}$. Числа $\varphi(v_1), \ldots, \varphi(v_n)$ называются метками вершин $v_1, \ldots, v_n$. Два помеченных графа (G_1, φ_1) и (G_2, φ_2) называются изоморными, если существует изоморфизм между нашими графами, кото-

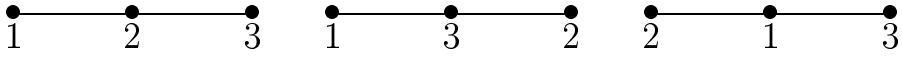
рый сохраняет распределение меток.

Приведем примеры всех помеченных неизоморфных деревьев порядка 2, 3, 4:

а) $n = 2$

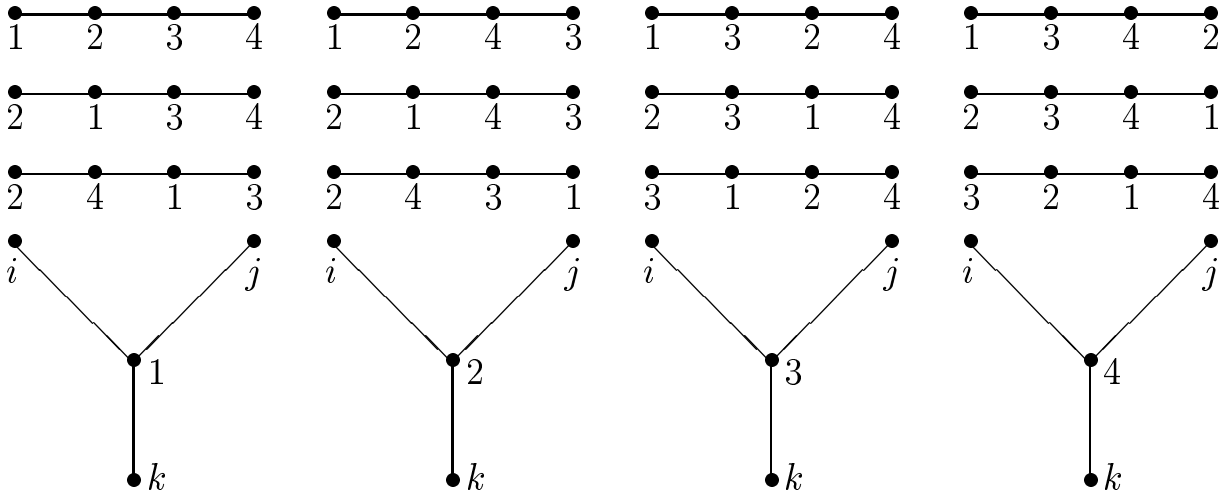
Их число равно 1.

б) $n = 3$



Их число равно 3.

в) $n = 4$



Их число равно 16.

Теорема 6.(А.Кэли, 1889)

Число различных помеченных деревьев порядка n равно n^{n-2}.

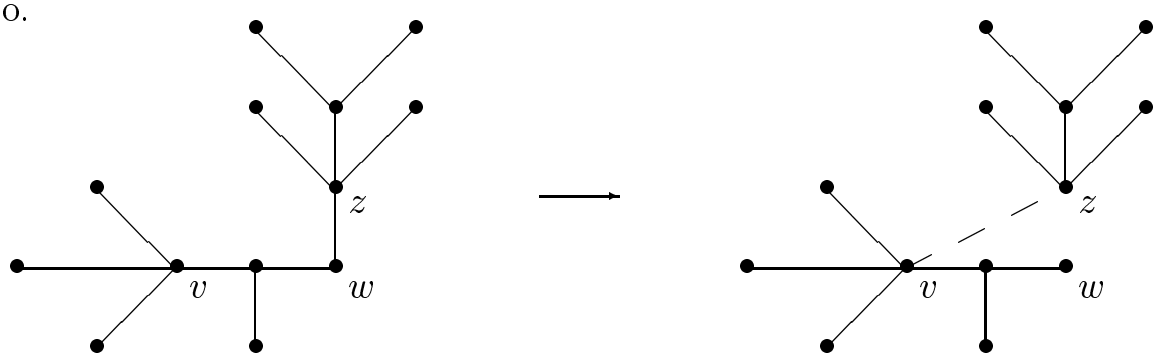
ИСТОРИЧЕСКАЯ СПРАВКА. Артур Кэли (1821-1895) – английский математик; известен исследованиями в теории групп и в теории колец (числа Кэли); автор работ по теории определителей (в частности, ввел в рассмотрение ныне действующее обозначение для определителя), по геометрии Лобачевского (модель Кэли-Клейна), по теории инвариантов и дифференциальным уравнениям.

ДОКАЗАТЕЛЬСТВО. Пусть $T(n, k)$ – число помеченных деревьев порядка n, в которых фиксированная вершина v имеет степень k. Докажем

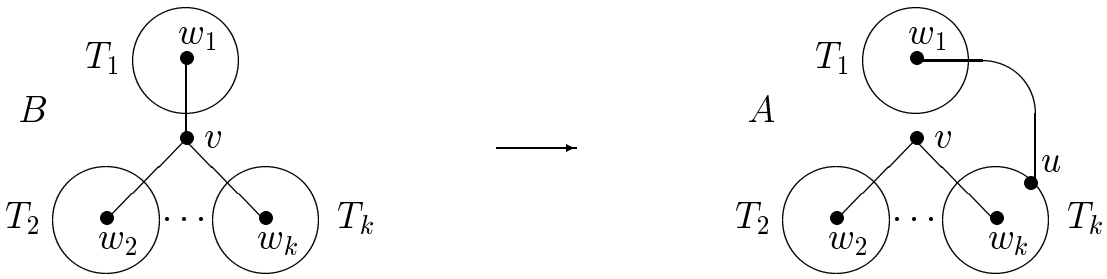
равенство $(*)$:

$$(n-1)(k-1)T(n,k) = (n-k)T(n,k-1).$$

Возьмем, сначала, любое помеченное дерево A порядка n, в котором $\rho(v) = k-1$. Возьмем в нем любое ребро $\{w, z\}$, не инцидентное v, и удалим его.



Из предыдущего следует, что удаленное ребро являлось мостом. Соединим вершину v новым ребром с вершиной z из другой связной компоненты. Тогда получим снова дерево B, в котором $\rho(v) = k$. Такую пару (A, B) мы будем называть связкой. Сколько таких связок? Дерево A можно выбрать $T(n, k-1)$ способами. Для каждого дерева A удаляемое из него ребро $\{w, z\}$ можно выбрать $(n-1)-(k-1) = n-k$ способами. Следовательно, число всех таких связок равно $(n-k)T(n,k-1)$. Возьмем теперь любое помеченное дерево B порядка n, в котором $\rho(v) = k$. Пусть $T_1, T_2, \ldots, T_k$ – поддеревья, полученные из B удалением вершины v с каждым из инцидентных ей ребер.



Удаляя, например, ребро $\{v, w_1\}$ и соединяя w_1 ребром с любой вершиной любого из оставшихся деревьев, мы получим дерево A, в котором

$\rho(v) = k - 1$. Т.е. получается связка (A, B) (и все связки получаются таким образом!). Подсчитаем другим способом число этих связок. Дерево B можно выбрать $T(n, k)$ способами. Для каждого такого выбора ребро $\{w_1, u\}$ можно получить $(n_2 + n_3 + \cdots + n_k) = (n - n_1 - 1)$ способами; ребро $\{w_2, u\}$ можно получить $(n - n_2 - 1)$ способами и т.д. Т.е. ребра $\{w_i, u\}$ можно получить $(n - n_1 - 1 + n - n_2 - 1 + \cdots + n - n_k - 1) =$
$= nk - k - (n - 1) = (n - 1)(k - 1)$ способами (мы использовали равенство $n_1 + n_2 + \cdots + n_k = n - 1$, где n_i – порядок дерева $T_i, i \leq k$). Следовательно, число всех связок равно $(n-1)(k-1)T(n, k)$, и формула $(*)$ доказана. Так как $T(n, n-1) = 1$, то из $(*)$ следует равенство

$$T(n, k) = C_{n-2}^{k-1} \cdot (n-1)^{n-k-1}.$$

Число $T(n)$ всех помеченных деревьев порядка n равно

$T(n) = T(n, 1) + T(n, 2) + \cdots + T(n, n-1) = \sum_{k=1}^{n-1} C_{n-2}^{k-1} \cdot (n-1)^{n-1-k} =$
$= ((n-1)+1)^{n-2} = n^{n-2}$. Теорема доказана.

Задача 26. Найти цикломатическое число полного графа.

Задача 27. Пусть $n \geq 3$. Доказать, что если полный граф K^n разложим в объединение гамильтоновых циклов (не имеющих общих ребер), то n – нечетное число.

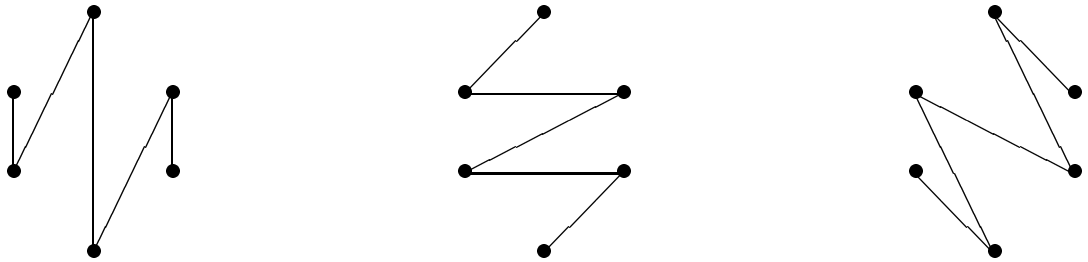
УКАЗАНИЕ. Граф K^n является однородным степени $(n-1)$. Каждый гамильтоновый цикл является 2-однородным. Следовательно, $2|(n-1)$ и n – нечетное число. Так как число всех ребер $|E(K^n)| = \frac{n(n-1)}{2}$, то в этом объединении будет $(n-1)/2$ циклов.

Задача 28. Пусть n – нечетное целое число ≥ 3. Доказать, что K^n является объединением $(n-1)/2$ гамильтоновых циклов (любые два из которых не имеют общих ребер).

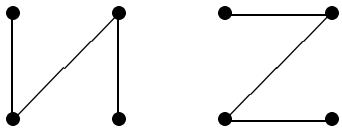
Задача 29. Полный граф $K^n (n \geq 2)$ разложим в объединение гамильтоновых путей (любые два из которых не имеют общих ребер) тогда и только тогда, когда n – четное число.

Примеры:

а) K^6 является объединением следующих гамильтоновых путей:



б) K^4 является объединением таких гамильтоновых путей



УКАЗАНИЕ. Если n – нечетное число, то с каждым гамильтоновым путем графа K^{n-1} можно связать гамильтонов цикл K^n (присоединяя оставшуюся вершину) и наоборот.

Задача 30. Доказать, что в связном конечном графе $G = (V, E)$, не являющимся деревом, каждой вершине можно поставить в соответствие смежное с ней ребро, т.е. существует инъективное отображение $\varphi : V \to E$ такое, что для любой вершины $v \in V$ существует вершина $u \in V$ такая, что $\varphi(v) = \{v, u\}$.

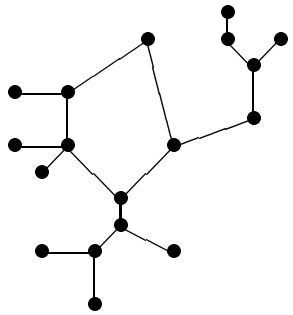
Иллюстрацией к этой задаче может служить пример города, в котором каждая улица имеет длину в один квартал, каждый перекресток (называется площадью) имеет название и из каждой площади исходит улица с тем же названием. Например, из площади Советов исходит улица Советская и т.д.

УКАЗАНИЕ. Если $n = |G| = |V|$, то $|E| \geq n$ (иначе, G – дерево).

Рассмотрим схему превращения G в дерево. Схема состоит из последовательного удаления ребер. Пусть $e = (a, b)$ – одно из таких удаляемых ребер и T – полученное в результате удаления дерево. Каждой вершине дерева T (кроме a!) поставим в соответствие смежное с ней ребро (это легко видеть,

если принять a за корень дерева), а вершине a поставим в соответствие удаленное ребро $e = (a, b)$.

Задача 31. Пусть $G = (V, E)$ – связный конечный граф. Существует инъективное отображение $\varphi : E \to V$ такое, что для любого ребра $e \in E$ вершина $\varphi(e)$ инцидентна e тогда и только тогда, когда G – дерево или G – цикл с деревьями, вырастающими из его вершин (см. рисунок).



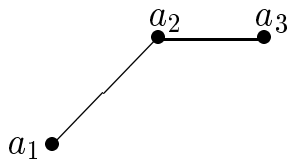
УКАЗАНИЕ. Если G – дерево и a_0 – его корень, то рассмотреть отображение $\{a_0, a_1\} \to a_1, \{a_0, a_2\} \to a_2, \{a_1, a_3\} \to a_3$ и т.д. Если G – цикл $a_1 a_2 \dots a_{n-1}$, то поставим в соответствие ребрам $\{a_{i-1}, a_i\} \to a_i, i \leq n-1$ и $\{a_{n-1}, a_1\} \to a_1$. Итак, ясно, что если граф имеет указанный в условии задачи вид, то искомое отображение существует. Обратно, если такое отображение существует и $C = a_1 a_2 \dots a_{n-1}$ – цикл G, то, например, $\varphi(\{a_1, a_2\}) = a_2$; и тогда $\varphi(\{a_2, a_3\}) = a_3$ и т.д. . Таким образом, $\varphi(C) = \{a_1, a_2, a_3, \dots, a_{n-1}\}$. Пусть $b_1 \in V$ инцидентна a_1. Тогда $\varphi(\{a_1, b_1\}) = b_1$ и a_1 – корень некоторого дерева, вырастающего из a_1. Аналогичные рассуждения относительно вершин $a_2, \dots, a_{n-1}$ приведут к решению задачи.

2.6 Экстремальные задачи, алгоритм Краскаля. Задача о четырех красках

Пусть у нас есть несколько деревень $a, b, c, \dots$, которые нужно соединить сетью асфальтированных дорог; при этом стоимость $f(a, b)$ дороги для каждой пары деревень $\{a, b\}$ известна. Как построить самую дешевую сеть

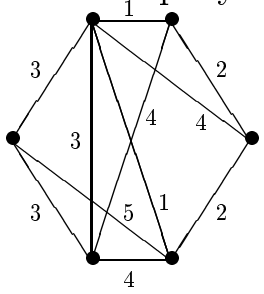
дорог, выполнив условие, что из любой деревни можно проехать в любую другую по такой дороге?

Если у нас три деревни



и $f(a_1, a_2) \leq f(a_2, a_3) \leq f(a_1, a_3)$, то ясно, что $f(a_1, a_2) + f(a_2, a_3)$ является минимальным.

В случае 6 деревень, с указанным на рисунке распределением стоимости,



решение уже не является очевидным.

Пусть $G = (V, E)$ – конечный связный граф и $f : E \to \mathbf{R}^+$. Укажем алгоритм нахождения связного подграфа $T = (V, E')$ графа G, для которого значение

$$f(T) = \sum_{\{x,y\} \in E'} f(\{x, y\})$$

является минимальным из возможных.

Если такой подграф существует, то он является деревом, т.к. если $a_1 a_2 \ldots a_{k-1}$ – некоторый цикл в нем, то удаление ребра $\{a_{k-1}, a_1\}$ не нарушает его связности, но уменьшает значение $f(T)$. Итак, если T существует, то T – дерево. Алгоритм нахождения такого дерева (его предложил Д.Краскаль (J.B.Kruskal, 1956)) назовем правилом экономичности, а само дерево назовем экономичным деревом. Алгоритм Краскаля:

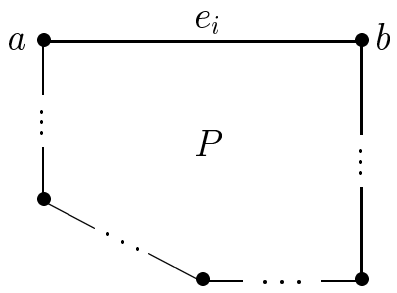
Шаг 1. Выберем вершины $a_1, a_2 \in V$ такие, что $f(\{a_1, a_2\})$ – минимальное из возможных значений.

Шаг 2. Присоединим к вершинам a_1, a_2 и ребру $e_1 = \{a_1, a_2\}$ ребро e_2 (и соответствующую вершину) с минимальным значением $f(e_2)$ таким, что

полученные ребра не образуют цикла.

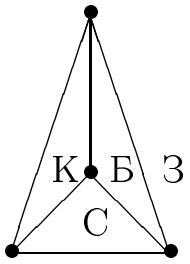
Предположим, что мы построили вершины $\{a_1, \ldots, a_{k+1}\}$ и соответствующие звенья (ребра) $e_1, e_2, \ldots, e_k$. Выберем самое дешевое ребро из $E \setminus \{e_1, \ldots, e_k\}$ такое, что его присоединение не приводит к появлению цикла.

Докажем, что так построенное экономичное дерево T действительно является минимальным из возможных. Так как среди подграфов G существуют деревья с числом вершин, равным порядку G, и их общее число является конечным, то, очевидно, существует и минимальное дерево T_0, т.е. $f(T_0)$ является минимальным из возможных. Занумеруем ребра $\{e_1, e_2, \ldots, e_{n-1}\}$ экономичного дерева T в порядке их присоединения. Если $T_0 \neq T$, то пусть $e_i = \{a, b\}$ – первое ребро, не принадлежащее $E(T_0)$. Пусть P – цепь дерева T_0, соединяющая (в T_0!) вершины a и b :



Так как T не содержит циклов, то найдется ребро e_i' в пути P такое, что $e_i' \notin E(T)$. Рассмотрим дерево $T_0' = (T_0 + \{e_i\}) \setminus \{e_i'\}$ (это связный граф с $n = |G|$ вершинами и $(n-1)$ ребрами!). Так как $f(T_0') = f(T_0) + f(e_i) - f(e_i') \geq f(T_0)$, то $f(e_i) \geq f(e_i')$. Так как $f(e_i)$ было минимальным, то $f(e_i') = f(e_i)$ и $f(T_0') = f(T_0)$. Но дерево T_0' имеет с T одним общим ребром больше, чем T_0. Рассуждая аналогично, мы докажем, что $f(T_0) = f(T_0') = f(T)$.

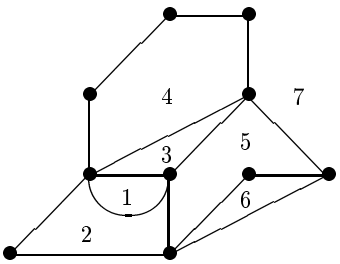
Во второй половине XIX века в Англии математиками Ф.Гутри, А.Де Морганом и А.Кэли была поставлена задача о возможности раскраски произвольного многоугольного графа на плоскости при помощи четырех красок так, что соседние страны имеют различный цвет. Следующий пример показывает, что 3-х красок может быть недостаточно



где К, Б, З, С – начальные буквы соответственного красного, белого, зеленого и синего цветов. В 1892 г. английский математик Хивуд доказал, что любую карту можно раскрасить пятью красками (см. теорему ниже). В 1976 г. американские математики К.Аппель и В.Хакен с помощью ЭВМ установили положительное решение данной проблемы.

Сначала уточним понятие многоугольного графа $G(V, E)$. Это конечный плоский связный граф, в котором ни один многоугольник не лежит внутри другого. Граничные ребра многоугольника образуют цикл, внутренняя часть которого называется грань графа. Цикл графа, окружающий весь граф, называется максимальным, а его внешняя часть называется бесконечной гранью (F_∞).

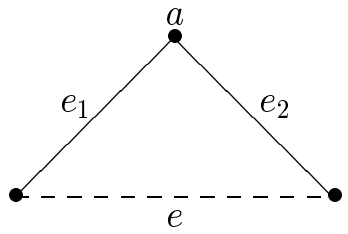
Пример (многоугольного графа).



Теорема 7(Хивуд).*Каждый многоугольный граф $G = (V, E)$ можно раскрасить пятью красками.*

Замечание 1. Можно считать, что граф G не содержит вершин степени два.

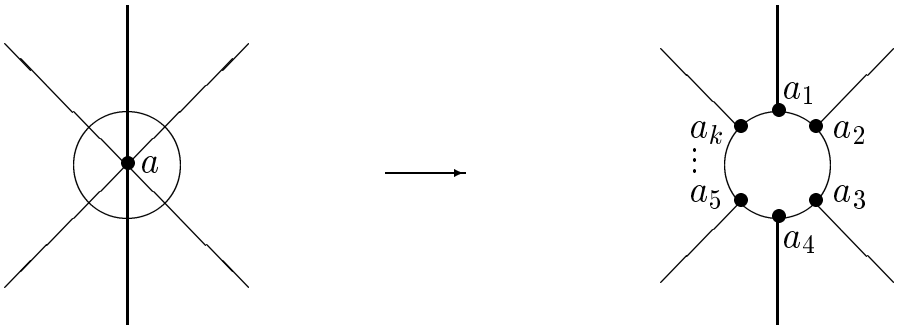
ДОКАЗАТЕЛЬСТВО. Действительно, если существует такая вершина $a \in V$, что $\rho(a) = 2$



то, удаляя эту вершину и объединяя инцидентные с ней два ребра e_1, e_2 в одно ребро e, мы получим многоугольный граф G'. Раскрашивание графа G' пятью красками влечет за собой искомое раскрашивание графов G.

Замечание 2. В силу замечания 1 степень каждой вершины графа G не меньше 3. Оказывается, мы можем свести нашу задачу к однородным графам степени 3.

ДОКАЗАТЕЛЬСТВО. Действительно, если существует вершина $a \in V$ такая, что $\rho(a) \geq 4$, то проведя достаточно малую окружность с центром в точке a и удаляя вершину a с частями ребер, лежащими внутри этой окружности, мы получим новый граф G', в котором вместо вершины a появились вершины $a_1, \ldots, a_k (k \geq 4)$ степени 3 (см. рис.)



Раскрашивание графа G' пятью красками влечет за собой очевидное искомое раскрашивание графа G.

Замечание 3. Итак, мы можем считать, что $G = (V, E)$ – это связный плоский (конечный) однородный степени 3 граф.

Докажем, что он содержит грань, ограниченную не более 5 ребрами. Рассмотрим равенства: $2 + p = b + r$ (формула Эйлера), $3b = 2\varphi_2 + 3\varphi_3 + 4\varphi_4 + \ldots$, где φ_k – число граней с k ребрами и k вершинами. Выразим число ребер p и число граней через $\varphi_2, \varphi_3, \ldots$ следующим образом:

$$2p = 2\varphi_2 + 3\varphi_3 + 4\varphi_4 + \ldots,$$

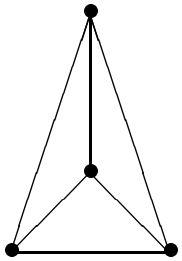
$$r = \varphi_2 + \varphi_3 + \varphi_4 + \dots .$$

Подставив выражения r, p, b через $\varphi_2, \varphi_3, \dots$ в формулу Эйлера, имеем

$$12 = 4\varphi_2 + 3\varphi_3 + 2\varphi_4 + \varphi_5 - \varphi_7 - 2\varphi_8 - \dots .$$

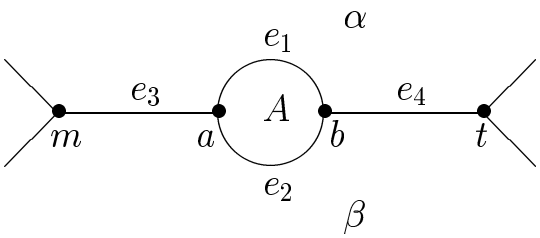
Следовательно, одно из чисел $\varphi_2, \varphi_3, \varphi_4, \varphi_5$ больше нуля.

ДОКАЗАТЕЛЬСТВО теоремы. Минимально возможное число граней для однородного графа степени 3 равно 4

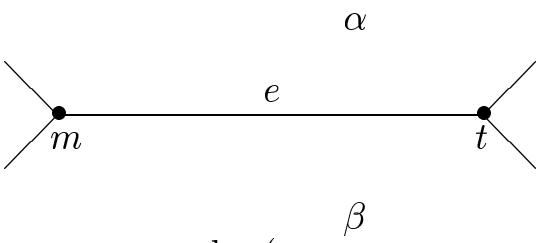


и, следовательно, для такого графа теорема справедлива. Предположим, что теорема верна для графов с числом граней, меньшим числа $|E(G)|$.

Случай 1. Граф G содержит кратные ребра, т.е. $\varphi_2 \geq 1$:

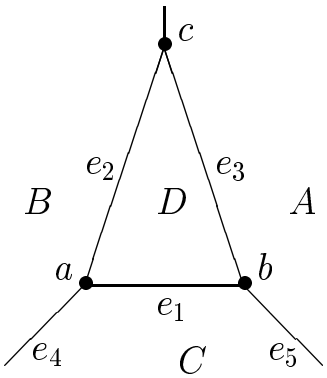


Исключив вершины a, b и ребро e_1, а ребра e_3, e_2, e_4 заменив на единственное ребро e (см. рис.), мы получим новый граф:



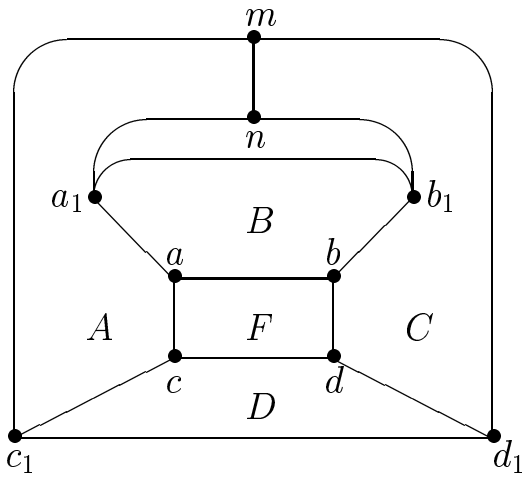
Ясно, что раскраска нового графа (а она существует по предположению индукции) влечет искомую раскраску графа G.

Случай 2. $\varphi_2 = 0,\ \varphi_3 \geq 1$. Т.е. граф G не содержит кратных ребер, но содержит треугольную грань:



Удаляя из G_1 ребро e_1, вершины a и b, а также "склеивая" ребра e_2, e_4 в ребро e', а ребра e_3, e_5 в ребро e'', мы придем к новому (однородному степени 3) графу G' с меньшим числом граней. Из раскраски G', очевидно, следует искомая раскраска графа G.

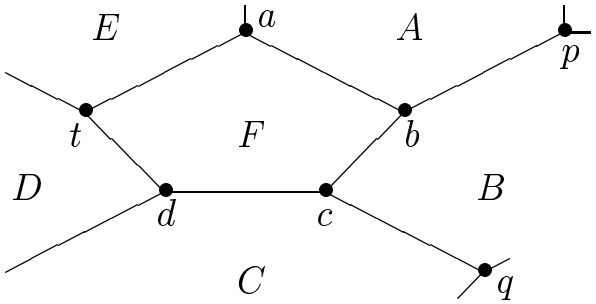
Случай 3. $\varphi_2 = \varphi_3 = 0,\ \varphi_4 \geq 1$. Т.е. граф G содержит четырехугольную грань, но не содержит кратных ребер и треугольных граней:



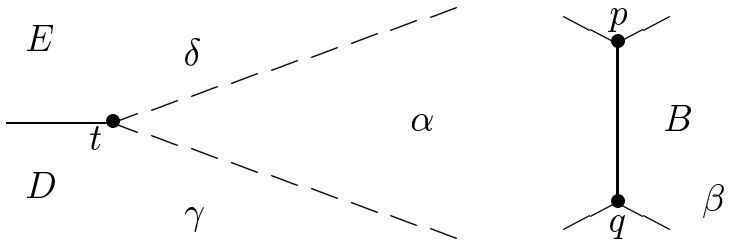
При этом можно считать, что грани B и D не являются частями одной грани и не граничат друг с другом. Исключим ребра $\{a, b\}, \{c, d\}$, объединим $\{a_1, a\}$, $\{c, c_1\}$ и $\{a, c\}$ в одно ребро $\{a_1, c_1\}$, а ребра $\{b_1, b\}$, $\{b, d\}$, $\{d, d_1\}$ в ребро $\{b_1, d_1\}$. Мы получим однородный (степени 3) граф G_1 с меньшим числом граней. По предположению индукции, для него существует искомая раскраска. Пусть, например, грани A и C раскрашены в цвета α и β, а грань $B + F + D$ в цвет γ. Возвращаясь к графу G, мы грани B и D оставляем окрашенными в цвет γ, а грань F закрашиваем в 4-й цвет δ.

Случай 4. $\varphi_2 = \varphi_3 = \varphi_4 = 0,\ \varphi_5 \geq 1$.

Рассмотрим фрагмент графа G



Можно считать, что грани A и C не являются частями одной и той же грани и не имеют общей границы. Исключим ребра $\{a,b\},\{c,d\}$:



По предположению индукции, новый граф можно раскрасить в 5 цветов: $\alpha,\beta,\gamma,\delta,\mu$. Пусть, например, грани B, D, E и $(A+F+C)$ раскрашены соответственно $\beta,\gamma,\delta,\alpha$ цветами. Восстанавливая граф G, мы оставляем раскраску прежней, кроме грани F, которую закрашиваем в цвет μ. Теорема доказана.

Задача 32. Пусть G – многоугольный однородный степени 4 граф. Тогда G содержит либо 4 двухкратных ребра, либо треугольную грань.

УКАЗАНИЕ. Имеем

$$4b=\sum_{n\geq 2} n\varphi_n,\ 2p=\sum_{n\geq 2} n\varphi_n,\ b+r=2+p,\ r=\sum_{n\geq 2}\varphi_n.$$

Откуда следует, что $4b+4r=\sum\limits_{n\geq 2}(n+4)\varphi_n=8+\sum\limits_{n\geq 2}2n\cdot\varphi_n$,
$8=2\varphi_2+\varphi_3-\varphi_5-2\varphi_6-\ldots$. Если $\varphi_3=0$, то $\varphi_2\geq 4$.

Задача 33. Исследовать возможные значения $\varphi_2,\varphi_3,\varphi_4$ для многоугольного однородного степени 5 графа.

Задача 34. Пусть G – планарный конечный граф. Число $\chi(G)=(b-p)$ называется эйлеровой характеристикой графа G. Доказать, что

а) если G – связный граф, то $\chi(G) \leq 1$;

б) если G – связный граф, то $\chi(G) = 1$ тогда и только тогда, когда G – дерево;

в) если G – лес, то число деревьев в нем равно $\chi(G)$.

Задача 35 (алгоритм выбора экономичного дерева в связном графе).

Пусть $G = (V, E)$ – конечный связный граф и $f : E \to \mathbf{R}^+$. Выберем любую вершину $x_1 \in V$ и выберем вершину x_2, инцидентную x_1, имеющую минимальное значение $f(\{x_1, x_2\})$. Затем выберем x_3, инцидентную одной из вершин x_1, x_2 и имеющую с ними самое "дешевое" ребро. Пусть мы выбрали вершины $x_1, \ldots, x_k$. Выберем среди вершин, инцидентных указанным, вершину $x_{k+1} \notin \{x_1, \ldots, x_k\}$, имеющую самое "дешевое" ребро $\{x_{k+1}, x_i\}, i \leq k$. Наш алгоритм останавливается на $(n-1)$ шаге. Проверить, что в результате мы действительно получаем экономичное дерево.

УКАЗАНИЕ. Воспользоваться доказательством теоремы Краскаля.

2.7 Теорема о целочисленности. Потоки в сетях. Теорема о максимальном потоке и минимальном разрезе

В пункте 1.4 была доказана теорема Ф.Холла о представителях. Некоторые авторы называют ее задачей о свадьбах и дают ей следующую интерпретацию. Имеется некоторое количество юношей $\{ю_1, \ldots, ю_n\}$ и девушек $\{д_1, \ldots, д_m\}$. Каждый юноша знаком с несколькими девушками. Найти необходимые и достаточные условия, чтобы каждого юношу можно было женить на знакомой ему девушке (см. [21]).

Запишем условие задачи в виде двудольного графа $G(V_1, V_2)$, взяв в качестве $V_1 = \{ю_1, \ldots, ю_n\}$, а в качестве $V_2 = \{д_1, \ldots, д_n\}$ и соединив ребром вершину $ю_i$ с вершиной $д_j$ тогда и только тогда, когда они знакомы. Инъективное отображение V_1 в V_2 называется совершенным паросочетанием, если соответствующие вершины (всегда) соединены ребром.

Итак, на языке теории графов задача о свадьбах звучит следующим

образом: найти необходимое и достаточное условие на двудольный граф $G = (V_1, V_2)$ для того, чтобы в нем существовало совершенное паросочетание.

Приведем доказанную ранее теорему Ф.Холла в терминах теории графов.

Теорема 8 (Ф.Холл, 1935). *Пусть $G = G(V_1, V_2)$ – конечный двудольный граф и для любого подмножества $A \subseteq V_1$ через $\varphi(A)$ обозначим множество вершин из V_2, которые смежны хотя бы одной вершине из A. Совершенное паросочетание в G существует тогда и только тогда, когда для любого подмножества $A \subseteq V_1$*

$$|A| \leq |\varphi(A)|.$$

Задача 36 (задача о гареме). Обозначим через Ю некоторое множество юношей и предположим, что каждый юноша из Ю желает взять в жены более чем одну знакомую ему девушку. Найти необходимые и достаточные условия разрешимости этой задачи.

УКАЗАНИЕ. Пусть Ю=$\{$ю$_1, \ldots,$ ю$_n\}$ и Д=$\{$ д$_1, \ldots,$ д$_m\}$. Предположим, что гарем ю$_1$ должен состоять из трех девушек, а гаремы ю$_2, \ldots,$ ю$_n$ из двух девушек. Рассмотрим новое множество юношей

$$\text{Ю}' = \{\ \text{ю}_{11},\ \text{ю}_{12},\ \text{ю}_{13},\ \text{ю}_{21},\ \text{ю}_{22},\ \text{ю}_{31},\ \text{ю}_{32}, \ldots,\ \text{ю}_{n1},\ \text{ю}_{n2}\}.$$

Остается применить к Ю$'$ теорему Холла.

Если $S_1, \ldots, S_m$ – непустые подмножества E, то трансверсалью этого семейства подмножеств $F = (S_1, \ldots, S_m)$ называется такое подмножество $\{e_1, \ldots, e_m\} \subseteq E$, что $e_i \in S_i, i \leq m$. Другими словами, это система различных представителей наших подмножеств. Теорема Холла утверждает, что трансверсаль семейства F существует тогда и только тогда, когда $|S_{i_1} \cup \cdots \cup S_{i_k}| \geq k$ для любой выборки $\{i_1, \ldots, i_k\} \subseteq \{1, 2, \ldots, m\}$. Трансверсаль произвольного подсемейства F называется частичной трансверсалью F.

Задача 37. Пусть $S_1, \ldots, S_m \subseteq E, S_i \neq \phi, i \leq m$, и $F = (S_1, \ldots, S_m)$.

Семейство F имеет трансверсаль мощности t тогда и только тогда, когда для любой выборки $\{i_1, \ldots, i_k\} \subseteq \{1, 2, \ldots, m\}$, $|S_{i_1} \cup \cdots \cup S_{i_k}| \geq k + t - m$.

УКАЗАНИЕ. Рассмотрим новое семейство $F' = (S_1 \cup D, S_2 \cup D, \ldots, S_m \cup D)$, где D – любое $(m-t)$ – элементное множество, не пересекающееся с E. F имеет частичную трансверсаль мощности t тогда и только тогда, когда F' имеет трансверсаль. По теореме Холла это возможно тогда и только тогда, когда

$$|S_{i_1} \cup \cdots \cup S_{i_k} \cup D| \geq k,$$

$$|S_{i_1} \cup \cdots \cup S_{i_k}| \geq k - |D| = k + t - m,$$

так как $(S_{i_1} \cup \cdots \cup S_{i_k}) \cap D = \phi$.

Задача 38. Какие из следующих семейств подмножеств множества $E = \{1, 2, 3, 4, 5\}$ имеют трансверсали:

1) $(\{1\}, \quad \{2, 3\}, \quad \{1, 2\}, \quad \{1, 3\}, \quad \{1, 4, 5\})$;

2) $(\{1, 2\}, \quad \{2, 3\}, \quad \{4, 5\}, \quad \{4, 5\})$;

3) $(\{1, 3, 4\}, \quad \{1, 4, 5\}, \quad \{2, 3, 5\}, \quad \{2, 4, 5\})$?

Задача 39. Пусть E – множество букв в слове MATROIDS. Найти трансверсали семейства

$$(STAR, ROAD, MOAT, RIOT, RIDS, DAMS, MIST).$$

Пусть $M = (m_{ij})$ – матрица порядка $m \times n$, где $1 \leq m \leq n$
и $1 \leq m_{ij} \leq n$. Если выполнено условие, что все элементы в каждой строке и в каждом столбце различны, то M называется латинским $(m \times n)$ – прямоугольником. Если $m = n$, то латинский прямоугольник называется латинским квадратом.

Примеры: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{pmatrix}$.

Теорема 9. *Пусть M – латинский $(m \times n)$ – прямоугольник и $m \leq n-1$.*

Тогда M можно расширить до латинского квадрата добавлением новых $(n-m)$ строк.

Доказательство следует из леммы.

Лемма. *Латинский $(m \times n)$ – прямоугольник можно расширить до латинского $(m+1) \times n$ – прямоугольника.*

ДОКАЗАТЕЛЬСТВО. Пусть $E = \{1, 2, \ldots, n\}$ и $F = (S_1, \ldots, S_n)$, где S_i – множество элементов E, не встречаючихся в i-м столбце M, $i = 1, 2, \ldots, n$. Докажем, что F имеет трансверсаль. Предположим, что $|S_{i_1} \cup \cdots \cup S_{i_k}| \leq k-1$ для некоторой выборки $\{i_1, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$. Т.к. в $S_{i_1} \cup \cdots \cup S_{i_k}$ присутствует $(n-m) \cdot k$ элементов (включая повторения), то некоторый элемент повторялся бы более чем $(n-m)$ раз. Противоречие.

Задача 40. Докажите, что существует по крайней мере

$$n!(n-1)! \ldots 2!1!$$

латинских $(n \times n)$ – квадратов.

Задача 41. Показать, что таблицу умножения в конечной группе можно рассматривать как латинский квадрат. Существует ли латинский квадрат, который нельзя получить таким способом?

УКАЗАНИЕ. Пусть p – простое число. Число латинских квадратов порядка $p \times p$ не меньше числа $p!(p-1)! \ldots 1!$, а число групп порядка p в точности равно 1.

Рассмотрим, далее, конечный связный граф $G = (V, E)$ и пусть v, w – различные его вершины.

Определение 1. Простые цепи, соединяющие v с w и не имеющие общих ребер, называются реберно непересекающимися.

Определение 2. Простые цепи, соединяющие v с w и не имеющие общих вершин (кроме v и w), называются вершино непересекающимися.

Определение 3. Множество ребер A графа G называется vw-разделяющим в G, если любая простая цепь из v в w содержит ребро из A.

Определение 4. Множество вершин B графа G называется vw-отделя-

ющим, если $v \notin B, w \notin B$ и любая простая цепь из v в w обязательно содержит вершину из B.

Теорема 10 (Менгер, Форд, Фалкерсон; 1955). *Пусть $G = (V, E)$ – связный конечный граф и v, w – различные его вершины. Тогда максимальное число реберно непересекающихся простых цепей, соединяющих v с w, равно минимальному числу k ребер в vw-разделяющем множестве.*

Укажем схему доказательства. Ясно, что число всех непересекающихся простых цепей, соединяющих v с w, не превосходит k. Чтобы доказать равенство этих чисел, можно воспользоваться методом математической индукции по числу ребер $n = |V|$. Предположим, что теорема верна для графов с числом ребер $< n$. Доказательство теоремы следует из рассмотрения двух случаев ([21]):

Случай 1. vw-разделяющее множество A минимальной мощности k содержит ребро, не инцидентное v, а также ребро, не инцидентное w.

Случай 2. Каждое vw – разделяющее множество минимальной мощности k состоит из ребер, каждое из которых инцидентно v, либо из ребер, каждое из которых инцидентно w.

Пользуясь аналогичной схемой, можно доказать следующую теорему.

Теорема 11 (Менгер, 1927). *Максимальное число вершинно непересекающихся простых цепей, соединяющих две различные несмежные вершины v, w связного конечного графа, равно минимальному числу вершин в vw-отделяющем множестве.*

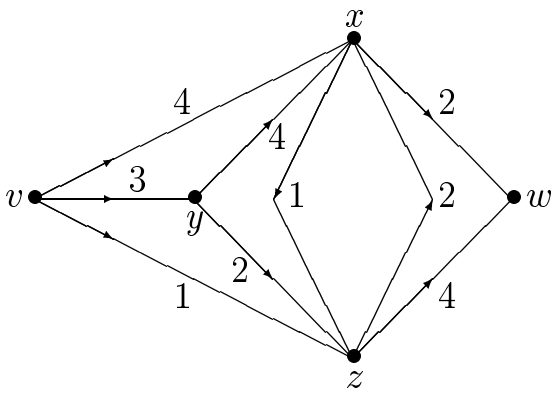
Рассматривая конечные связные ориентированные графы (орграфы) и дублируя соответствующую терминологию, мы можем сформулировать (без доказательства) следующий результат (см. [21]).

Теорема 12 (теорема о целочисленности).

Максимальное число непересекающихся по дугам простых орцепей, соединяющих две различные вершины v и w орграфа, равно минимальному числу дуг vw-разделяющего множества.

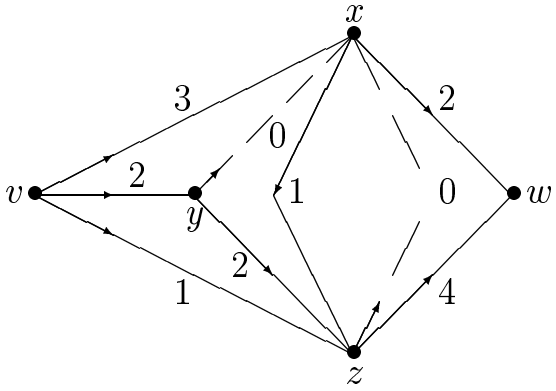
Определение. Сеть – это пара $N = (D, \psi)$ где D – орграф, а ψ – функция, отображающая множество дуг D в $\mathbf{R}^+ \cup \{0\}$. Для каждой дуги e значение $\psi(e)$ называется ее пропускной способностью. Для каждой вершины x положим $\overleftarrow{\rho}(x) = \sum\limits_z \psi((x,z))$ (и назовем полустепенью исхода вершины x), $\overrightarrow{\rho}(x) = \sum\limits_z((z,x))$ (и назовем полустепенью захода вершины x).

Пример.



Здесь $\psi((y,x)) = 4$, $\overrightarrow{\rho}(x) = 10$, $\overleftarrow{\rho}(z) = 6$. Будем считать, что орграф D содержит один источник v и один сток w. Приведем пример иллюстрирующий понятие сети на практике. Предположим, что завод-изготовитель (v) отправляет на рынок (w) свою продукцию, используя различные каналы. Каждый канал имеет максимальную пропускную способность (например, на рис. $\psi((v,x)) = 4$). Вопрос: как максимизировать отправку готовой продукции?

Для вышеприведенного примера ответом является следующий алгоритм:



Определение. Пусть $N = (D, \Psi)$ – сеть. Функция φ, ставящая в со-

ответствие каждой дуге a из D неотрицательное число $\varphi(a)$ (называемое потоком через a), называется потоком через N, если:
1) $\varphi(a) \leq \Psi(a)$;
2) по отношению к сети (D, φ) полустепень исхода и полустепень захода любой вершины $(\neq v, w)$ равны между собой, т.е. полный поток, входящий в любую вершину $(\neq v, w)$, равен полному потоку, выходящему из нее, и поток через дугу не превосходит ее пропускной способности.

Разрезом сети $N = (D, \Psi)$ называется множество дуг A орграфа D такое, что любая простая орцепь из v в w содержит дугу из A, т.е. разрез N – это vw-разделяющее множество в D. Сумма пропускных способностей всех дуг разреза называется пропускной способностью разреза. Минимальным разрезом называется разрез, обладающий наименьшей возможной пропускной способностью. Следующая теорема эквивалентна теореме 12.

Теорема 13 (о максимальном потоке и минимальном разрезе). *Во всякой сети величина любого максимальноого потока равна пропускной способности любого минимальноого разреза.*

Замечание. Теорема 13 доказана в 1955 г. Л.Фордом и Д.Фалкерсоном (см. "Потоки в сетях". – М.: Мир, 1966).

Глава 3

ТЕОРИЯ КОДИРОВАНИЯ

3.1 Основные определения. Примеры кодов

Рассмотрим множество $A = \{a_1, \ldots, a_n\}$, состоящее из n элементов. Множество A назовем алфавитом объема n, а его элементы будем называть символами или буквами алфавита. Например, русские буквы образуют алфавит объема 33, а латинские буквы составляют алфавит объема 27. Последовательность из букв алфавита A длины $m \quad a_{i_1} \ldots a_{i_m}$ назовем словом длины m.

Определение [12]. Любое непустое множество слов, записанное в алфавите A, называется кодом в этом алфавите. Мощность этого множества называется объемом кода, а его элементы называются кодовыми словами. Код называется равномерным, если его кодовые слова имеют одинаковую длину m (m называется длиной равномерного кода).

Упражнение. Доказать, что объем равномерного кода длины m не превосходит $n^m = 2^{mlog_2 n}$.

Пусть $X = \{x_1, \ldots, x_e\}$ – конечное множество. Скажем, что X является дискретным ансамблем сообщений, если на X задано распределение вероятностей $p(x)$, т.е. каждому элементу $x_i \in X, \qquad i \leq e$, сопоставлено число $p(x_i)$. При этом $p(x_i) \geq 0, i = \overline{1, e}$ и $\sum\limits_{i=1}^{e} p(x_i) = 1$. Каждому подмножеству

$Y \subseteq X$ сопоставим вероятность (число)

$$P(Y) = \sum_{x \in Y} p(x).$$

Определение [12]. Произвольное отображение

$$\varphi : X \to K$$

дикретного ансамбля X в код K алфавита A называется кодированием X.

Пример 1 [12]. Предположим, что на телеграфе имеется автоматическая обработка телеграмм, с объемом запоминающегося устройства, равным N двоичным ячейкам. Рассмотрим 2 способа кодирования телеграмм: побуквенное и кодирование целых слов. В первом случае каждой букве русского алфавита (будем отождествлять буквы ь, ъ) ставится в соответствие слово длины 5 в алфавите $\{0, 1\}$, равное номеру этой буквы в русском алфавите, который записывается в двоичной системе счисления. Например, а $\to (00001)$, б $\to (00010)$, в $\to (00011)$, г $\to (00100)$. Мы получаем однородное кодирование. Если допустить, что каждая телеграмма в среднем содержит 20 слов, а средняя длина слова 5 букв, то в запоминающее устройство можно записать $N/500$ телеграмм.

Во втором случае можно составить словарь из $2^{13} = 8192$ слов, которые обычно используются при составлении телеграмм. Каждому такому слову в русском языке можно поставить в соответствие слово длины 13 в алфавите $\{0, 1\}$. Ясно, что в запоминающее устройство можно записать $N/260$ телеграмм (т.е. объем памяти запоминающего устройства при втором кодировании почти в два раза больше).

Определение [12]. Код называется декодируемым (или префиксным), если ни одно кодовое слово не совпадает с началом другого кодового слова.

Например, равномерный код декодируемый.

Замечание. Существуют непрефиксные коды, допускающие однозначное разделение последовательности букв на кодовые слова.

Рассмотрим несколько примеров кодирования слов русского языка.

Способ 1 (подстановочный шифр). Отождествим буквы е и ё, а также ь и ъ. Тогда мы получим алфавит, состоящий из 31 буквы. Если в романе Л.Н.Толстого "Война и мир" подсчитать частоту вхождения каждой буквы, то получится следующая таблица

N	Буква	Относительная частота	N	Буква	Относительная частота
1	а	0,062	18	с	0,045
2	б	0,014	19	т	0,053
3	в	0,038	20	у	0,021
4	г	0,013	21	ф	0,002
5	д	0,025	22	х	0,009
6	е,ё	0,072	23	ц	0,004
7	ж	0,007	24	ч	0,012
8	з	0,016	25	ш	0,006
9	и	0,062	26	щ	0,003
10	й	0,010	27	ы	0,016
11	к	0,028	28	ь,ъ	0,014
12	л	0,035	29	э	0,003
13	м	0,026	30	ю	0,006
14	н	0,053	31	я	0,018
15	о	0,090			
16	п	0,023			
17	р	0,040			

Из таблицы следует, что буква "о" наиболее встречаемая в русском тексте (достаточно большой длины). Это можно учитывать, например, при игре в "Поле чудес". Заметим также, что промежуток между словами имеет относительную частоту 0,175. Если рассмотреть инъективное отображение русского алфавита (с дополнительным символом, означающим промежуток между словами) в произвольное множество мощности ≥ 32, а затем подставить в текст вместо каждой буквы его образ в этом множестве, то

мы получим подстановочную криптограмму, расшифровать которую легко, исходя из нашей таблицы, если текст достаточно большой. Примером такого шифра является так называемый шифр Цезаря. Он состоит в следующей кодировке букв алфавита: а $\to$ я, б $\to$ а, в $\to$ б и т.д., т.е. вместо каждой буквы подставляем предшествующую ей в русском алфавите.

Упражнение. Закодировать шифром Цезаря фразу "математика ум в порядок приводит" (Ответ: лясдлясзйл тл б онпюгнй опзбнгзс).

Для расшифровки текста, закодированного шифром Цезаря, применяется "метод полосок". Каждая полоска состоит из выписанных вертикально (подряд) букв русского алфавита. Далее, для расшифровки слова "лясдлясзйл" в нашем упражнении берутся десять полосок и прикладываются друг к другу так, чтобы получить это слово. Ниже этого слова будет стоять ответ. Под шифром Цезаря понимается сдвиг алфавита не только на 1 букву назад, а на произвольное фиксированное число букв вниз или вверх. Например, следующая кодировка тоже называется шифром Цезаря: а $\to$ г, б $\to$ д, в $\to$ у, ... , ю $\to$ б, я $\to$ в, т.е образом каждой буквы является третья снизу от неё.

Способ 2 (перестановочный шифр). Данный способ предложен в работе Л.С.Хилла ("Concerning certain linear transformation apparatas of cryptography," Amer. Math. Monthly, v.38, 1931, p.135-154; см. также [27]).

Предположим, что нам необходимо зашифровать сообщение

"встреча состоится через неделю". (3.1)

Поставим в соответствие каждой букве её номер в алфавите, а промежутку между словами число 32. Тогда нашему сообщению соответствует последовательность чисел

$$3, 18, 19, 17, 6, 24, 1, 32, 18, 15, 18, 19, 15, 9, 19,$$
$$18, 31, 32, 24, 6, 17, 6, 8, 32, 14, 6, 5, 6, 12, 30. \quad (3.2)$$

Рассмотрим эту последовательность в кольце Z_{32}. Возьмем в этом кольце

произвольный обратимый элемент, например, $\bar{3} \in Z_{32}(\bar{3} \cdot \bar{1}1 = \bar{1})$. Умножим каждый член этой последовательности на 3:

$$9, 22, 25, 19, 18, 8, 3, 32, 22, 13, 22, 25, 13, 27, 25,$$
$$22, 29, 32, 8, 18, 19, 18, 24, 32, 10, 18, 15, 18, 4, 26. \tag{3.3}$$

Таким образом, наше сообщение кодируется в виде

$$\text{ихштсзв хмхшмышхэ зстсч йсосгщ} \tag{3.4}$$

Чтобы расшифровать сообщение (3.4), необходимо переписать его в виде (3.3), а затем умножить последовательность (3.3) на $\bar{1}1 = \bar{3}^{-1}$ (в кольце Z_{32}). Мы придем к последовательности (3.2). Подставляя вместо чисел соответствующие буквы, мы восстановим наш текст.

Усложним вышеприведенный метод, используя невырожденные матрицы над кольцом Z_{32}. Разобьем последовательность (3.2) на пары:

$$\begin{pmatrix} 3 \\ 18 \end{pmatrix}, \begin{pmatrix} 19 \\ 17 \end{pmatrix}, \begin{pmatrix} 6 \\ 24 \end{pmatrix}, \begin{pmatrix} 1 \\ 32 \end{pmatrix}, \begin{pmatrix} 18 \\ 15 \end{pmatrix}, \begin{pmatrix} 18 \\ 19 \end{pmatrix}, \begin{pmatrix} 15 \\ 9 \end{pmatrix}, \begin{pmatrix} 19 \\ 18 \end{pmatrix},$$
$$\begin{pmatrix} 31 \\ 32 \end{pmatrix}, \begin{pmatrix} 24 \\ 6 \end{pmatrix}, \begin{pmatrix} 17 \\ 6 \end{pmatrix}, \begin{pmatrix} 8 \\ 32 \end{pmatrix}, \begin{pmatrix} 14 \\ 6 \end{pmatrix}, \begin{pmatrix} 5 \\ 6 \end{pmatrix}, \begin{pmatrix} 12 \\ 30 \end{pmatrix}.$$

Умножим данные столбцы на матрицу $A = \begin{pmatrix} 2 & 7 \\ -3 & 6 \end{pmatrix} \in M_2(Z_{32})$, для которой существует обратная $A^{-1} = \begin{pmatrix} 6 & -7 \\ 3 & 2 \end{pmatrix} \in M_2(Z_{32})$.

Получим новую последовательность из столбцов

$$\begin{pmatrix} 4 \\ 3 \end{pmatrix}, \begin{pmatrix} -3 \\ 13 \end{pmatrix}, \begin{pmatrix} 20 \\ 30 \end{pmatrix}, \begin{pmatrix} 2 \\ -3 \end{pmatrix}, \begin{pmatrix} 13 \\ 4 \end{pmatrix}, \begin{pmatrix} 9 \\ 28 \end{pmatrix}, \begin{pmatrix} 15 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 19 \end{pmatrix},$$
$$\begin{pmatrix} -2 \\ 3 \end{pmatrix}, \begin{pmatrix} 26 \\ -4 \end{pmatrix}, \begin{pmatrix} 12 \\ -15 \end{pmatrix}, \begin{pmatrix} 16 \\ 14 \end{pmatrix}, \begin{pmatrix} 6 \\ 26 \end{pmatrix}, \begin{pmatrix} 20 \\ 21 \end{pmatrix}, \begin{pmatrix} 10 \\ 16 \end{pmatrix}. \tag{3.5}$$

Возвращаясь к буквам, мы получим следующую закодированную информацию

$$\text{гвэмуюбэмгиьовгтювщьлрпнещуфйп} \tag{3.6}$$

Чтобы её расшифровать, надо знать матрицу A. Действительно, так как порядок A равен 2×2, то подставляя в (3.6) вместо букв их номера в алфавите и разбивая полученные числа на пары, мы получим стоблцы (3.5). Умножая эту последовательность столбцов на A^{-1} (слева), мы восстановим наш текст.

Мы можем усложнить данный метод, разбив нашу исходную последовательность чисел (номеров) на 6 столбцов

$$\begin{pmatrix} 3 \\ 18 \\ 19 \\ 17 \\ 6 \end{pmatrix}, \quad \begin{pmatrix} 24 \\ 1 \\ 32 \\ 18 \\ 15 \end{pmatrix}, \quad \begin{pmatrix} 18 \\ 19 \\ 15 \\ 9 \\ 19 \end{pmatrix}, \quad \begin{pmatrix} 18 \\ 31 \\ 32 \\ 24 \\ 6 \end{pmatrix}, \quad \begin{pmatrix} 17 \\ 6 \\ 8 \\ 32 \\ 14 \end{pmatrix}, \quad \begin{pmatrix} 6 \\ 5 \\ 6 \\ 12 \\ 30 \end{pmatrix},$$

а затем умножить слева на фиксированную обратимую матрицу из кольца $M_5(Z_{32})$. Например, можно взять матрицу

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \qquad A^{-1} = \begin{pmatrix} 1 & 31 & 0 & 0 & 0 \\ 0 & 1 & 31 & 0 & 0 \\ 0 & 0 & 1 & 31 & 0 \\ 0 & 0 & 0 & 1 & 31 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Итак, для кодирования этим методом достаточно знать "ключевую" обратимую матрицу в кольце $M_n(Z_{32})$, а количество букв и промежутков в тексте должно делиться на n.

Замечание. Известный пример "казнить нельзя помиловать" показывает, что для более точного восприятия текста на русском языке необходимо ввести некоторые символы для точки и запятой. В этом случае мы будем работать над кольцом Z_{34}.

Способ 3 (перестановочный код). Как отмечено в книге [27], нижеследующий код был предложен в 1976 г. A.Shamir, L.Adleman, R.Rivest.

Рассмотрим естественную нумерацию букв русского алфавита:

а	б	в	...	ю	я	(интервал)
01	02	03	...	30	31	00,

записывая каждый номер в виде пары цифр и обозначая интервал между словами парой 00. Предположим, что нам необходимо закодировать слово "наступать". Перепишем его, подставляя вместо букв их номера

$$140118192016011926. \tag{3.7}$$

В исходном слове 9 букв. Выберем любое число $r \leq 9$. Например, $r = 2$. Разобьем последовательность (3.7) на блоки, состоящие из 2-х букв

$$1401, \qquad 1819, \qquad 2016, \qquad 0119, \qquad 2600. \tag{3.8}$$

Пусть q – простое число большее любого 4-х значного числа. Выберем целое число s такое, что $(s, \varphi(q)) = 1$. Тогда существует натуральное число t такое, что $st \equiv 1(mod\varphi(q))$. В частности, для любого числа w, взаимно простого с q, имеем $(w^s)^t \equiv w(modq)$. Заменим каждое из 5 чисел в (3.8) на его s-ю степень (по $modq$) :

$$(1401)^s, (1819)^s, (2016)^s, (0119)^s, (2600)^s \tag{3.9}$$

Мы получили искомую закодированную последовательность. Чтобы ее дешифровать, необходимо каждое число в (3.9) возвести в степень t (по $modq$). Конечно, в основе этого метода лежит теорема Ферма-Эйлера: $a^{\varphi(q)} \equiv 1(modq)$, если $(a, q) = 1$. Вернемся к нашему примеру. Возьмем $r = 1$ и $q = 101$. Тогда $\varphi(q) = 100$ и $s = 3, t = 67$. Имеем

$$
\begin{aligned}
14^3 &\equiv 17 \quad (mod 101)\\
1^3 &\equiv 1 \quad (mod 101)\\
18^3 &\equiv 75 \quad (mod 101)\\
19^3 &\equiv 92 \quad (mod 101)\\
20^3 &\equiv 21 \quad (mod 101)\\
16^3 &\equiv 70 \quad (mod 101)\\
1^3 &\equiv 1 \quad (mod 101)\\
19^3 &\equiv 92 \quad (mod 101)\\
26^3 &\equiv 2 \quad (mod 101)
\end{aligned}
$$

Итак, кодированное сообщение принимает вид 17 01 75 92 21 70 0192 02. К сожалению, здесь мы не можем числа (пары цифр) заменить на буквы. Чтобы расшифровать его, необходимо возвести каждое число в степень 67 (по $mod 101$). Ключом к данному шифру являются числа r, q, s и t.

Упражнение. Закодировать указанным методом слово "код", взяв $r = 1, r = 2$ и $r = 3$.

Способ 4 (перестановочный код). Предположим, что нам необходимо закодировать сообщение "Зельманов – лауреат филдсовской премии". Выберем ключевое слово, состоящее из различных букв и известное только посылавшему текст и адресату. Например, возьмем слово "Пушкин" (его трудно забыть). И рассмотрим таблицу

П	У	Ш	К	И	Н
4	5	6	2	1	3
З	Е	Л	Ь	М	А
Н	О	В	Л	А	У
Р	Е	А	Т	Ф	И
Л	Д	С	О	В	С
К	О	Й	П	Р	Е
М	И	И			

В ней ниже ключевого слова записаны числа, означающие порядок сле-

дования соответствующих букв в алфавите (получилось ключевое шестизначное число). Поставим в соответствие нашему тексту следующую криптограмму:

МАФВРЬЛТОПАУИСЕЗНРЛКМЕОДОИЛВАСЙИ,

записанную по столбцам нашей таблицы в соответствии с их номерами. Для декодирования этой криптограммы достаточно знать либо ключевое слово, либо число 456213.

Упражнение. Декодировать сообщение, пользуясь ключевым словом "ПУШКИН":

РСГЕАДЕЮМЖЧЗЬАНОЛСОПВОДАТРОЛВОЮЬОЗЯЫМСЯВ.

ОТВЕТ: ПОЗДРАВЛЯЮ С НОВЫМ ГОДОМ ЖЕЛАЮ СЧАСТЬЯ ЗДОРОВЬЯ.

Способ 5 (шифр Тритемиуса [1]). Рассмотрим нумерацию букв русского алфавита от 1 до 31. Выберем некоторое ключевое слово, например, "ПУШКИН". Чтобы закодировать некоторый текст, например, "Поздравляю Вас с днем рождения", рассмотрим запись:

ПОЗДРАВЛЯЮВАССДНЕМРОЖДЕНИЯ

ПУШКИНПУШКИНПУШКИНПУШКИНПУ.

Подставив вместо букв числа, получим таблицу:

16	15	8	5	17	1	3	12	31	30	3	1	18
16	20	25	11	9	14	16	20	25	11	9	14	16

18	5	14	6	13	17	15	7	5	6	14	9	31
20	25	11	9	14	16	20	25	11	9	14	16	20

Сложив соответствующие числа в первый и во второй строках (в кольце Z_{31}), получим последовательность чисел 1, 4, 2, 16, 26, 15, 19, 1, 25, 10, 12, 15, 3, 7, 30, 25, 15, 27, 2, 4, 1, 16, 15, 28, 25, 20.

Подставим вместо чисел буквы алфавита. Получим следующий закодированный текст: агбпщоташйловжюшоыбчапоьшу.

Чтобы его расшифровать, надо знать запись ключевого слова (в кольце Z_{31}), перейти от закодированного текста к числовой записи и вычесть из каждого числа (по mod 31) номер соответствующей ключевой буквы.

Способ 6. Рассмотрим произвольное инъективное отображение φ русского алфавита в $N \times N$. Кодирование каждого слова заключается в замене каждой буквы x её образом $\varphi(x)$. Например, пусть отображение φ задано в виде таблицы 6×6:

	1	2	3	4	5	6
1	а	о	н	м	л	к
2	п	б				й
3	р	я	в	щ		и
4	с	ю	ы	г	ш	з
5	т	э	ь	ч	д	ж
6	у	ф	х	ц		е

Тогда слову "университет" соответствует упорядоченный набор пар

((6,1), (1,3), (3,6), (3,3), (6,6), (3,1), (4,1), (3,6), (5,1), (6,6),(5,1)) или число 61 13 36 33 66 31 41 36 51 66 51, по которому однозначно декодируется исходное слово, если, конечно, знать таблицу. Очевидно, что это подстановочный шифр.

Упражнение. Пользуясь вышеприведенной таблицей, расшифровать сообщение

14 11 51 66 14 11 51 36 16 11 64 11 31 36 64 11 13 11 61 16.

ОТВЕТ: математика – царица наук.

Следующим примером может служить т.н. азбука Морзе – подстановочный код, использущый алфавит объема 2 (точка, тире) и применяемый для телеграфных сообщений (придуман Самуэлем Морзе; при передаче точка соответствует кратковременному импульсу тока, тире соответствует длительному импульсу тока).

Задача 1. Сколько существует двоичных слов длины n, не содержащих несколько нулей подряд?

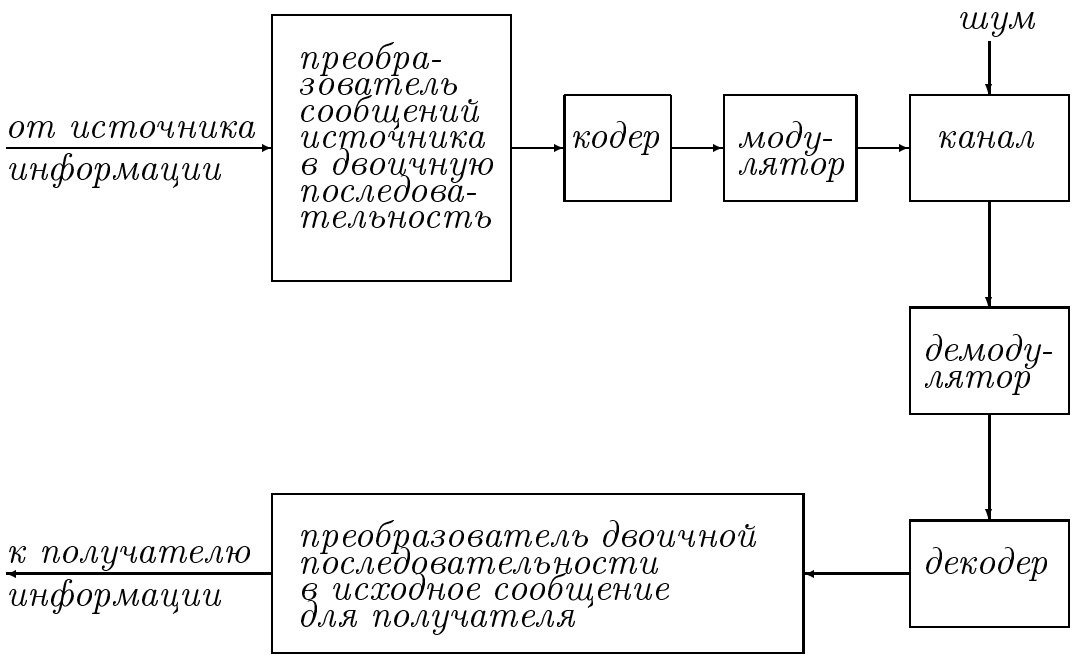
УКАЗАНИЕ. Ясно, что нулей $q = n - t \leq n/2$. Удалив из каждого такого слова по одной единице между любыми соседними нулями, мы получим слово длины $n - (q - 1)$, содержащее ровно q нулей. Это соответствие биективно. Поэтому искомое число равно $C^q_{n-q+1} = C^{n-t}_{t+1}$.

Задача 2. Используя код Цезаря, декодировать криптограмму:

елфиррлм феихоюм зиря носрофв н еиыиуц рсксеюи хцынл фхсволеюфснс е вфосп риди л нгкгося ри тоюол плпсг цшсзлол е фгпцб жоцдя огкцул

3.2 Примеры кодов, исправляющих ошибки

Машинистка, печатая некоторый текст на русском или английском языке, может сделать опечатки. Это обычно не мешает нам восстановить правильный текст. И связано это с избыточностью языка. Например, избыточность английского языка равна 70%([10]). При передаче закодированной информации могут возникать помехи, которые исказят передаваемую информацию. Поэтому необходимо уметь выявлять ошибки при передаче сообщений. Это делается за счет избыточности передаваемой информации. Сначала мы рассмотрим схему (модель) передачи закодированного сообщения



Исходная информация с помощью преобразователя преобразуется в последовательность двоичных символов, затем передается в кодер, где в неё вводится избыточность. Модулятор преобразует передаваемые ему символы в сигналы, которые, в свою очередь, передаются по каналу. В процессе передачи сигналы подвергаются воздействию помех и шумов. Возникают искажения. Демодулятор преобразует искаженные (неискаженные) сигналы в последовательность двоичных символов. Декодер, используя избыточность символов, обнаруживает и исправляет ошибки.

Рассмотрим примеры кодов, обнаруживающих ошибки.

Пример 1. Рассмотрим канал, по которому за время t_0 передается один импульс типа "0" или "1". Вероятность ошибки равна p. Каждый символ a передается по каналу пять раз, т.е. в виде импульсов $aaaaa$. При приеме полученную последовательность разбивают на блоки (по 5 символов в каждом). Если вероятность $C_5^3 p^3(1-p)^2 + C_5^4 p^4(1-p) + p^5$ мала, то блоки, содержащие не более двух 0 (из 5 возможных), декодируются как 11111, а блоки, содержащие не более двух 1, декодируются как 00000. Недостатком этого способа является большой объем времени (передача одного бита информации требует $5 \cdot t_0$ времени).

Задача 1. Пусть передаются по каналу n символов и вероятность ошибки при передаче равна p. Доказать, что вероятность k ошибок равна

$$C_n^k p^k (1-p)^{n-k}.$$

Пример 2. Предположим, что мы имеем C_n^k сообщений. Каждому сообщению поставим в соответствие последовательность длины n из 0 и 1, в которой число 1 равно k. Такое кодирование называется равновесным. Например, закодируем первые 10 чисел (цифр)

$$\begin{aligned}
0 &\rightarrow (000\ 11)\\
1 &\rightarrow (001\ 01)\\
2 &\rightarrow (001\ 10)\\
3 &\rightarrow (010\ 01)\\
4 &\rightarrow (010\ 10)\\
5 &\rightarrow (011\ 00)\\
6 &\rightarrow (100\ 01)\\
7 &\rightarrow (100\ 10)\\
8 &\rightarrow (101\ 00)\\
9 &\rightarrow (110\ 00)
\end{aligned}$$

Здесь $C_5^2 = 10$. Возникновение одной ошибки при передаче такой последовательности приводит к блоку из 5 символов, в котором либо одна 1, либо 3 единицы, т.е. мы обнаруживаем наличие ошибки, не зная, в каком месте она произошла.

Пример 3. Рассмотрим множество сообщений мощности не более 2^n. Каждое сообщение закодировано в виде последовательности из 0 и 1.

$$(a_1, \ldots, a_n).$$

Введем дополнительный символ a_{n+1}, удовлетворяющий условию $a_{n+1} \equiv \equiv \sum\limits_{i=1}^{n} a_i (mod 2)$. Вместо последовательности $(a_1, \ldots, a_n)$ будем передавать последовательность $(a_1, \ldots, a_n, a_{n+1})$. Число единиц в новой последовательности является четным. Если при передаче произошло нечетное число оши-

бок (в частности, одна ошибка), то число единиц в переданной последовательности

$$(a'_1, \ldots, a'_{n+1})$$

является нечетным. Т.е. этим способом "проверки на четность" мы можем обнаружить только существование ошибок, если их число нечетное.

Задача 2. Предположим, что множество сообщений имеет мощность не более 10^4. Поставим в соответствие каждому сообщению α натуральное число $\overline{abcd}$, т.е. $\alpha \to \overline{abcd}$, $a, b, c, d \in \{0, 1, \ldots, 9\}$. Вместо передачи по каналу последовательности $abcd$ будем посылать $abcde$, где $(e + a + b + c + d) \equiv$ $\equiv 0(mod 9)$. Что позволяет обнаружить такое кодирование при передаче?

ОТВЕТ: Мы обнаружим, что либо ошибки нет, либо 0 заменена на 9, либо цифра 9 заменена на 0, либо число ошибок не менее двух.

Пример 4 (R.W.Hamming, 1950). Приведем пример кода, исправляющего одну ошибку в словах длины 7, содержащих 4 бита информации. Именно, предположим, что нам необходимо передать последовательность (a, b, c, d) из нулей и единиц. Рассмотрим вектор

$$C = \begin{pmatrix} x \\ y \\ a \\ z \\ b \\ c \\ d \end{pmatrix},$$

где $x + a + b + d = 0, \qquad y + a + c + d = 0, \qquad z + b + c + d = 0$. Запишем эти условия в матричном виде. Пусть

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix},$$

матрица, в которой $i-$й столбец $\begin{pmatrix} z \\ s \\ t \end{pmatrix}$ имеет такие вхождения r, s, t, что

$$i = r \cdot 2^0 + s \cdot 2^1 + t \cdot 2^2 = (tsr)_2,$$

т.е. это цифры в двоичной записи числа i. Тогда $H \cdot C = 0$. Пусть получатель получает на выходе вектор

$$R = \begin{pmatrix} b_1 \\ \vdots \\ b_7 \end{pmatrix}.$$

Если p – вероятность ошибки при передачи одной цифры, то вероятность того, что при передаче C допущено не более одной ошибки, равна $v = (1-p)^7 + 7(1-p)^6 \cdot p$. Например, если $p = 0,1$, то $v = 0,998$. Если v – вероятность близка к 1, то у нас есть уверенность, что вектор R отличается от C не более, чем на одно вхождение (одну координату). Рассмотрим $E == R - C$. Тогда $HR = HC + HE = HE$. Если $R = C$, то $E = 0$ и $HE = 0$. Если $R \neq C$, то E – вектор-столбец, в котором одна координата равна единице, а остальные равны нулю. В этом случае HE – столбец H, номер i которого в H совпадает с номером координаты, равной 1 в E. Например, если

$$R = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \text{ то } H \cdot R = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix},$$

$$H \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \text{ т.е. } C = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

Упражнение 1.

а) Если $R = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$, то проверить, что $H \cdot R = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$ и $C = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$;

б) если $R = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$, то $HR = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ и $C = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$;

в) если $R = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$, то $H \cdot R = 0$ и $C = R$;

г) декодировать слово (вектор) $\begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$.

Перед изложением нижеследующих примеров 5-7 приведем необходимые сведения из теории коммутативных колец.

3.3 Фактор-кольца коммутативных колец

Пусть R – коммутативное кольцо с единицей и I – идеал кольца R (в обозначении $I \triangleleft R$). Рассмотрим множество смежных классов относительно идеала I :

$$\bar{R} = R/I = \{\bar{a} = a + I; a \in R\}.$$

Определим на $\bar{R}$ операции "$+$" и "$\cdot$" по правилам:

$$\bar{a} + \bar{b} = \overline{a+b}, \qquad \bar{a} \cdot \bar{b} = \overline{ab}.$$

Корректность этих операций следует из определения идеала и следующей леммы.

Лемма 1. $\bar{a} = \bar{b} \Longleftrightarrow (a - b) \in I$.

Доказательство предоставляется читателю.

Кольцо $\bar{R} = R/I$ является ассоциативным, коммутативным и содержит единицу $\bar{1}$. Оно называется фактор-кольцом кольца R по идеалу I. Отображение

$$\pi : R \to R/I, \pi(a) = \bar{a}$$

является сюръективным гомоморфизмом кольца R на R/I (и называется естественным гомоморфизмом R на R/I). Идеал I кольца R назовем мак-

симальным, если для любого другого идеала $M \triangleleft R$ такого, что $I \subseteq M \subseteq R$ следует, что либо $I = M$, либо $M = R$.

Упражнение 1:

а) доказать, что $I \triangleleft \mathbf{Z}$ является максимальным тогда и только тогда, когда $I = (p)$, где p – простое число;

б) кольцо с единицей является полем тогда и только тогда, когда (0) – единственный максимальный идеал в нем.

Предложение 1. *Пусть $I \triangleleft R$. Фактор-кольцо R/I является полем тогда и только тогда, когда I – максимальный идеал.*

ДОКАЗАТЕЛЬСТВО. Пусть R/I – поле и M – идеал, содержащий I. Если $M \neq I$, то $M/I \ni \bar{a} \neq \bar{0}$. Так как R/I – поле, то $\bar{a} \cdot \bar{a}^{-1} = \bar{1} \in M/I$ и для некоторого элемента $m \in M (1 - m) \in I \subseteq M$. Таким образом, $1 \in M$ и, следовательно, для любого элемента $x \in R \qquad x = x \cdot 1 \in M$. Поэтому $R = M$. Обратно, пусть I – максимальный идеал и $\bar{a} \neq 0 \in R/I$. Тогда идеал $(a) + I \neq I$ и, следовательно, $(a) + I = R$. Откуда следует равенство $1 = ax + i$ для некоторых $x \in R, i \in I$. Поэтому $\bar{1} = \bar{a} \cdot \bar{x}$, т.е. R/I – поле.

Предложение 2. *Пусть R – область главных идеалов, т.е. кольцо без делителей нуля с единицей, в котором каждый идеал $I \triangleleft R$ однопорожден, (т.е. $I = (a)$ для некоторого $a \in R$). Если π – неразложимый элемент в R, то (π) – максимальный идеал и $R/(\pi)$ – поле.*

ДОКАЗАТЕЛЬСТВО. Если $M \triangleleft R$ и $M \supset (\pi)$, то $M = (a)$ и $\pi = ax$. Так как $a \notin (\pi)$, то a – обратимый элемент, т.е. $M = R$. По предложению 1 $R/(\pi)$ – поле.

Примерами таких колец (ОГИ) являются $\mathbf{Z}, k[x]$, где k – поле. Если в кольце без делителей нуля имеется алгоритм деления с остатком (такие кольца называются евклидовыми), то они являются областями главных идеалов. Например, $\mathbf{Z}[i], \mathbf{Z}[i\sqrt{2}], \mathbf{Z}[\sqrt{2}]$.

Упражнение 2. Кольцо R называется евклидовой областью, если R –

кольцо делителей нуля с единицей и определено отображение $\varphi : R \to \mathbf{Z}$ такое, что:

а) если $b \neq 0, a \neq 0$ и b/a, то $\varphi(b) \leq \varphi(a)$;

б) для любых элементов $a, b \in R, b \neq 0$ существуют элементы q, $r \in R$ такие, что $a = bq + r$, где $\varphi(r) < \varphi(b)$.

Доказать, что если R – евклидова область, то

1) $\varphi(0) < \varphi(b)$ для любого $b \neq 0 \in R$;

2) $\varphi(a) = \varphi(b)$, если a и b ассоциированы;

3) a и b ассоциированы, если a/b и $\varphi(a) = \varphi(b)$;

4) $\varphi(\varepsilon) = \varphi(1) \Longleftrightarrow \varepsilon | 1$;

5) R – ОГИ;

6) R – область с однозначным разложением на множители.

Упражнение 3. Доказать, что следующие кольца являются евклидовыми:

а) $\mathbf{Z}[i],\ \varphi(a + bi) = a^2 + b^2$;

б) $\mathbf{Z}[\sqrt{2}],\ \varphi(a + b\sqrt{2}) = |a^2 - 2b^2|$;

в) $\mathbf{Z}[i\sqrt{2}],\ \varphi(a + bi\sqrt{2}) = a^2 + 2b^2$;

г) $\mathbf{Z},\ \varphi(n) = |n|$;

д) $k[x],\ \varphi(f(x)) = deg f(x), k$ – поле $(\varphi(0) = -1)$.

3.4 Существование и строение конечных полей

Предложение 3. *Пусть k – поле. Тогда для любого многочлена $f(x) \in k[x]$ существует поле $k_1 \supseteq k$, содержащее некоторый корень этого многочлена.*

ДОКАЗАТЕЛЬСТВО. Пусть $p(x)$ – неприводимый множитель $f(x)$ в $k[x]$. Тогда $k[x]/(p)$ является полем, и $\alpha = \bar{x}$ – корень $f(x) = 0$.

Следствие. *Для любого $f(x) \in k[x]$ существует поле $E \supseteq k$, содержащее все корни $f(x)$.*

ДОКАЗАТЕЛЬСТВО. Действительно, согласно предложению 3, существует поле $k_1 \supseteq k$, содержащее один корень α_1 многочлена $f(x)$. По лемме Безу $(x - \alpha_1)|(f(x)$. Рассмотрим многочлен $f(x)/(x - \alpha_1) \in k_1[x]$. Для него существует поле $k_2 \supseteq k_1$, содержащее его корень α_2. По лемме Безу $(x - \alpha_2)|\frac{f(x)}{(x-\alpha_1}$. Рассматривая $\frac{f(x)}{(x-\alpha_1)(x-\alpha_2)}$ и рассуждая аналогично, придем к доказательству следствия.

Пусть p – простое число и $q = p^n$. Рассмотрим поле $E \supseteq GF(p)$, содержащее все корни $\alpha_1, \ldots, \alpha_q$ многочлена $x^q - x \in GF(p)[x]$. Так как $(x^q - x)' = qx^{q-1} - 1 = -1$, то данный многочлен не имеет кратных корней, т.е. $\alpha_i \neq \alpha_j$ при $i \neq j$. Пусть $GF(q) = \{\alpha_1, \ldots, \alpha_q\}$. Докажем, что $GF(q)$ – подполе E. Действительно, пусть $\alpha, \beta \in GF(q)$. Тогда $(\alpha\beta)^q = \alpha^q \cdot \beta^q = \alpha\beta$ и $(\alpha + \beta)^q = ((\alpha + \beta)^p)^{p^{n-1}} = (\alpha^p + \beta^p)^{p^{n-1}} = \cdots = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$. Следовательно, $\alpha\beta,\ \alpha + \beta,\ \alpha^{-1} \in GF(q)$, если $\alpha \neq 0$.

С другой стороны, если P – конечное поле с единицей e, то среди элементов $e, 2e, 3e, \ldots$ найдутся два одинаковых. Например, $ae = b \cdot e$, $a > b$. В частности, $(a - b) \cdot e = 0$.

Пусть $p = min\{n \in \mathbf{N}; n > 0, ne = 0\}$. Тогда p – простое число (доказать!) и $P \supseteq GF(p) = \{0, e, 2e, \ldots, (p-1)e\}$. P является векторным пространством над $GF(p)$. Если $n = dimP$, то $P = \{\beta_1 v_1 + \ldots \beta_n v_n; \beta_i \in GF(p), \{v_1, \ldots, v_n\}$ – базис $\}$. Следовательно, $|P| = p^n = q$. Множество $P \setminus 0$ является группой порядка $(q - 1)$ относительно операции умножения. По следствию из тео-

ремы Лагранжа любой элемент $a \in P \setminus 0$ удовлетворяет равенству $a^{q-1} = e$ или $a^q = a$. Итак, элементы из P являются корнями $(x^q - x) \in GF(p)[x]$. Таким образом, конечные поля существуют, совпадают с множеством всех корней многочлена $(x^q - x) \in GF(p)[x]$, где $q = p^n$, в некотором расширении поля $GF(p)$.

Предложение 4. *Мультипликативная группа конечного поля $GF(q)$ является циклической.*

ДОКАЗАТЕЛЬСТВО. Пусть $G = GF(q) \setminus 0 = \{a_1, \ldots, a_{q-1}\}$. Порядок $k_i = |a_i|$ является делителем $q-1 = p_1^{l_1} \ldots p_s^{l_s}$. Пусть $m = [k_1, \ldots, k_{q-1}]$ – НОК чисел $k_1, \ldots, k_{q-1}$. Если $m = p_1^{t_1} \ldots p_s^{t_s}$, то найдутся элементы $a_{j_1}, \ldots, a_{j_s}$ такие, что $k_{j_1} = p_1^{t_1} \cdot v_1, \ldots, k_{j_s} = p^{t_s} \cdot v_s$. Тогда элементы $b_1 = a_{j_1}^{v_1}, \ldots, b_s = a_{j_s}^{v_s}$ имеют порядки $p_1^{t_1}, \ldots, p^{t_s}$ соответственно, а элемент $b_1 b_2 \ldots b_s = c$ будет иметь порядок m. Так как $k_i | m, i \leq q-1$, то каждый элемент из G является корнем $x^m - 1 \in GF(p)[x], q = p^n$. Т.е. $q - 1 \leq m$. С другой стороны, $m = |c| \mid (q-1)$ и $q - 1 = m$, т.е. $G = \langle 1, c, \ldots, c^{q-2} \rangle$.

Упражнение 1. Найти циклические порождающие полей $GF(4)$, $GF(9)$.

Упражнение 2. Найти все неприводимые многочлены степени два над $GF(5)$.

Упражнение 3:

а) решить в поле $GF(7)$ уравнение $x^4 = 3$;

б) решить в поле $GF(8)$ уравнения: 1) $x^6 = 5$; 2) $x^2 + x + 1 = 0$.

Упражнение 4. Пусть $R = \mathbf{Z}[i]$ и $I = (\alpha) \lhd R$. Доказать, что R/I – поле, если

1) $\alpha = 1 + i$ (порядка 4);

2) $\alpha = 3$ (порядка 9).

Если $\alpha = 5$, то доказать, что R/I не является полем.

Упражнение 5. Доказать, что в поле $GF(32)$ каждый элемент, не равный 0, 1, является циклическим порождающим (т.е. примитивным).

Упражнение 6. Поле $GF(q)$ содержит $\varphi(q-1)$ примитивных элементов.

Упражнение 7. Доказать, что группа обратимых элементов Z_{15} не является циклической.

Упражнение 8:

а) доказать изоморфизм полей

$$Z_2[x]/(x^3+x+1) \text{ и } Z_2[x]/(x^3+x^2+1);$$

б) найти корни (x^2+x+1) в поле $Z_2[x]/(x^4+x+1)$.

Упражнение 9. Пусть $N(n,p)$ – число неприводимых многочленов степени n в $Z_p[x]$. Доказать, что

$$N(n,p) = \frac{1}{n} \cdot \sum_{d|n} \mu(\frac{n}{d}) p^d.$$

УКАЗАНИЕ. Многочлен $(x^{p^n} - x)$ является произведением всех неприводимых многочленов степеней $d, d|n, d \leq n$. Следовательно,
$p^n = \sum\limits_{d|n} d \cdot N(d,p)$. По формуле обращения Мебиуса $nN(n,p) = \sum\limits_{d|n} \mu(\frac{n}{d}) p^d$.

Упражнение 10:

а) вычислить $N(n,2),\ n \leq 9$;

б) доказать, что $N(6,7) = 19544$.

3.5 Примеры кодов, исправляющих ошибки (продолжение: код Боуза-Чоудхури-Хоквингема)

Пример 5 (Bose-Chaudhuri-Hocquenghem, 1960).

Предположим, что нам необходимо передать получателю слово (a,b,c,d), где $a,b \in \{0,1\}$. Рассмотрим поле $GF(8) = Z_2[x]/(x^3+x+1) = \langle 0, 1, \alpha, \alpha^2, \ldots, \alpha^6 \rangle$, где $\alpha = \bar{x}$. По лемме о делении с остатком существуют многочлены $q(x)$ и $r(x)$ такие, что $ax^6 + bx^5 + cx^4 + dx^3 = (x^3+x+1)q(x) + r(x)$, где $r(x) = rx^2 + sx + t$. Положим $C(x) = ax^6 + bx^5 + cx^4 + dx^3 + rx^2 + sx + +t$. Вместо (a,b,c,d) будем передавать последовательность

(a, b, c, d, r, s, t). Предположим, что на выходе получатель получает последовательность (A, B, C, D, R, S, T) и число ошибок не превосходит одной. Укажем алгоритм ее обнаружения. Рассмотрим многочлен

$$R(x) = Ax^6 + Bx^5 + Cx^4 + Dx^3 + Rx^2 + Sx + T.$$

Пусть $E(x) = C(x) - R(x)$. Тогда либо $E(x) = 0$, либо $E(x) = x^e$, где $(e+1)$ – номер координаты, содержащей ошибку (если считать справа).

Если $R(\alpha) = 0$, то $E(\alpha) = C(\alpha) - R(\alpha) = 0$, и ошибки нет. Если $R(\alpha) = \alpha^e$, то $R(\alpha) = E(\alpha) = \alpha^e$ и $(e+1)$ – номер ошибочной координаты.

Например, закодируем последовательность (1, 1, 0, 1). Имеем

$x^6 + x^5 + x^3 = (x^3 + x + 1)q(x) + 1$. Следовательно, $C(x) = x^6 + x^5 + x^3 + 1$. Кодер выдает последовательность (1, 1, 0, 1, 0, 0, 1). Если получатель получает, например, последовательность (1, 1, 0, 1, 1, 0, 1), то
$R(x) = x^6 + x^5 + x^3 + x^2 + 1$ и $R(\alpha) = \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + 1 =$
$= (\alpha^2 + 1) + (\alpha^2 + \alpha + 1) + (\alpha + 1) + \alpha^2 + 1 = \alpha^2$, т.е ошибка произошла в пятом символе, считая слева.

Упражнение 1. Закодировать сообщения:

а) (1, 0, 0, 0);

б) (0, 1, 1, 0);

в) (1, 1, 1, 0).

Упражнение 2. Декодировать сообщения:

а) (1, 1, 1, 0, 0, 0, 1);

б) (1, 0, 1, 1, 0, 1, 1);

в) (0, 1, 0, 1, 0, 1, 0).

Пример 6 (Bose-Chaudhuri-Hocquenghem, 1960). Рассмотрим способ кодирования сообщений длины 7, позволяющий исправлять две ошибки. Для этого рассмотрим поле

$GF(16) = \mathbf{Z}_2[x]/(x^4 + x + 1) = \langle 0, 1, \alpha, \alpha^2, \ldots, \alpha^{14} \rangle$, где $\alpha = \bar{x}$ и $\alpha^4 = \alpha + 1, \alpha^5 = \alpha^2 + \alpha, \alpha^6 = \alpha^3 + \alpha^2, \alpha^7 = \alpha^3 + \alpha + 1,\ \alpha^8 = \alpha^2 + 1, \alpha^9 = \alpha^3 + \alpha, \alpha^{10} = \alpha^2 + \alpha + 1, \alpha^{11} = \alpha^3 + \alpha^2 + \alpha,\ \alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1, \alpha^{13} = \alpha^3 + \alpha^2 + 1, \alpha^{14} = \alpha^3 + 1.$

Найдем минимальный многочлен для α^3. Имеем

$$1 \cdot \alpha^3 = 0 \cdot 1 + 0 \cdot \alpha + 0 \cdot \alpha^2 + 1 \cdot \alpha^3,$$

$$\alpha \cdot \alpha^3 = 1 \cdot 1 + 1 \cdot \alpha + 0 \cdot \alpha^2 + 0 \cdot \alpha^3,$$

$$\alpha^2 \cdot \alpha^3 = 0 \cdot 1 + 1 \cdot \alpha + 1 \cdot \alpha^2 + 0 \cdot \alpha^3,$$

$$\alpha^3 \cdot \alpha^3 = 0 \cdot 1 + 0 \cdot \alpha + 1\alpha^2 + 1 \cdot \alpha^3.$$

Откуда следует, что $\begin{pmatrix} 0-\alpha^3 & 0 & 0 & 1 \\ 1 & 1-\alpha^3 & 0 & 0 \\ 0 & 1 & 1-\alpha^3 & 0 \\ 0 & 0 & 1 & 1-\alpha^3 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 \end{pmatrix} = 0.$

Следовательно, определитель матрицы равен нулю, т.е.

$(-\alpha^3) \cdot (1-\alpha^3)^3 - 1 = 0$. Таким образом, α^3 – корень многочлена

$f = t(1-t)^3 - 1 = t^4 + 3t^3 + 3t^2 + t + 1 = t^4 + t^3 + t^2 + t + 1.$

Многочлен $f(x)$ является неприводимым. Поэтому многочлен

$g(x) = (x^4 + x + 1)f(x) = x^8 + x^7 + x^6 + x^4 + 1$

является многочленом наименьшей степени, корнями которого являются α и α^3. Так как $g(\alpha^2) = g(\alpha)^2 = 0$, то $\alpha, \alpha^3, \alpha^2, \alpha^4, \alpha^6$ – корни многочлена $g(x)$. Рассмотрим информационное слово длины 7

$$(a_{14}, a_{13}, \ldots, a_8).$$

Разделим многочлен $C_1(x) = a_{14}x^{14} + a_{13}x^{13} + \cdots + a_8x^8$ на $g(x)$ с остатком

$$C_1(x) = g(x)q(x) + r(x),$$

где $r(x) = a_0 + a_1x + \cdots + a_7x^7$. Тогда

$C(x) = C_1(x) + r(x) = a_0 + a_1x + \cdots + a_{14}x^{14} = g(x)q(x).$

Рассмотрим новый (избыточный!) информационный вектор

$$C = (a_{14}, a_{13}, \ldots, a_1, a_0).$$

После отправления его получатель получает вектор $R = (b_{14}, b_{13}, \ldots, b_0)$. Декодируем его при предположении, что число ошибок не превосходит двух.

Рассмотрим вектор ошибок $E = R - C$ и соответствующие многочлены $E(x), R(x), C(x)$. Так как $\alpha, \alpha^2, \alpha^3$ – корни $C(x)$, то $E(\alpha) = R(\alpha), E(\alpha^2) = R(\alpha^2)$ и $E(\alpha^3) = R(\alpha^3)$, и многочлен $E(x)$ содержит не более двух ненулевых членов. Рассмотрим матрицу

$$S = \begin{pmatrix} S_1 & S_2 \\ S_2 & S_3 \end{pmatrix},$$

где $S_i = R(\alpha^i), i = 1, 2, 3$.

Случай 1. Ошибок нет. Тогда $E(x) = 0$ и $S = 0$.

Случай 2. Имеется одна ошибка. Тогда $E(x) = x^i,\ i \leq 14$ и $S = \begin{pmatrix} \alpha^i & \alpha^{2i} \\ \alpha^{2i} & \alpha^{3i} \end{pmatrix}$. Следовательно, ранг $r(S) = 1$. Так как $R(\alpha) = E(\alpha) = \alpha^i$, то ошибка содержится в i-ой координате.

Случай 3. Имеются две ошибки. Тогда $E(x) = x^i + x^j$, $S = \begin{pmatrix} \alpha^i + \alpha^j & \alpha^{2i} + \alpha^{2j} \\ \alpha^{2i} + \alpha^{2j} & \alpha^{3i} + \alpha^{3j} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \alpha^i & \alpha^j \end{pmatrix} \begin{pmatrix} \alpha^i & 0 \\ 0 & \alpha^j \end{pmatrix} \begin{pmatrix} 1 & \alpha^i \\ 1 & \alpha^j \end{pmatrix}$ и $r(S) = 2$.

Таким образом, ранг матрицы S равен числу ошибок при передаче информации. В третьем случае укажем алгоритм нахождения ошибочных координат. Именно найдем i, j, где $E(x) = x^i + x^j$.

Решим уравнение $\begin{pmatrix} S_1 & S_2 \\ S_2 & S_3 \end{pmatrix} \begin{pmatrix} \tau_2 \\ \tau_1 \end{pmatrix} = \begin{pmatrix} S_3 \\ S_4 \end{pmatrix}$.

Это возможно, т.к. $detS \neq 0$. Пусть

$(x - \alpha^i)(x - \alpha^j) = x^2 + \sigma_1 x + \sigma_2 \in GF(16)[x]$. Тогда

$$\alpha^{2i} + \sigma_1 \alpha^i + \sigma_2 = 0,$$

$$\alpha^{2j} + \sigma_1 \alpha^j + \sigma_2 = 0.$$

Умножая эти равенства соответственно на α^i и α^j, а затем складывая, имеем, что

$$S_3 + \sigma_1 S_2 + \sigma_2 S_1 = 0.$$

Аналогично, умножая вышеприведенные равенства на α^{2i}, α^{2j} и затем складывая, имеем, что

$$S_4 + \sigma_1 S_3 + \sigma_2 S_2 = 0,$$

т.е. $\begin{pmatrix} S_1 & S_2 \\ S_2 & S_3 \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} S_3 \\ S_4 \end{pmatrix}$.

Следовательно, $\tau_2 = \sigma_2$ и $\tau_1 = \sigma_1$. Итак, α^i и α^j – корни многочлена

$$x^2 + \sigma_1 x + \sigma_2 = 0.$$

Эти корни находятся путем перебора всех элементов поля $GF(16) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}\}$. Найдя их, мы одновременно найдем ошибочные координаты вектора R.

Рассмотрим пример, когда информационное слово (вектор) имеет вид (1, 1, 0, 1, 1, 0, 1). Разделим соответствующий многочлен

$C_1(x) = x^{14} + x^{13} + x^{11} + x^{10} + x^8$ на $g(x) = x^8 + x^7 + x^6 + x^4 + 1$.

Остаток при делении будет равен многочлену $(x + x^2 + x^4 + x^5 + x^7)$.

Следовательно, $C(x) = x^{14} + x^{13} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x$, и посылаемое кодовое слово имеет вид

(1, 1, 0, 1, 1. 0, 1, 1, 0, 1, 1, 0, 1, 1, 0).

Предположим, что мы получили вектор

(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0).

Вычислим $S_i = R(\alpha^i),\ i \le 4$. Имеем

$R(\alpha) = R(\alpha^2) = 1,\ R(\alpha^3) = \alpha + 1,$

$R(\alpha^4) = \alpha^{4\cdot 14} + \alpha^{4\cdot 13} + \alpha^{44} + \alpha^{40} + \alpha^{36} + \alpha^{32} + \alpha^{20} + \alpha^{16} + \alpha^8 + \alpha^4 = \alpha^{11} + \alpha^7 + \alpha^{14} + \alpha^{10} + \alpha^6 + \alpha^2 + \alpha^5 + \alpha + \alpha^8 + \alpha^4 = (\alpha^3 + \alpha^2 + \alpha) + (\alpha^3 + \alpha + 1) + (\alpha^3 + 1) + (\alpha^2 + \alpha + 1) + (\alpha^3 + \alpha^2) + \alpha^2 + (\alpha^2 + \alpha) + \alpha + (\alpha^2 + 1) + (\alpha + 1) = 1.$

Ранг матрицы $S = \begin{pmatrix} 1 & 1 \\ 1 & \alpha + 1 \end{pmatrix}$ равен двум. Следовательно, число ошибок равно двум. Решаем систему

$$\sigma_1 + \sigma_2 = \alpha + 1;$$

$$(\alpha+1)\sigma_1+\sigma_2=1.$$

Получаем, что $\sigma_1=1, \sigma_2=\alpha$. Найдем подбором корни многочлена x^2+x+ $+\alpha=0$. Они равны α^7, α^9. Действительно,

$$\alpha^{14}+\alpha^7+\alpha=(\alpha^3+1)+(\alpha^3+\alpha+1)+\alpha=0,$$

$$\alpha^{18}+\alpha^9+\alpha=\alpha^3+(\alpha^3+\alpha)+\alpha=0.$$

Следовательно, мы получили ошибки в седьмой и девятой координатах (считая справа и начиная с нуля).

Упражнение 3:

а) закодировать сообщения:

1) (1, 1, 1, 0, 0, 1, 1);

2) (1, 0, 1, 0, 1, 0, 1);

б) декодировать сообщения:

1) (011 001 011 101 100);

2) (100 100 100 100 100).

Пример 7 (Bose-Chandhuri-Hocquenghem, 1960). Используя поле $GF(16)$, построим алгоритм выявления трех ошибок в словах (информационных векторах) длины 15, содержащих 10 избыточных символов. Воспользуемся обозначениями примера 6. Многочлен x^2+x+1 является минимальным для α^5. Поэтому многочлен $m_{135}(x)=g(x)(x^2+x+1)$ является многочленом наименьшей степени, корнями которого являются элементы $\alpha, \alpha^3, \alpha^5$. Заметим, что $\deg m_{135}=10$ и $\alpha^2, \alpha^4, \alpha^6$ также являются корнями $m_{135}(x)$. Предположим, что мы должны послать сообщение $(a_{14}, a_{13}, a_{12}, a_{11}, a_{10})$. Рассмотрим многочлен

$$C_1(x)=a_{14}x^{14}+\cdots+a_{10}x^{10}$$

и разделим его с остатком $r(x)$ на $m_{135}(x)$. Положим

$C(x)=C_1(x)+r(x)=a_{14}x^{14}+\cdots+a_0$.

Посылаем вектор $C=(a_{14}, \ldots, a_0)$. Предположим, что получатель получает сообщение R. Рассмотрим вектор ошибок $E=R-C$. Имеем, что для

соответствующих многочленов $R(\alpha^i) = E(\alpha^i) = S_i,\ i = 1,2,3,4,5,6$, так как $C(\alpha^i) = 0,\ i = \overline{1,6}$. Рассмотрим матрицу

$$S = \begin{pmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{pmatrix}.$$

Случай 1. Если ошибок нет, то $E = 0$ и $S = 0$.

Случай 2. Если существует одна ошибка, то $E(x) = x^i$ и

$$S = \begin{pmatrix} \alpha^i & \alpha^{2i} & \alpha^{3i} \\ \alpha^{2i} & \alpha^{3i} & \alpha^{4i} \\ \alpha^{3i} & \alpha^{4i} & \alpha^{5i} \end{pmatrix}$$ имеет ранг 1.

При этом ошибка на месте $(i+1)$ координаты, считая справа.

Случай 3. Если имеется две ошибки, то $E(x) = x^i + x^j$ и

$$S = \begin{pmatrix} \alpha^i + \alpha^j & \alpha^{2i} + \alpha^{2j} & \alpha^{3i} + \alpha^{3j} \\ \alpha^{2i} + \alpha^{2j} & \alpha^{3i} + \alpha^{3j} & \alpha^{4i} + \alpha^{4j} \\ \alpha^{3i} + \alpha^{3j} & \alpha^{4i} + \alpha^{4j} & \alpha^{5i} + \alpha^{5j} \end{pmatrix}$$

имеет ранг два. В этом случае декодирование производится, как в примере 6, с помощью матрицы $S(2) = \begin{pmatrix} S_1 & S_2 \\ S_2 & S_3 \end{pmatrix}$.

Случай 4. При передаче совершено три ошибки, т.е.

$E(x) = x^i + x^j + x^k$. Рассмотрим матрицу

$$S = \begin{pmatrix} \alpha^i + \alpha^j + \alpha^k & \alpha^{2i} + \alpha^{2j} + \alpha^{2k} & \alpha^{3i} + \alpha^{3j} + \alpha^{3k} \\ \alpha^{2i} + \alpha^{2j} + \alpha^{2k} & \alpha^{3i} + \alpha^{3j} + \alpha^{3k} & \alpha^{4i} + \alpha^{4j} + \alpha^{4k} \\ \alpha^{3i} + \alpha^{3j} + \alpha^{3k} & \alpha^{4i} + \alpha^{4j} + \alpha^{4k} & \alpha^{5i} + \alpha^{5j} + \alpha^{5k} \end{pmatrix}.$$

Её ранг равен 3. Таким образом, число ошибок определяется рангом матрицы S. Как в последнем случае найти i, j, k, т.е. правильно декодировать сообщение? Для этого необходимо решить систему

$$S \cdot \begin{pmatrix} \sigma_3 \\ \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} S_4 \\ S_5 \\ S_6 \end{pmatrix}$$

.

А затем найти корни уравнения

$$x^3 + \sigma_1 x^2 + \sigma_2 x + \sigma_3 = 0.$$

Если эти корни равны $\alpha^i, \alpha^j, \alpha^k$, то i, j, k определяют номера ошибок в R.

Замечание 1. Работая в поле $GF(16)$ с помощью аналогичной техники, можно декодировать слова длины 15, содержащие 14 избыточных символов и не более 4-х ошибок.

Замечание 2. Используя поле $GF(2^5)$, можно декодировать сообщение длины 31, содержащее 20 избыточных символов и не более 5 ошибок.

Замечание 3. Используя поле $GF(2^6)$, можно декодировать слова длины 63, содержащие 33 избыточных символа и не более 6 ошибок, а также 56 избыточных символов и не более 15 ошибок (см. [5]).

Упражнение 4. В поле $GF(16) = Z_2(\alpha) = Z_2[x]/(x^4 + x + 1)$ решить систему

$$\begin{pmatrix} \alpha^3 + \alpha^4 & \alpha^6 + \alpha^8 \\ \alpha^6 + \alpha^8 & \alpha^9 + \alpha^{13} \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} \alpha^9 & + & \alpha^{12} \\ \alpha^{12} & + & \alpha^{16} \end{pmatrix}$$

и найти корни (в $Z_2[\alpha]$) уравнения

$$x^2 + \sigma_1 x + \sigma_2 = 0.$$

УКАЗАНИЕ. Воспользоваться равенствами $\alpha^4 = \alpha + 1,\ \alpha^8 = \alpha^2 + 1,$ $\alpha^{16} = \alpha$ и т.д.

Упражнение 5. Решить в $GF(16)$ систему

$$\begin{pmatrix} \alpha^2 + \alpha^5 + \alpha^{10} & \alpha^4 + \alpha^{10} + \alpha^{20} & \alpha^6 + \alpha^{15} + \alpha^{30} \\ \alpha^4 + \alpha^{10} + \alpha^{20} & \alpha^6 + \alpha^{15} + \alpha^{30} & \alpha^8 + \alpha^{20} + \alpha^{40} \\ \alpha^6 + \alpha^{15} + \alpha^{30} & \alpha^8 + \alpha^{20} + \alpha^{40} & \alpha^{10} + \alpha^{25} + \alpha^{50} \end{pmatrix} \begin{pmatrix} \sigma_3 \\ \sigma_2 \\ \sigma_1 \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha^8 & +\alpha^{20} & +\alpha^{40} \\ \alpha^{10} & +\alpha^{25} & +\alpha^{50} \\ \alpha^{12} & +\alpha^{30} & +\alpha^{60} \end{pmatrix}$$ и найти корни $x^3 + \sigma_1 x^2 + \sigma_2 x + \sigma_3 = 0.$

ОТВЕТ: корни равны $\alpha^2, \alpha^5, \alpha^{10}$.

Упражнение 6. Найти минимальный многочлен для $\alpha^7 \in GF(16)$.

УКАЗАНИЕ. Рассмотреть действие α^7 на базис $\{1, \alpha, \alpha^2, \alpha^3\}$.

Упражнение 7. Закодировать сообщение (1, 0, 0, 1, 1) кодом, допускающим не более трех ошибок.

Упражнение 8. Декодировать сообщения:

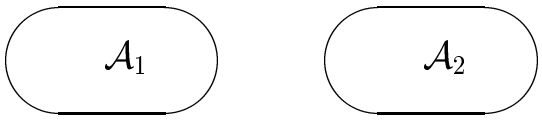
а) (101 1001 1001 1100),

б) (101 000 01 001 1110),

зная, что число ошибок не превосходит трех и кодировка проводилась методом примера 7.

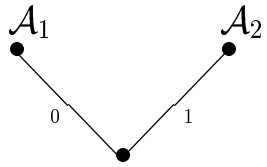
3.6 Однозначно декодируемые коды. Неравенство Крафта

Для уменьшения длины кодового текста и с целью экономии времени его передачи сообщения, встречающиеся чаще, кодируют словами меньшей длины, а редкие сообщения кодируют словами большой длины. Отчетливо это видно на примере азбуки Морзе. Рассмотрим произвольный ансамбль сообщений $\mathcal{A} = \{A_1, \ldots, A_n\}$ с набором вероятностей $P(A_1) \geq \geq P(A_2) \geq \cdots \geq P(A_n), \sum\limits_{i=1}^{n} P(A_i) = 1$. Применим т.н. алгоритм кодирования Фано. Разобьем множество $\mathcal{A}$ на две группы так, чтобы суммы вероятностей сообщений каждой из двух групп были как можно более близки друг к другу:

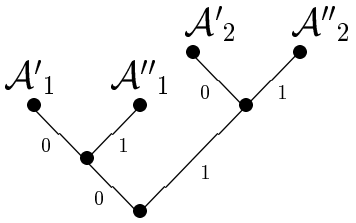


Припишем сообщениям 1-ой группы $\mathcal{A}_1$ символ 0, сообщениям из группы $\mathcal{A}_2$ – символ 1. По этому принципу каждая из групп $\mathcal{A}_1, \mathcal{A}_2$ разбивается на два множества: $\mathcal{A}_1 = \mathcal{A}_1' \cup \mathcal{A}_1'', \mathcal{A}_2 = \mathcal{A}_2' \cup \mathcal{A}_2''$. Припишем сообщениям из $\mathcal{A}_1'$ символ 00, из $\mathcal{A}_1''$ – символ 01, из $\mathcal{A}_2'$ – символ 10, из $\mathcal{A}_2''$ – символ 11. Продолжаем данный алгоритм до получения множеств, состоящих из 1 сообщения. В результате каждому сообщению ставится в соответствие

кодовое слово из 0 и 1. Чем больше вероятность $P(a_i)$ сообщения A_i, тем короче будет соответствующее кодовое слово. Указанный алгоритм может быть интерпретирован на языке теории графов. Именно, первый шаг алгоритма Фано соответствует графу (дереву):



Второй шаг соответствует графу:

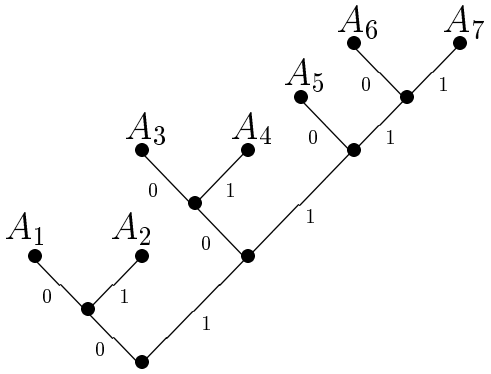


В результате мы получим кодовое дерево Фано нашего ансамбля (множества) сообщений. Разберем пример. Пусть дано множество $\mathcal{A} = \{A_1, \ldots, A_7\}$ из 7 сообщений, вероятности которых равны соответственно $p_1 = p_2 = 1/4, p_3 = p_4 = p_5 = 1/8$ и $p_6 = p_7 = 1/16$.

При первом разбиении $\mathcal{A}_1 = \{A_1, A_2\}, \quad \mathcal{A}_2 = \{A_3, A_4, A_5, A_6, A_7\}$.

При втором разбиении $\mathcal{A}'_1 = \{A_1\},\ \mathcal{A}''_1 = \{A_2\},\ \mathcal{A}'_2 = \{A_3, A_4\}$, $\mathcal{A}''_2 = \{A_5, A_6, A_7\}$. Продолжая аналогичные разбиения с множествами $\mathcal{A}'_2$ и $\mathcal{A}''_2$, мы получаем следующее дерево и соответствующие кодовые слова:

а)



б)

сообщения	A_1	A_2	A_3	A_4	A_5	A_6	A_7
кодовые слова	00	01	100	101	110	1110	1111

Покажем экономность вышеприведенного кодирования Фано примера из семи сообщений $\{A_1, \ldots, A_7\}$ по сравнению с равномерным кодированием: $A_1 \to 000,\ A_2 \to 001,\ A_3 \to 010, A_4 \to 011,\ A_5 \to 100,\ A_6 \to 110,\ A_7 \to 101$. Действительно, если нам предстоит передать текст, состоящий из 1000 сообщений в алфавите $\{A_1, \ldots, A_7\}$, то при равномерном кодировании мы используем 3000 двоичных символов, а при кодировании методом Фано мы используем

$250 \cdot 2 + 250 \cdot 2 + 125 \cdot 3 + 125 \cdot 3 + 125 \cdot 3 + \frac{125}{2} \cdot 4 + \frac{125}{2} \cdot 4 = 2625$ двоичных символов. Критерием экономности кода является т.н. средняя длина кодового слова

$$\bar{e} = \sum_{i=1}^{N} l_i P(A_i),$$

где l_i – длина кодового слова для A_i. Для нашего примера

$\bar{e} = 2 \cdot \frac{1}{4} + 2 \cdot \frac{1}{4} + \frac{3 \cdot 3}{8} + \frac{4}{16} \cdot 2 = 2\frac{5}{8} \approx 2,62.$

Упражнение 1. Закодировать двоичным кодом Фано следующие множества сообщений, найдя соответствующую среднюю длину и построив кодовое дерево:

а) десять сообщений с вероятностями

$$p_1 = p_2 = 0,22;\ p_3 = p_4 = p_5 = p_6 = 0,1;\ p_7 = p_8 = p_9 = p_{10} = 0,04;$$

б) четыре сообщения с вероятностями

$$p_1 = 0,5;\ p_2 = 0,25;\ p_3 = p_4 = 0,125.$$

Выяснить выигрыш по сравнению с равномерным кодированием.

Применяя в алгоритме Фано разбиение не на две группы с одинаковыми суммарными вероятностями, а на d равновероятных групп, мы придем к кодировке сообщений алфавитом из d символов. Соответствующее дерево имеет в каждой вершине не более d ребер.

Упражнение 2. Закодировать троичным кодом Фано 9 сообщений с вероятностями 1/3, 1/9, 1/9, 1/9, 1/9, 1/9, 1/27, 1/27,1/27.

Упражнение 3. Закодировать троичным кодом Фано 8 сообщений с вероятностями 0,3; 0,15; 0,15; 0,15; 0,07; 0,07; 0,07; 0,04.

Кодирование методом Фано является неравномерным. Ясно, что неравномерное кодирование приводит порой к неоднозначности декодирования. Например, если сообщения A_1 и A_2 кодируются соответственно 1 и 11, то кодированная последовательность 111 может быть дешифрована одним из следующих способов:

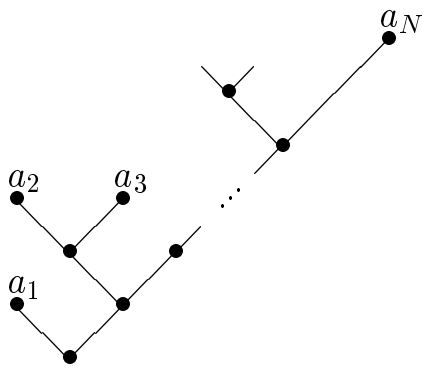
$$\{A_1, A_2\}, \{A_2, A_1\}, \{A_1, A_1, A_1\}.$$

Если код удовлетворяет условию, что каждая последовательность кодовых символов единственным образом разбивается на кодовые слова, то такой код называется однозначно декодируемым (или кодом без запятой). Примерами таких кодов является любой равномерный код, а также префиксный код (т.е. код, в котором никакое кодовое слово не является началом другого кодового слова). Код Фано является префиксным, так как кодовые слова соответствуют концевым вершинам кодового дерева. Более того, этот двоичный код является полным, т.е. добавление любого нового кодового слова в данном алфавите нарушает свойство префиксности.

Упражнение 4. Доказать, что соответствующие коды являются однозначно декодируемыми и не являются префиксными

$$\{1, 10\}, \{01, 10, 011\}.$$

Пусть $V = \{a_1, \ldots, a_N\}$ – некоторый префиксный двоичный код. Из префиксности следует, что V – концевые вершины некоторого (двоичного) графа (дерева)



Пусть n_k – число кодовых слов длины k, т.е. n_k – число вершин k-ого этажа. Ясно, что $n_k \leq 2^k$. Так как из каждой вершины i-го этажа вырастает (априори) 2^{k-i} вершин k-ого этажа, то в случае префиксного кода имеем неравенства

$$n_k \leq 2^k - 2^{k-1}n_1 - 2^{k-2}n_2 - \cdots - 2 \cdot n_{k-1},$$
$$\frac{n_1}{2} + \frac{n_2}{2^2} + \cdots + \frac{n_k}{2^k} < 1.$$

Если l – максимальная длина кодовых слов, то получаем так называемое неравенство Крафта

(1). $\sum\limits_{i=1}^{e} \frac{n_i}{2^i} \leq 1$ или $\frac{1}{2^{e_1}} + \frac{1}{2^{e_2}} + \cdots + \frac{1}{2^{e_n}} \leq 1$, где l_i – длина $a_i, i \leq N$.

Обратно, если выполнено неравенство (1), то существует префиксный код с длинами кодовых слов $l_1, l_2, \ldots, l_N$. Из (1) следуют неравенства: $n_1 \leq 2,\ n_2 \leq 4 - 2n_1,\ n_3 \leq 8 - 4n_1 - 2n_2, \ldots$. На первом этаже двоичного дерева выберем n_1 вершин, на 2-м этаже выберем произвольные n_2 вершин, исходящие из свободных (невыбранных)вершин первого этажа и т.д. Соответствующие двоичные кодировки образуют искомый префиксный код.

Упражнение 5. Префиксный код является полным тогда и только тогда, когда $\frac{1}{2^{e_1}} + \frac{1}{2^{e_2}} + \cdots + \frac{1}{2^{e_N}} = 1$.

УКАЗАНИЕ. Воспользоваться интерпретацией кода как двоичной записью концевых вершин некоторого графа (дерева).

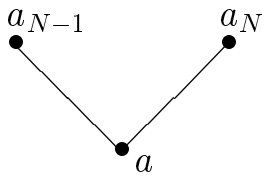
Замечание. Аналогично доказывается, что в алфавите из d символов существует префиксный код с длинами кодовых слов $e_1, \ldots, e_N$ тогда и только тогда, когда $\frac{1}{d^{e_1}} + \frac{1}{d^{e_2}} + \cdots + \frac{1}{d^{e_N}} \leq 1$.

Префиксный код Фано не является (в общем случае) оптимальным в том смысле, что средняя длина кодовых слов не является минимальной. Рассмотрим метод кодирования, принадлежащий Д. Хаффмену (1952 г.) и дающий префиксный оптимальный код. Рассмотрим ансамбль (множество) сообщений $\mathcal{A} = \{A_1, \ldots, A_N\}$, вероятности которых равны соответственно $p_1, p_2, \ldots, p_N$. При этом можно считать, что $p_1 \geq p_2 \geq \cdots \geq p_N$. Предположим, что эти сообщения закодированы в двоичном алфавите словами $a_1, a_2, \ldots, a_N$, длины которых равны соответственно $l_1, l_2, \ldots, l_N$. Если $l_{i+t} < l_i$, то, поменяв кодовые обозначения для A_i и A_{i+t}, мы получим, что средняя длина уменьшится на величину

$$p_i l_i + p_{i+t} l_{i+t} - p_i l_{i+t} - p_{i+t} l_i = (p_i - p_{i+t})(l_i - l_{i+t}) \geq 0.$$

Таким образом, при $p_{i+t} < p_i$ мы можем уменьшить среднюю длину, если $l_{i+t} < l_i$. Если $p_i = p_{i+1}$ и $l_{i+1} < l_i$, то переставим сообщения A_i и A_{i+1} местами (и соответственно переставим их кодовые слова).

В результате указанных действий мы, стремясь к оптимальности кодирования, можем так упорядочить наши сообщения $A_1, \ldots, A_N$ и так изменить порядок кодирования словами $\{a_i\}$, что $p_1 \geq p_2 \geq \cdots \geq p_N$ и $l_1 \leq l_2 \leq \cdots \leq l_N$. В частности, сообщение A_N кодируется словом наибольшей длины l_N. Если такое слово является единственным (т.е. $l_{N-1} < l_N$), то, отбрасывая последний символ слова a_N (длины l_N), мы получим префиксный код с меньшей средней длиной. Если $l_t = l_{t+1} = \cdots = l_N, l_{t-1} < l_t$ и среди слов $a_t, \ldots, a_N$ нет слов, отличающихся от a_N последним символом, то опять, отбрасывая в слове a_N последний символ, мы получим префиксный код с меньшей длиной. Если же слово $a_s (s \leq N-1)$ имеет ту же длину l_N (т.е. $l_s = l_{s+1} = \cdots = l_N$) и отличается от a_N последним символом, то, меняя местами кодовые слова a_s и a_{N-1}, мы можем считать, что два последних слова наибольшей длины a_{N-1}, a_N отличаются только последним символом.



Вернемся к нашему исходному множеству сообщений

$$\mathcal{A} = \{A_1, A_2, \ldots, A_{N-1}, A_N\},$$

где $p_i = p(A_i), i \leq N$. Рассмотрим его сжатие $\mathcal{A}^{(1)} = \{A_1, A_2, \ldots, A_{N-2}, A\}$, где $p(A_i) = p_i, i \leq N-2$ и $p(A) = p_{N-1} + p_N$. Пусть для $\mathcal{A}^{(1)}$ построена кодировка $K^{(1)} = \{a_1, a_2, \ldots, a_{N-2}, a\}$, т.е. кодовое дерево с концевыми вершинами $a_1, \ldots, a_{N-2}, a$. Сопоставим исходной системе $\mathcal{A}$ следующую систему кодовых обозначений $K = \{a_1, \ldots, a_{N-2}, a0, a1\}$, т.е. $a_{N-1} = a0, a_N = a1$. Такое сопоставление называется расщеплением.

Лемма. *Код K является оптимальным для системы $\mathcal{A}$, если код $K^{(1)}$ был оптимальным для системы $\mathcal{A}^{(1)}$.*

ДОКАЗАТЕЛЬСТВО. Предположим противное. Тогда существует код системы K_1 системы $\mathcal{A}$, для которого средняя длина $\bar{l}_1 = l(K_1) < l(K) = \bar{l}$. Пусть $K_1 = \{b_1, \ldots, b_{N-1}, b_N\}$. Согласно предыдущим замечаниям мы можем считать, что b_{N-1} и b_N – кодовые слова для наименее вероятных сообщений A_{N-1} и A_N. Причем они отличаются только последним символом, т.е. $b_{N-1} = b0, b_N = b1$ (или $b_{N-1} = b1, b_N = b0$). Рассмотрим код $K_1^{(1)} = \{b_1, \ldots, b_{N-2}, b\}$ для $\mathcal{A}^{(1)}$. Имеем $\bar{l}_1 = \bar{l}'_1 + p$ ($\bar{l}'_1 = l(K_1^{(1)})$). Так как $\bar{l}'_1 < \bar{l}$ и $\bar{l} = \bar{l}' + p$ (где $\bar{l}' = l(K^{(1)})$), то $\bar{l}'_1 < \bar{l}'$. Противоречие.

Согласно лемме, мы, используя несколько раз сжатие множества сообщений (соответственно, расщепление кодовых обозначений), можем построить оптимальный код (сначала сжимая, а потом расширяя).

Пример.

сообщ. $\mathcal{A}$	вероят- ности		сообщ. $\mathcal{A}^{(1)}$	вероят- ности		сообщ. $\mathcal{A}^{(2)}$		вероят- ности	средняя длина
A_1	0,5	0	A_1	0,5	0	A_1	0	0,5	
A_2	0,25	10	A_2	0,25	10	$\tilde{A}$	1	0,5	1,75
A_3	0,125	110	A	0,25	11				
A_4	0,125	111							

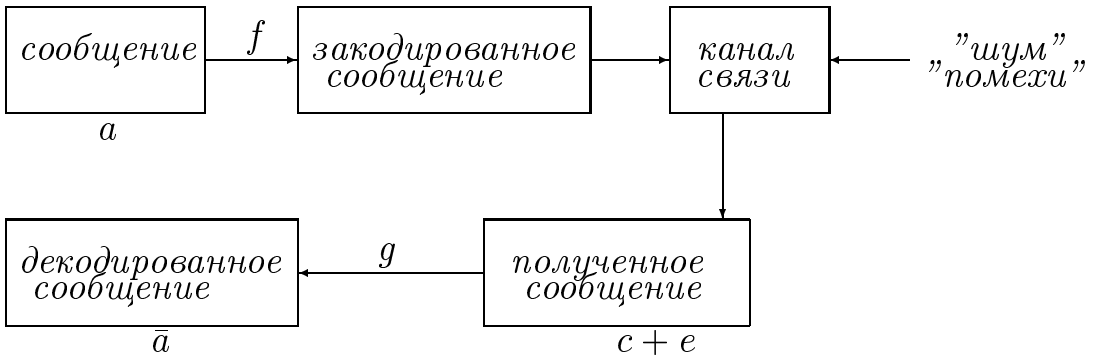
Упражнение 6. Закодировать двоичным кодом Хаффмена множество сообщений с вероятностями:

а) 0,4; 0,15; 0,15; 0,15; 0,15;

б) 0,25; 0,2; 0,15; 0,15; 0,15; 0,1.

3.7 Линейные коды

Как уже отмечалось ранее, используемый код должен быть надежным, быстрым в передаче и удобным. Сочетание этих трех моментов, а также наличие помех при передаче сообщения не позволяет использовать оптимальные коды в их явном виде. Для этого используются коды с избыточной информацией. Напомним упрощенную модель связи



Мы будем считать, что символы, входящие в запись сообщений и кодов, являются элементами поля $GF(q) = F_q$. Кодирование – это отображение $f : F_q^k \to F_q^n$, где $n > k$. Т.е. каждое сообщение $a_1 a_2 \dots a_k$ $(a_i \in F_q)$ заменяется кодовым словом $c_1 \dots c_n$. Аналогично, декодирование – это отображение g :

$F_q^n \to F_q^k$.

Пусть $x, y \in F_q^n$. Расстоянием Хэмминга $d(x, y)$ между векторами x, y называется число координат, которыми векторы x и y отличаются друг от друга, а весом Хэмминга $w(x)$ называется число ненулевых координат этого вектора. Ясно, что $d(x, y) = w(x - y)$, и если x – передаваемое слово, а y – полученное слово, то $d(x, y)$ – число ошибок, сделанных при передаче. Легко видеть, что функция $d(x, y)$ удовлетворяет следующим трем свойствам метрики в пространстве $F_q^n (\forall x, y, z \in F_q^n)$:

$1) d(x, y) = 0 \Leftrightarrow x = y;$

$2) d(x, y) = d(y, x);$

$3) d(x, z) \leq d(x, y) + d(y, z).$

Пусть $V \subseteq F_q^n$ – некоторое множество кодовых слов и t – натуральное число. Скажем, что код V исправляет не более t ошибок, если для любого $b \in F_q^n$ существует не более одного вектора $a \in V$ такого, что $d(b, a) \leq t$, т.е. в окрестности $B_t(b) = \{x \in F_q^n; d(b, x) \leq t\}$ существует не более одного вектора из V.

Число $d(V) = min\{d(a_1, a_2);\ a_1, a_2 \in V,\ a_1 \neq a_2\}$ называется кодовым (минимальным) расстоянием кода V.

Предложение 1. *Пусть* $d(V) \geq 2t+1$. *Тогда код* V *исправляет не более* t *ошибок.*

ДОКАЗАТЕЛЬСТВО. Пусть $b \in F_q^n$. Если шар (окрестность) $B_t(b)$ содержит два вектора $a_1, a_2 \in V$, то $d(a_1, a_2) \leq d(a_1, b) + d(a_2, b) \leq 2t$. С другой стороны, $d(a_1, a_2) \geq 2t + 1$. Противоречие доказывает предложение.

Т.е. если при передаче слова a произошло не более t ошибок, то для принятого слова b имеем неравенство $d(b, a) \leq t$ и для любого другого кодового слова $c \in V$ $d(b, c) \geq t + 1$.

Определение [13]. Пусть H – матрица над полем F_q порядка $(n-k) \times n$ и ранга $(n-k)$. Линейным (n, k) – кодом над полем F_q называется множество

C решений $c \in F_q^n$ системы линейных однородных уравнений

$$H \cdot c^T = 0.$$

Ясно, что $dim_{F_q}\mathbf{C} = k$. Число k называется размерностью кода, а число n – его длиной. Матрица H называется проверочной матрицей кода C, а элементы C называются кодовыми словами, или кодовыми векторами. Если $q = 2$, то код называется бинарным. Если $H = (AI_{n-k})$, где A – матрица порядка $(n-k, k)$, а I_{n-k} – единичная матрица порядка $(n-k)$, то код C называется систематическим. Если в систематическом коде C первые k символов в каждом кодовом слове являются информационными (т.е. совпадают с k символами исходного сообщения), а остальные $(n-k)$ символов являются проверочными, то система уравнений $H \cdot c^T = 0$ называется системой уравнений проверки на четность. Пример 3 в 3.2 соответствует систематическому бинарному коду с матрицей $H = (\underbrace{11\ldots1}_{k}1)$. Пример 1 из §2 соответствует линейному $(n, 1)$-коду с проверочной матрицей $H = (-1I_{n-1})$, т.е.

$$H = \begin{pmatrix} -1 & 1 & 0 & 0 & \ldots 0 \\ -1 & 0 & 1 & 0 & \ldots 0 \\ \vdots & \vdots & & & \\ -1 & 0 & 0 & \ldots & 0 \quad 1 \end{pmatrix} \in (F_q)_{(n-1)\times n}.$$

Пусть $H = (AI_{n-k})$ – проверочная матрица линейного (n, k) – кода. Тогда матрица $G = (I_k - A^T)$ порядка $k \times n$ называется порождающей (кодирующей) матрицей кода C. Эта матрица возникает в связи с равенством

$$c^T = \begin{pmatrix} I_k \\ -A \end{pmatrix} a^T = (a(I_k - A^T))^T,$$

где $a = a_1 \ldots a_k$ – передаваемое сообщение, $c = c_1 \ldots c_n$ – соответствующее кодовое слово и $Hc^T = 0$ – проверочное уравнение.

Так как $Hc^T = 0$ и $c = aG$, то $HG^T = 0$ (или $G \cdot H^T = 0$). Из этого равенства следует, что код C порождается строками G. В случае произвольного

линейного кода C его порождающей матрицей называется любая $(k \times n)$ матрица, строки которой порождают пространство C.

Определение. Пусть c – кодовое слово и y – слово, полученное после передачи сообщения по каналу (с помехами). Разность $e = y - c = e_1 \dots e_n$ называется вектором ошибок, или шумовым вектором.

Для линейного кода C минимальное расстояние Хэмминга $d_c = min\{d(u,v); u,v \in C, u \neq v\}$ совпадает с минимальным весом Хэмминга $min\{w(c); c \in C, c \neq 0\}$. Докажем следующий критерий для нижней границы минимального расстояния линейного кода C с проверочной матрицей H.

Предложение 2. *$d_c \geq s+1$ тогда и только тогда, когда любые s столбцов H линейно независимы.*

ДОКАЗАТЕЛЬСТВО. Если в H найдутся s столбцов $h_{i_1}, \dots, h_{i_s}$, которые линейно зависимы $\lambda_1 h_{i_1} + \dots + \lambda_s h_{i_s} = 0$, то вектор

$$c = (0, 0, \dots, 0, \lambda_1, 0, \dots, 0, \lambda_s, 0, \dots, 0) \in C$$

и имеет вес s, т.е. $d_c \leq s$. Обратно, пусть любые s столбцов H являются линейно независимыми и $d_c \leq s$. Пусть $a \in H, w(a) = d_c, a \neq 0$. Тогда из равенства $H \cdot a^T = 0$ следует, что некоторые $d_c \leq s$ столбцов H линейно зависимы.

Пусть далее C – линейный (n,k)-код над полем F_q. Разложим пространство F_q^n на смежные классы по C:

$$F_q^n = (0 + C) \cup (b^{(1)} + C) \cup \dots \cup (b^{(s)} + C),$$

где $s = q^{n-k} - 1$. В каждом классе $b^{(i)} + C (b^{(0)} = 0)$ существует элемент минимального веса. Выберем его и назовем лидером этого смежного класса. Если передавалось кодовое слово $c \in C$, а было принято слово y, то вектор ошибок $e = y - c$ принадлежит тому же смежному классу, что и y. Если $a^{(i)}$ – лидер класса $y + C$, то декодируем y как $x = y - a^{(i)} \in C$. Этот способ декодирования называется алгоритмом декодирования по ли-

деру смежного класса. Детализируем этот алгоритм. Пусть $a^{(1)}, \ldots, a^{(s)}$ – лидеры смежных классов $\bar{b}^{(1)}, \ldots, \bar{b}^{(s)}$ и $C = \{c^{(1)} = 0, c^{(2)}, \ldots, c^{(q^k)}\}$ – все элементы кода C. Пусть y – принятый вектор. Вектор Hy^T длины $(n-k)$ называется синдромом y. Ясно, что синдром векторов $y, z \in F_q^n$ совпадает тогда и только тогда, когда их смежные классы равны. Считаем далее синдром $S(y) = H \cdot y^T$. Зная синдром лидеров $S(a^{(1)}), \ldots, S(a^{(s)})$, мы определим смежный класс, в котором содержится y. Например, $y \in \bar{a}^{(i)}$. Тогда декодируем y как $x = (y - a^{(i)})$.

Пример. Рассмотрим бинарный (5,2) – код C с проверочной матрицей $H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix}$.

Пусть $y = (1, 1, 0, 1, 1)$ – полученное слово с синдромом $S(y) = H \cdot y^T = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$. Приведем все смежные классы, выделив в начале их лидеров:

(0, 0, 0, 0, 0), (0, 1, 0, 1, 1), (1, 0, 1, 0, 1), (1, 1, 1, 1, 0)
(1, 0, 0, 0,0), (1, 1, 0, 1, 1), (0, 0, 1, 0, 1), (0, 1, 1, 1, 0)
(0, 1, 0, 0, 0), (0, 0, 0, 1, 1), (1, 1, 1, 0, 1), (1, 0, 1, 1, 0)
(0, 0, 1, 0, 0), (0, 1, 1, 1, 1), (1, 0, 0, 0, 1), (1, 1, 0, 1, 0)
(0, 0, 0, 1, 0), (0, 1, 0, 0, 1), (1, 0, 1, 1, 1), (1, 1, 1, 0, 0)
(0, 0, 0, 0, 1), (0, 1, 0, 1, 0), (1, 0, 1, 0, 0), (1, 1, 1, 1, 1)
(1, 0, 0, 1, 0), (1, 1, 0, 0, 1), (0, 0, 1, 1, 1), (0, 1, 1, 0, 0)
(1, 1, 0, 0, 0), (1, 0, 0, 1, 1), (0, 1, 1, 0, 1), (0, 0, 1, 1, 0)

Так как $S(y) = S(a^{(1)}) = S \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$,

то искомое кодовое слово равно $x = y - a^{(1)} = (0, 1, 0, 1, 1)$.

Предложение 3. *Пусть C – бинарный (n, k)-код с проверочной матрицей H. Тогда синдром получаемого вектора y равен сумме столбцов H, номера которых совпадают с номерами ошибочных координат y.*

ДОКАЗАТЕЛЬСТВО. Действительно, пусть передавалось слово $x \in C$. Тогда
$y = x+e$ и $S(y) = He^T = h_{i_1}+h_{i_2}+\cdots+h_{i_s}$, где $e = (0, \ldots, 0, 1, 0, \ldots, 0, 1, 0, \ldots, 0)$, причем единицы стоят на местах i_1 и i_s.

Если все столбцы H различны и существует только одна ошибка в i-й координате, то $S(y) = h_i$, т.е. удачный выбор матрицы позволяет обнаруживать и исправлять одну ошибку.

Определение. Бинарный код C_m длины $2^m - 1 = n(m \geq 2)$ с проверочной матрицей H порядка $m \times (2^m - 1)$ называется кодом Хэмминга, если столбцы H представляют собой запись в двоичной системе чисел $1, 2, \ldots, 2^m - 1$.

Предложение 4. *Бинарный код C_m имеет размерность $(2^m - m - 1)$ и исправляет одну ошибку.*

ДОКАЗАТЕЛЬСТВО. Ранг матрицы C_m равен m и, следовательно,

$dim_{F_2} C_m = 2^m - 1 - m$. Так как любые два столбца C_m линейно независимые и C_m содержит их сумму, то $d_{c_m} = 2 + 1 = 3$ (см. предложение 2). По предложению 1 код C_m является кодом, исправляющим одну ошибку.

Пример. Пусть C_3 – бинарный (7, 4) – код Хэмминга. Его проверочная матрица равна

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

1	2	3	4	5	6	7

Пусть $y = (0, 0, 1, 0, 1, 0, 1)$ – полученное слово. Его синдром равен $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$.
Это первый столбец H. Следовательно, ошибка допущена в первой координате, и искомое кодовое слово равно (1, 0, 1, 0, 1, 0, 1).

В заключении параграфа докажем некоторые оценки относительно основных параметров, характеризующих код.

Предложение 5 (граница Хэмминга). *Пусть C – код над полем F_q, содержащий M кодовых слов, имеющий длину n и исправляющий t ошибок. Тогда*

$$M \cdot (1 + C_n^1(q-1) + \cdots + C_n^t(q-1)^t) \leq q^n.$$

ДОКАЗАТЕЛЬСТВО. Действительно, шары радиуса t с центрами в кодовых словах попарно не пересекаются. Каждый такой шар содержит помимо кодового слова ещё $C_n^1(q-1)$ слов, отличающихся от него одной координатой, $C_n^2(q-1)^2$ слов, отличающихся двумя координатами, и т.д. Так как $|\mathbf{F}_q^n| = q^n$, то неравенство доказано.

Приведем без доказательства следующее предложение [13]:

Предложение 6 (граница М.Плоткина). *Пусть C – линейный (n, k)-код над полем $\mathbf{F}_q$. Тогда*

$$d_c \leq \frac{n \cdot q^{k-1}(q-1)}{(q^k - 1)}.$$

3.8 Циклические коды

Линейный (n, k)-код C над полем $\mathbf{F}_q$ называется циклическим, если для любого вектора $(a_0, a_1, \ldots, a_{n-1}) \in C$ вектор

$$(a_{n-1}, a_0, a_1, \ldots, a_{n-2}) \in C.$$

Отождествим пространство $\mathbf{F}_q^n$ с фактор-кольцом $\mathbf{F}_q[x]/(x^n-1)$ относительно изоморфизма $(a_0, a_1, \ldots, a_{n-1}) \to \overline{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}}$. Смежный класс $\bar{a} \in F_q[x]/(x^n-1)$ часто будем записывать без черты.

Утверждение 1. *Линейный код C является циклическим тогда и только тогда, когда C-идеал в $\mathbf{F}_q[x]/(x^n-1)$.*

ДОКАЗАТЕЛЬСТВО. Действительно, если C – идеал и $(a_0, a_1, \ldots, a_{n-1}) \in C$, то $\bar{x} \cdot (\overline{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}}) = \overline{a_{n-1} \cdot 1 + a_0 \cdot x + \cdots + a_{n-2} \cdot x^{n-1}} \in C$, т.е. $(a_{n-1}, a_0, \ldots, a_{n-2})$ принадлежат C. Обратно, если C – циклический код, то для любого элемента $b \in C$ элементы $\bar{x}b, \ldots, \bar{x}^{n-1}b$ принадлежат C. Следовательно, для любого элемента

$$v = \overline{p_0 \cdot 1 + \cdots + p_{n-1}x^{n-1}} \in \mathbf{F}_q[x]/(x^n-1),\ v \cdot b = \sum_{i=0}^{n-1} p_i \bar{x}^i \cdot b \in C.$$

Если C – идеал в $F_q[x]/(x^n-1)$, то он является гомоморфным образом некоторого идеала P в $F_q[x]$, содержащего идеал (x^n-1).

Утверждение 2. *Идеал P является главным, т.е. $P = (g(x))$, где $g(x)$ – некоторый делитель (x^n-1) и старший коэффициент $g(x)$ равен единице.*

ДОКАЗАТЕЛЬСТВО. Пусть $g(x)$ – ненулевой многочлен минимальной степени из идеала P. Тогда можно считать, что старший коэффициент $g(x)$ равен единице, и если $\varphi(x) \in P$, то по лемме о делении с остатком $\varphi = g \cdot \psi + r$, где $r = 0$, либо $degg > degr$. Так как $r = \varphi - g\psi \in P$, то, ввиду минимальности $deg(g), r = 0$ и $P = (g(x))$. Так как $(x^n-1) \in P$, то $g(x)$ делит (x^n-1).

Ясно, что $C = (\overline{g(x)})$. Многочлен $g(x)$ называется порождающим многочленом кода C, а многочлен $h(x) = (x^n-1)/g(x)$ называется проверочным многочленом кода C.

Пусть $g(x) = g_0 + g_1 x + \cdots + 1 \cdot x^{n-k}$ и $h(x) = h_0 + h_1 x + \cdots + h_k x^k$. Тогда $g_0 h_0 = -1$, $\sum\limits_{i \le n-k} g_i h_{m-i} = 0, 1 \le m \le n-1, h_k = 1$. Далее, из включений $\bar{g}, \overline{xg}, \ldots, \overline{x^{k-1}}g \in C$ и неравенства $g_0 \neq 0$ следует, что следующую матрицу

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_{n-k} & 0 & 0 & \dots & o \\ 0 & g_0 & \dots & & g_{n-k} & 0 & \dots & 0 \\ \vdots & & & & & & & \\ 0 & 0 & \dots & 0 & g_0 & \dots & & g_{n-k} \end{pmatrix}$$

ранга k, где $g_{n-k} = 1$, можно взять в качестве порождающей для кода C (т.е. векторы $\bar{g}, \bar{x}g, \dots, \overline{x^{k-1}g}$ действительно образуют базис идеала C). Матрица

$$H = \begin{pmatrix} 0 & 0 & \dots & 0 & h_k & h_{k-1} & \dots & h_2 & h_1 & h_0 \\ 0 & 0 & \dots & h_k & h_{k-1} & \dots & & h_1 & h_0 & 0 \\ \vdots & h_k & & & & & & & \vdots & \\ h_k & h_{k-1} & \dots & h_0 & 0 & \dots & & & 0 & \end{pmatrix}$$ является провероч-

ной.

Как уже отмечалось, порождающих матриц для линейного кода много, т.к. они соответствуют базисам этого кода. Укажем некоторый **канонический** алгоритм выбора порождающей матрицы циклического кода C с порождающим многочленом $g(x)$ степени $(n-k)$ и с проверочным многочленом $h(x) = (x^n - 1)/g(x)$.

Замечание 1. Пусть $\overline{v(x)} \in F_q[x]/(x^n - 1)$. Тогда $\overline{v(x)} \in C \Leftrightarrow \bar{v} \cdot \bar{h} = \bar{0}$.

Замечание 2. Предположим, что нам необходимо передать информацию $(a_0, a_1, \dots, a_{k-1})$. Рассмотрим элемент

$$\bar{a}(x) = \overline{a_0 + a_1 x + \dots + a_{k-1}x^{k-1}} \text{ в } F_q[x]/(x^n - 1).$$

Закодируем его многочленом $\overline{w(x)} = \overline{a(x)g(x)}$ в $\mathbf{F}_q[x]/(x^n - 1)$, где $g(x)$ – порождащий многочлен кода C. Пусть $\overline{v(x)}$ – принятый для декодирования многочлен. Если остаток $v(x)$ от деления на $g(x)$ не равен нулю, то при передаче произошла ошибка.

Рассмотрим алгоритм Евклида (деления с остатком):

$$x^{n-k} = a_{n-k}(x)g(x) + r_{n-k},$$

$$x^{n-k+1} = a_{n-k+1}(x) \cdot g(x) + r_{n-k+1},$$

$$\dots,$$

$$x^{n-1} = a_{n-1}(x)g(x) + r_{n-1},$$

где $degr_j < n-k, j \leq n-1$.

В силу замечания 1, $(x^j - r_j) \in C$. Следовательно, многочлены $g_j(x) = \overline{x^k(x^j - r_j)} \in C,\ j = n-k,\ n-k+1, \dots, n-1$. Если многочлены g_j линейно зависимые, то при некоторых $\lambda_j \in \mathbf{F}_q$ (не все λ_j равны нулю) $\sum\limits_{j \leq n-1} \lambda_j g_j = 0$. Откуда следует, что

$$x^k(\overline{\lambda_{n-1}a_{n-1} + \lambda_{n-2}a_{n-2} + \dots + \lambda_{n-k}a_{n-k}}) \cdot \bar{g}(x) = \bar{0}.$$

Так как x не делит h и $deg(\lambda_{n-1}a_{n-1} + \dots + \lambda_{n-k}a_{n-k}) \leq k-1$, то $h(x)$ не делит $x^k(\sum \lambda_j a_j)$. Следовательно, $\lambda_i = 0, i \leq n-1$. Пусть

$$g_{n-k} = x^k(x^{n-k} - r_{n-k}) = x^k(-r_{n-k0} - r_{n-k1}x - \dots - r_{n-k,n-k-1}x^{n-k-1} + x^{n-k}),$$

$$\dots \qquad \dots$$

$$g_{n-1} = x^k(x^{n-1} - r_{n-1}) = x^k(-r_{n-10} - r_{n-11}x - \dots - r_{n-1n-k-1}x^{n-k-1} + x^{n-1}).$$

Соответствующая порождающая матрица равна

$$(I_k R) = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & -r_{n-k,0} & -r_{n-k,1} & \dots & -r_{n-k,n-k-1} \\ 0 & 1 & 0 & \dots & 0 & -r_{n-k+1,0} & -r_{n-k+1,1} & \dots & -r_{n-k+1,n-k-1} \\ \vdots & & \ddots & & & & & & \\ 0 & 0 & 0 & \dots & 1 & -r_{n-10} & -r_{n-1,1} & \dots & -r_{n-1,n-k-1} \end{pmatrix}.$$

Будем считать в дальнейшем, что $(n, q) = 1$. Если $x^n - 1 = f_1 f_2 \dots f_m$ – разложение на неприводимые многочлены в $\mathbf{F}_q[x]$, то, так как $(x^n - 1)' = nx^{n-1}$ и $(n, q) = 1$, $(x^n - 1)$ не имеет кратных корней.

В силу 3.3 каждый идеал (f_i) является максимальным, а соответствующий код называется максимальным циклическим кодом. Код, порожденный $(x^n - 1)/f_i$, называется неприводимым циклическим кодом.

Замечание 3. Так как каждый делитель (x^n-1) имеет вид $f_1^{\varepsilon_1}\dots f_m^{\varepsilon_m}$, где $\varepsilon_i=0,1$, то число нетривиальных делителей $(\neq 1, x^n-1)$ равно (2^m-2), т.е. циклических кодов длины n не более (2^m-2).

Замечание 4. Пусть $\alpha_1,\dots,\alpha_s$ – элементы алгебраического замыкания поля $\mathbf{F}_q$ и $p_1(x),\dots,p_s(x)$ – (соответственно) их минимальные многочлены над $\mathbf{F}_q$. Пусть n – минимальное натуральное число с условием, что $\alpha_1^n=\alpha_2^n=\dots=\alpha_s^n=1$. Тогда $g(x)=$ Н.О.К. $[p_1,p_2,\dots,p_s]$ делит (x^n-1). Пусть $C\subseteq\mathbf{F}_q^n$ – циклический код с порождающим многочленом $g(x)$. Тогда $f(x)\in C$ в том и только в том случае, если $f(\alpha_1)=\dots=f(\alpha_s)=0$.

Утверждение 3. *Пусть α – примитивный элемент поля F_{2^m} и $p(x)=(x-\alpha)(x-\alpha^2)\dots(x-\alpha^{2^{m-1}})$ – его минимальный многочлен над полем F_2. Тогда бинарный циклический код C длины $n=2^m-1$ с порождающим многочленом $p(x)$ эквивалентен бинарному $(2^m-1,2^m-m-1)$-коду Хэмминга.*

ДОКАЗАТЕЛЬСТВО. Так как $\{1,\alpha,\dots,\alpha^{m-1}\}$ – базис F_{2^m} над F_2, то имеют место равенства

$$\begin{array}{lcllllll}
\alpha^0 & = & 1\cdot 1 & + & 0\cdot\alpha & + \dots + & 0\cdot\alpha^{m-1},\\
\alpha^1 & = & 0\cdot 1 & + & 1\cdot\alpha & + \dots + & 0\cdot\alpha^{m-1},\\
 & & & & \vdots & & \\
\alpha^{m-1} & = & 0\cdot 1 & + & 0\cdot\alpha & + \dots + & 1\cdot\alpha^{m-1},\\
\alpha^m & = & a_{0,m+1}\cdot 1 & + & a_{1,m+1}\cdot\alpha & + \dots + & a_{m-1,m+1}\cdot\alpha^{m-1},\\
 & & & & \vdots & & \\
\alpha^{2^m-2} & = & a_{0,2^m-2}\cdot 1 & + & a_{1,2^m-2}\cdot\alpha & + \dots + & a_{m-1,2^m-2}\cdot\alpha^{m-1}.
\end{array}$$

Рассмотрим соответствующую матрицу

$$H=\begin{pmatrix}
1 & 0 & \dots & 0 & a_{0,m+1} & \dots & a_{0,2^m-2}\\
0 & 1 & \dots & 0 & a_{1,m+1} & \dots & a_{1,2^m-2}\\
\vdots & \vdots & \ddots & \vdots & \vdots & \dots & \vdots\\
0 & 0 & \dots & 1 & a_{m-1,m+1} & \dots & a_{m-1,2^m-2}
\end{pmatrix}.$$

Покажем, что H – проверочная матрица для кода C. Пусть

$a = (b_0, b_1, \ldots, b_{n-1})$ и $a(x) = b_0 + b_1 + \cdots + b_{n-1}x^{n-1}$ – соответствующий многочлен. Имеем

$$H \cdot a^T = \begin{pmatrix} 1 & 0 & \ldots & 0 & a_{0,m+1} & \ldots & a_{0,2^m-2} \\ 0 & 1 & \ldots & 0 & a_{1,m+1} & \ldots & a_{1,2^m-2} \\ \vdots & \vdots & \ddots & \vdots & \ldots & \ldots & \vdots \\ 0 & 0 & \ldots & 1 & a_{m-1,m+1} & \ldots & a_{m-1,2^m-2} \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} =$$

$$= \begin{pmatrix} b_0 & + & a_{0,m+1}b_m & + & \ldots & + & a_{0n}b_{n-1} \\ b_1 & + & a_{1,m+1}b_m & + & \ldots & + & a_{1n}b_{n-1} \\ & & & \vdots & & & \\ b_{m-1} & + & a_{m-1,m+1}b_m & + & \ldots & + & a_{m-1,n}b_{n-1} \end{pmatrix} \text{ и}$$

$$a(\alpha) = (b_0 + a_{0m+1}b_m + \cdots + a_{0n}b_{n-1}) \cdot 1 + (b_1 + a_{1m+1}b_m + \cdots + a_{1n}b_{n-1}) \cdot \alpha + \cdots + (b_{m-1} + a_{m-1m+1}b_m + \cdots + a_{m-1n}b_{n-1})\alpha^{m-1}.$$

Ясно, что $Ha^T = 0$ тогда и только тогда, когда $a(\alpha) = 0$. Последнее условие равносильно делимости $p(x)|a(x)$, так как $p(x)$ – неприводимый многочлен. Итак, мы доказали, что H – проверочная матрица для линейного $(n, n-m)$-кода C.

Для доказательства того, что C – ход Хэмминга, осталось доказать, что множество столбцов H исчерпывает множество чисел

$$1, 2, \ldots, 2^m - 1$$

в двоичной системе исчисления. Для этого достаточно заметить, что никакие два (ненулевых!) столбца не совпадают. В противном случае $\alpha^k = 1$, где $k \leq 2^m - 2$, что противоречит примитивности α (α – циклический порождающий группы $F^*_{2m} = F_{2m} \setminus \{0\}$).

Утверждение 4. *Пусть C – циклический код в $\mathbf{F}_q[x]/(x^n - 1)$ с порождающим многочленом $g(x)$, корни которого равны $\alpha_1, \ldots, \alpha_{n-k}$. Многочлен $f(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} \in C$ тогда и только тогда, когда*

$$H \cdot \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = 0, \text{ где } H = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ & & & \vdots & \\ 1 & \alpha_{n-k} & \alpha_{n-k}^2 & \dots & \alpha_{n-k}^{n-1} \end{pmatrix}.$$

ДОКАЗАТЕЛЬСТВО. Многочлен $f(x) \in C$ тогда и только тогда, когда $f(\alpha_i) = 0,\ i \leq n-k$. На матричном языке эти условия равносильны равенству $H \cdot \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = 0.$

Предположим, что мы имеем циклический код с порождающим многочленом $g(x)$, который, в свою очередь, является минимальным многочленом для $\alpha \in F_q m,\ \alpha^n = 1$, над полем F_q. Согласно предыдущему для исправления ошибки в полученном слове y необходимо вычислить синдром этого слова. Укажем один из алгоритмов такого вычисления. Элемент α является корнем $\varphi(x) \in F_q[x]/(x^n - 1)$ тогда и только тогда, когда $g(x)|\varphi(x)$. Следовательно, синдромом вектора $y = (y_0, y_1, \dots, y_{n-1})$ можно считать вектор $S(y) = (1\alpha\alpha^2 \dots \alpha^{n-1}) \cdot y^T = y(\alpha) = y_0 + y_1\alpha + \dots + y_{n-1}\alpha^{n-1}$. Если при передаче слова w получено слово y и совершено не более одной ошибки, то $y = w + e$, где $e = 0, x^{j-1}$ (в бинарном коде). Следовательно, синдром $S(y) = S(e) = 0, \alpha^{j-1}$. Этот синдром еще называют локатором ошибок. Если $S(y) = \alpha^{j-1}$, то ошибка произошла в j-ой координате (ибо $\alpha^i \neq \alpha^j$ при $i \neq j,\ i \leq n-1,\ j \leq n-1$).

3.9 Коды Боуза-Чоудхури-Хоквингема

Определение. Пусть m – мультипликативный порядок числа $q \in N$ по модулю n, т.е. $q^m \equiv 1(modn)$ и $q^i \not\equiv 1(modn)$ при $1 \leq i \leq m-1$. Далее, $b \in N \cup \{0\}$ и $\alpha \in \mathbf{F}_{q^m}$ такой, что $\alpha^n = 1, \alpha^i \neq 1, 1 \leq i \leq n-1$. Кодом Боуза-Чоудхури-Хоквингема (или БЧХ-кодом) длины n с конструктивным

расстоянием $d, 2 \leq d \leq n$, над полем F_q называется циклический код с порождающим многочленом, определяемым элементами

$$\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+d-2}.$$

Другими словами, порождающий многочлен $g(x)$ этого кода совпадает с НОК многочленов $m^{(b)}(x), \ldots, m^{(b+d-2)}(x)$, где $m^{(i)}(x)$ – минимальный многочлен α^i (над полем F_q).

Замечание. Если $n = q - 1$, то БЧХ-код называется кодом Рида-Соломона. Если $n = q^m - 1$, то БЧХ-код называется примитивным. Если $b = 1$, то БЧХ-код называется БЧХ-кодом в узком смысле.

Теорема. *Минимальное расстояние БЧХ-кода с конструктивным расстоянием d не меньше, чем d.*

ДОКАЗАТЕЛЬСТВО. Согласно утвержденияю 4 из 3.8, наш код совпадает с нуль-пространством проверочной матрицы

$$H = \begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \ldots & \alpha^{b(n-1)} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \ldots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & & \\ 1 & \alpha^{b+d-2} & \alpha^{2(b+d-2)} & \ldots & \alpha^{(n-1)(b+d-2)} \end{pmatrix}.$$

Согласно предложению 2 из 3.7, для доказательства теоремы достаточно показать, что любые $(d-1)$ различных столбцов этой матрицы являются линейно независимыми. Действительно, рассмотрим определитель

$$\begin{pmatrix} \alpha^{bi_1} & \alpha^{bi_2} & \ldots & \alpha^{bi_{d-1}} \\ \alpha^{(b+1)i_1} & \alpha^{(b+1)i_2} & \ldots & \alpha^{(b+1)i_{d-1}} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha^{(b+d-2)i_1} & \alpha^{(b+d-2)i_2} & \ldots & \alpha^{(b+d-2)i_{d-1}} \end{pmatrix} =$$

$$= \alpha^{b(i_1+\cdots+i_{d-1})} \prod_{t<s} (\alpha^{i_s} - \alpha^{i_t}) \neq 0.$$ Теорема доказана.

Эта теорема является важной, так как позволяет строить коды, исправляющие t ошибок. Для этого нужно выбрать числа d, n, q, m так, чтобы $2t + 1 \leq d \leq m$, m – мультипликативный порядок числа q по модулю n (мы предполагаем, что $(q, n) = 1$ и, следовательно, $m | \varphi(n)$). Так как группа

$GF(q^m)^*$ является циклической, то в ней существует элемент α порядка n. Т.е. мы всегда можем построить такой код.

Перейдем к описанию схемы декодирования БЧХ-кодов. Пусть $w(x), v(x)$ и $e(x)$ – соответственно передаваемый кодовый многочлен, принимаемый многочлен и многочлен ошибок ($e = w - v$). Пусть H – проверочная матрица из теоремы. Тогда синдром принятого вектора v равен $S(v) = H \cdot v^T = (S_b, S_{b+1}, \ldots, S_{b+d-2})^T$, где $S_j = v(\alpha^j) = e(\alpha^j)$, $b \le j \le b + d - 2$.

Пусть при передаче произошло r ошибок, где $r \le t \le \frac{d-1}{2}$. Тогда $e(x) = c_1 x^{a_1} + c_2 x^{a_2} + \cdots + c_r x^{a_r}$, где $a_1, \ldots, a_r$ – различные числа из множества $\{0, 1, \ldots, n-1\}$. Элементы $y_i = \alpha^{a_i} \in F_q m$ называются локаторами ошибки, а элементы $c_i \in F_q$ – значениями ошибки. В новых обозначениях координаты синдрома вектора v равны $S_j = e(\alpha^i) = c_1 y_1^j + c_2 y_2^j + \cdots + c_r y_r^j$,
$b \le j \le b + d - 2$. В силу тождества $(\beta + \gamma)^q = \beta^q + \gamma^q$ в поле $F_q m$ и так как $c_i \in F_q$, имеем равенства $S_j^q = \sum\limits_{i=1}^{r} c_i y_i^{jq} = S_{jq}$, $b \le j \le b + d - 2$. Рассмотрим далее многочлен $\prod\limits_{i=1}^{r}(y_j - x) = \sigma_r - \sigma_{r-1}x + \cdots + (-1)^r \sigma_0 x^r$, где $\sigma_0 = 1$, $\sigma_1, \sigma_2, \ldots, \sigma_r$ – элементарные симметрические многочлены от $y_1, \ldots, y_r$. Подставляя y_i вместо x, получаем систему равенств

$$\sigma_r - \sigma_{r-1} \cdot y_i + \cdots + (-1)^r \sigma_0 \cdot y_i^r = 0, \quad 1 \le i \le r.$$

Умножим i-ое равенство на $c_i y_i^j$ и сложим их все. Получим

$$(-1)^r \cdot \sigma_r \cdot S_j + (-1)^{r-1} \sigma_{r-1} \cdot S_{j+1} + \cdots + (-1)\sigma_1 \cdot S_{j+r-1} + S_{j+r} = 0, \quad (3.10)$$

где $b \le j \le b + r - 1$. Матрица этой системы равна

$$\begin{pmatrix} S_b & S_{b+1} & \ldots & S_{b+r-1} \\ S_{b+1} & S_{b+2} & \ldots & S_{b+r} \\ \vdots & \vdots & & \\ S_{b+r-1} & S_{b+r} & \ldots & S_{b+2r-2} \end{pmatrix} = V \cdot D \cdot V^T,$$

где $D = \begin{pmatrix} c_1 y_1^b & & 0 \\ & \ddots & \\ 0 & & c_r y_r^b \end{pmatrix}, V = \begin{pmatrix} 1 & 1 & \dots & 1 \\ y_1 & y_2 & \dots & y_r \\ \vdots & & & \\ y_1^{r-1} & y_2^{r-1} & \dots & y_r^{r-1} \end{pmatrix}$.

Ранг этой матрицы равен r тогда и только тогда, когда в векторе v имеется r ошибок. Многочлен вида $s(x) = \prod_{i=1}^{r}(1 - y_i x) = \sum_{i=0}^{r}(-1)^i \sigma_i x^i$ называется многочленом локаторов ошибки. Его корни равны $y_1^{-1}, \dots, y_r^{-1}$. Итак, приведем алгоритм декодирования БЧХ-кода с конструктивным расстоянием $d \geq 2t + 1$. Предположим, что передавалось слово w, а получено слово v.

Шаг 1. Находим синдром слова v

$$S(v) = (S_b, S_{b+1}, \dots, S_{b+d-2})^T.$$

Шаг 2. Находим максимальное число $r \leq \frac{d-1}{2}$ такое, что система уравнений

$$\begin{array}{ccccccccc} S_{b+r} & + & S_{b+r-1}x_1 & + & \dots & + & S_b x_r & = & 0 \\ S_{b+1+r} & + & S_{b+r}x_1 & + & \dots & + & S_{b+1}x_r & = & 0 \\ \vdots & & & & & & & & \\ S_{b+2r-1} & + & S_{b+2r-2}x_1 & + & \dots & + & S_{b+r-1}x_r & = & 0 \end{array}$$

имеет невырожденную матрицу коэффициентов (см. также (3.10)). Решая ее, мы найдем многочлен локаторов ошибки

$$S(x) = \prod_{i=1}^{r}(1 - y_i x) = \sum_{i=0}^{r} x_i x^i,$$

где $x_0 = 1$.

Шаг 3. Находим корни многочлена $s(x) = 0$, подставляя вместо x степени α.

Шаг 4. Рассмотрим систему уравнений

$$\begin{array}{ccccccc} c_1 y_1^b & + & \ldots & + & c_r y_r^b & = & S_b \\ c_1 y_1^{b+1} & + & \ldots & + & c_r y_r^{b+1} & = & S_{b+1} \\ \vdots & & & & & & \\ c_1 y_1^{b+r+1} & + & \ldots & + & c_r y_r^{b+r-1} & = & S_{b+r-1}. \end{array}$$

Определитель этой матрицы равен $(y_1 \ldots y_r)^b \prod\limits_{i<j}(y_i - y_j) \neq 0$. Следовательно, система имеет единственное решение $c_1, \ldots, c_r$. Итак, мы можем найти вектор ошибки $e(x)$. Из уравнения $w(x) = v(x) - e(x)$ находим слово w. Примеры в 3.5 иллюстрируют применение БЧХ-кода.

ЛИТЕРАТУРА

Учебники и монографии:

1. Аршинов М.И., Садовский Л.Е. Коды и математика. // Библ. Квант. Вып. 30, 1983.

2. Басакер Р., Саати Г. Конечные графы и сети. – М.: Наука, 1974.

3. Белов В.В. и др. Теория графов. – М.: Высш.школа, 1976.

4. Берж К. Теория графов и ее применение. – М.: Изд-во иностр. лит., 1962.

5. Берлекэмп Э. Алгебраическая теория кодирования. – М.: Мир, 1971.

6. Биркгоф Г., Барти Т. Современная прикладная алгебра. – М.: Мир, 1976.

7. Галлагер Р. Теория информации и надежная связь. – М.: Сов. радио, 1974.

8. Гроссман И., Магнус В. Группы и их графы. – М.: Мир, 1971.

9. Зыков А.А. Теория конечных графов. – М.: Наука, 1969.

10. Кассами Т., Токура Н. и др. Теория кодирования. – М.: Мир, 1978.

11. Колесник В.Д., Полтырев Г.Ш. Введение в теорию информации: Учеб. пособие. – Л.: Изд-во ЛГУ, 1980.

12. Колесник В.Д., Полтырев Г.Ш. Курс теории информации. – М.: Наука, 1982.

13. Лидл Р., Нидеррайтер Г. Конечные поля. Т.1-2. – М.: Мир, 1988.

14. Мак-Вильямс Ф., Слоэн Н.Дж. Теория кодов, исправляющих ошибки. – М.: Связь, 1969.

15. Марков А.А. Введение в теорию кодирования. – М.: Наука, 1982.

16. Оре О. Графы и их применение. – М.: Мир, 1965.

17. Оре О. Теория графов. – М.: Мир, 1968.

18. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. – М.: Мир, 1976.

19. Райзер Г.Д. Комбинаторная математика. – М.: Мир, 1966.

20. Риордан Дж. Введение в комбинаторный анализ. – М.: Изд-во иностр. лит., 1963.
21. Уилсон Р. Введение в теорию графов. – М.: Мир, 1977.
22. Харари Ф. Теория графов. – М.: Мир, 1973.
23. Холл М. Комбинаторика. – М.: Мир, 1970.
24. Шеннон К. Работы по теории информации и кибернетике. – М.: Изд-во иностр. лит., 1963.
25. Яблонский С.В. Введение в дискретную математику. – М.: Наука, 1979.
26. Bollobas Bela Graph theory: an introductory course. – New-York: Springer-Verlag, 1979.
27. Lindsay Childs. A concrete introduction to higher algebra: Undergrad. texts in Math. – New-York: Springer-Verlag, 1992.

Задачники:

28. Гаврилов Г.П., Сапоженко А.А. Сборник задач по дискретной математике. – М.: Наука, 1977.
29. Стечкин Б.С., Макаров Ю.Н., Меньшиков М.В., Ревякин А.М., Копылова А.Н. Комбинаторный анализ (задачи и упражнения). – М.: Наука, 1982.

Мальцев Юрий Николаевич
Петров Евгений Петрович

ВВЕДЕНИЕ В ДИСКРЕТНУЮ МАТЕМАТИКУ

Элементы комбинаторики, теории графов и теории кодирования

Учебное пособие

ЛР 020261
Н/К

Компьютерный набор – Т.И. Пиникер
Компьютерная верстка – Е.П. Петров
Оригинал-макет представлен в авторской редакции

Подписано в печать	17.02.1997.	Формат 60 × 84/16.
Бумага для множительных аппаратов.	Офсетная печать.	Уч.-изд. л. 6,07.
	Тираж 150 экз.	Заказ

Типография издательства
Алтайского государственного университета:
656099, Барнаул-99, ул. Димитрова, 66.