Конспект лекций по дискретной математике

Подготовил студент 105 группы:
Бугаевский Владимир

Большое спасибо за помощь в создании
всему коллективу 105 группы и отдельно
Морозову Никите и Петрову Илье

Версия от 06.06.2014

Внимание: в данном материале может содержаться туча ошибок

Глава 1

Функции алгебры логики. Булевы функции

$E_2 = B = \{0, 1\}$ - алфавит значений переменных;
$U = \{x_1, x_2...\}$ - алфавит переменных;
$E_2^n = B^n = \{(\alpha_1, \alpha_2, ...\alpha_n) | \alpha_i \in E_2, i = \overline{1, n}$ - n-мерный булев куб (гиперкуб).

Пример: $n = 2 \quad E_2^2 = \{(0,0), (0,1), (1,0), (1,1)\}$

Определение: Пусть $n \in \mathbb{N}$. Тогда булевой функцией называется всякая функция вида:

$$f(x_1, ...x_n) : E_2^n \to E_2$$

Определение: $\tilde{\alpha} = \alpha = \tilde{\alpha}^n = (\alpha_1...\alpha_n)$ - набор из n чисел. Введем число $\nu(\tilde{\alpha}) = |\tilde{\alpha}| = \sum_{i=1}^{n} \alpha_i * 2^{n-i} = (\alpha_1...\alpha_n)_2$. $\nu(\tilde{\alpha}^n)$ может принимать все значения от 0 до $2^n - 1$.

Определение: Порядок следования всех наборов $\tilde{\alpha}^n$ из E_2^n в соответствии с естественным возрастанием чисел $\nu(\tilde{\alpha}^n)$ от 0 до $2^n - 1$ называется лексикографическим.

Табличный способ задания булевой функции:
Пусть задана функция $f(\tilde{x}^n) : E_2^n \to E_2$

набор следует в лексикографическом порядке $\downarrow$

x_1	x_2	...	x_{n-1}	x_n	$f(\tilde{x}^n)$
0	0	...	0	0	$f(0,0,..0)$
0	0	...	0	1	$f(0,0,..1)$
...	...	...	...	...	...
α_1	α_2	...	α_{n-1}	α_n	$f(\alpha_1, \alpha_2, ..\alpha_n)$
...	...	...	...	...	...
1	1	...	1	0	$f(1,1,..0)$
1	1	...	1	1	$f(1,1,..1)$

Всего различных 2^n наборов.
Вектор значений булевой функции: $\tilde{\alpha}^n_{f(\tilde{x}^n)} = (f(0,0,...0,0), f(0,0,...0,1), ...f(1,1,...1,0), f(1,1,...1,1)$

Определение: Слово в алфавите A - это последовательность символов из множества. Количество членов этой последовательности - длина слова. Λ - пустое слово (длина 0).

Лемма 0: Количество попарно различных слов длины $l \in \mathbb{N}$ в алфавите из $r \in \mathbb{N}$ букв равно r^l.

Доказательство: с помощью метода математической индукции
▶ Базис: $l = 1$ - очевидно $r = r^1 = r^l$
Предположение: пусть верно для $l = l'$
Шаг: $l = l' + 1$. Рассмотрим любой слово ω длины $l' + 1$.

$$\omega = \underbrace{a_{i_1}a_{i_2}...a_{i_{l'}}}_{\omega'} a_{i_{l'+1}}$$

Перечислим все слова для $l' + 1$ с помощью таблицы:

$\omega_{l'+1}$ / ω'	a_1	a_2	...	a_r
$a_1...a_1a_1$	$a_1...a_1a_1\|a_1$	$a_1...a_1a_1\|a_2$	...	$a_1...a_1a_1\|a_r$
$a_1...a_1a_2$	$a_1...a_1a_2\|a_1$	$a_1...a_1a_2\|a_2$	...	$a_1...a_1a_2\|a_r$
...	...	...	...	...
$a_r...a_ra_r$	$a_r...a_ra_r\|a_1$	$a_r...a_ra_r\|a_2$	...	$a_r...a_ra_r\|a_r$

Ясно, что всего попарно различных слов длины $l+1$ в алфавите A из r букв - число клеток в таблице, т.е.

$$r^l r = r^{l+1}, \blacksquare.$$

Определение: P_2 - множество всех булевых функций; $P_2(n)$ - множество всех булевых функций от $x_1, x_2, ...x_n$. Так как таблицы различных функций из $P_2(n)$ отличаются одна от другой только столбцами значений функций, то из леммы 0 следует теорема 1.

Теорема 1: При $n \in \mathbb{N}$ $|P_2(n)| = 2^{2^n}$.

Элементарные булевы функции

x	f_1	f_2	f_3	f_4
0	0	0	1	1
1	0	1	0	1

f_1 - константа 0;
f_2 - тождественная функция;
f_3 - отрицание ($\bar{x}$);
f_4 - константа 1.

x_1	x_2	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}
0	0	0	0	1	0	1	1	1
0	1	0	1	1	1	0	1	0
1	0	0	1	0	1	0	1	0
1	1	1	1	1	0	1	0	0

x_1	x_2	x_3	m
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

$f_5 = x_1 \& x_2 = x_1 \cdot x_2 = x_1 \wedge x_2$ - логическое умножение, конъюнкция;
$f_6 = x_1 \vee x_2$ - логическое сложение, дизъюнкция;
$f_7 = x_1 \to x_2$ - импликация;
$f_8 = x_1 \oplus x_2$ - сложение по mod 2;
$f_9 = x_1 \sim x_2$ - эквивалентность;
$f_{10} = x_1|x_2$ - штрих Шеффера;
$f_{11} = x_1 \downarrow x_2$ - стрелка Пирса.
m - медиана, функция голосования.

Существенные и фиксированные переменные

Определение: Переменная x_i булевой функции $f(\tilde{x}^n)$ называется существенной переменной для f тогда и только тогда, когда существует набор $(\alpha_1, \alpha_2, ...\alpha_{i-1}, \alpha_i, \alpha_{i+1}, ...\alpha_n) \in E_2$ такой, что

$$f(\alpha_1, \alpha_2, ...\alpha_{i-1}, 0, \alpha_{i+1}, ...\alpha_n) \neq f(\alpha_1, \alpha_2, ...\alpha_{i-1}, 1, \alpha_{i+1}, ...\alpha_n).$$

Если переменная не является существенной, то ее называют фиктивной или несущественной.

Пример:

x_1	x_2	x_3	f
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0

x_1 - фиктивная;
x_2 - существенная;
x_3 - существенная.

Пусть x_i - фиктивная переменная булевой функции $f(\tilde{x}^n)$. Преобразуем таблицу для f следующим образом: вычеркнем все строки, где $x_i = 1$, а затем вычеркнем столбец x_i. Получим таблицу для булевой функции $f'(\alpha_1, \alpha_2, ...\alpha_{i-1}, 0, \alpha_{i+1}, ...\alpha_n)$. Будем говорить, что f' получена из f применением операции удаления фиктивной переменной x_i. Обратная операция, добавление фиктивной переменной x_i, позволяет по таблице f' получить таблицу f.

Определение: Булевы функции g_1 и g_2 равны тогда и только тогда, когда g_2 можно получить из g_1 последовательным применением операций добавления/удаления фиктивных переменных (число примененных операций конечно).

Задание булевой функции формулами

Пусть Q - множество булевых функций ($Q \subseteq P_2$). $Q = \{f_1, f_2, ...\}$.

Индуктивное определение формулы над Q:
Базис: Всякое выражение вида $f(x_1, ...x_n)$, где $f \in Q$, x_j - переменная ($j = \overline{1, n}$) - формула над Q.
Шаг: Пусть $f \in Q$, A_j - либо формула над Q, либо символ переменной. Тогда $f(A_1, A_2, ...A_n)$ - формула над Q.
Ничего другого.

В соответствии с этим определением каждой формуле над Q можно сопоставить реализуемую ей булеву функцию.

Каждая из формул, получаемая индуктивным построением формулы A - подформула A (в том числе сама A).

Определение: Две формулы A_1 и A_2 эквивалентны тогда и только тогда, когда реализуемые ими функции равны.

Тождества для элементарных булевых функций

1. Коммутативность: $\odot \in \{\cdot, \vee, \oplus, \sim, |, \downarrow\}$

$$x \odot y = y \odot x$$

2. Ассоциативность: $\odot \in \{\cdot, \vee, \oplus, \sim, |, \downarrow\}$

$$(x \odot y) \odot z = x \odot (y \odot z)$$

3. Дистрибутивность: $(\odot, \diamond) \in \{(\cdot, \vee), (\vee, \cdot), (\vee, \oplus)\}$

$$x \odot (y \diamond z) = (x \odot y) \diamond (x \odot z)$$

4. Правила де Моргана:

$$\overline{x \cdot y} = \bar{x} \vee \bar{y};$$
$$\overline{x \vee y} = \bar{x} \cdot \bar{y}$$

5. Правила поглощения:

$$x \vee (x \cdot y) = x;$$
$$x \cdot (x \vee y) = x$$

6. $$x \vee (\bar{x} \cdot y) = x \vee y;$$
$$x \cdot (\bar{x} \vee y) = x \cdot y$$

7. Разные правила:

$$x = \bar{\bar{x}} = x \oplus 0 = x \cdot x = x \vee x = x \cdot 1 = x \vee 0$$
$$\bar{x} = x \oplus 1$$
$$0 = x \cdot \bar{x} = x \oplus x = x \cdot 0$$
$$1 = x \vee \bar{x} = x \sim x = x \vee 1$$
$$x \to y = \bar{x} \vee y$$

Соглашения о виде тождеств

1. Внешние скобки формул можно не писать.
2. Внутренние скобки подформул, в которых используется лишь одна связка, обладающая ассоциативностью, можно не писать.
3. Конъюнкция старше остальных двуместных связок; внешние скобки подформул, внутри которых только функции, можно не писать.
4. Подформулы, над которыми расположена черта отрицания, можно записывать без внешних скобок.
5. $\&_{i=1}^{n} x_i = x_1 \cdot x_2 \cdot ... \cdot x_n$; $\bigvee\limits_{i=1}^{n} x_i = x_1 \cdot x_2 \cdot ... \cdot x_n$;
   $\sum\limits_{i=1}^{n} x_i = x_1 \oplus x_2 \oplus ... \oplus x_n$
6. $x^\sigma = \begin{cases} \bar{x}; \sigma = 0 \\ x; \sigma = 1 \end{cases}$

Определение: Всякое выражение вида: $K(\tilde{x}^n) = x_{i_1}^{\sigma_1} \cdot x_{i_2}^{\sigma_2} \cdot ... \cdot x_{i_r}^{\sigma_r}$, где $1 \leq i_1 \leq ... \leq i_r \leq n$, а $\sigma_1, ..., \sigma_r$ лежат в E_2, называется элементарной конъюнкцией ранга r от $x_1, .., x_n$.

Определение: Всякое выражение вида: $K(\tilde{x}^n) = x_{i_1}^{\sigma_1} \vee x_{i_2}^{\sigma_2} \vee ... \vee x_{i_r}^{\sigma_r}$, где $1 \leq i_1 \leq ... \leq i_r \leq n$, а $\sigma_1, ..., \sigma_r$ лежат в E_2, называется элементарной дизъюнкцией ранга r от $x_1, .., x_n$.

Определение: Монотонная конъюнкция - либо константа 1, либо конъюнкция различных переменных без отрицания.

Определение: Дизъюнктивная нормальная форма (ДНФ) - дизъюнкция различных элементарных конъюнкций.

Определение: Конъюктивная нормальная форма (КНФ) - конъюнкция различных элементарных дизъюнкций.

Определение: Полином Жегалкина - либо константа 0, либо сумма по $mod\ 2$ различных монотонных конъюнкций.

Теорема 2: (о разложении булевых функций по k переменным) Для любой булевой функции $f(\tilde{x}^n)$ и любого $k \in \{1..n\}$ имеет место равенство:

$$f(x_1, ..., x_k, x_{k+1}, ..., x_n) = \bigvee_{(\sigma_1,...,\sigma_k) \in E_2^k} x_1^{\sigma_1} \cdot x_2^{\sigma_2} \cdot ... \cdot x_k^{\sigma_k} \cdot f(\sigma_1, ..., \sigma_k, x_{k+1}, ..., x_n)$$

Доказательство: Докажем равенство для произвольного набора $\tilde{\alpha} = (\alpha_1, ..., \alpha_n)$ значений переменных $(x_1, ..., x_n)$ соответственно.

Левая часть равенства есть $f(\tilde{\alpha})$. Рассмотрим правую:

Случай 1: $(\sigma_1, ..., \sigma_n) : \forall i \in \{1, ..., k\} : \alpha_i = \sigma_i$. Следовательно соответствующее слагаемое имеет вид: $\underbrace{\alpha_1^{\sigma_1}}_{=1} \cdot ... \cdot \underbrace{\alpha_k^{\sigma_k}}_{=1} \cdot f(\sigma_1, ..., \sigma_k, \alpha_{k+1}, ..., \alpha_n) = f(\tilde{\alpha})$.

Случай 2: $(\sigma_1, ..., \sigma_n) : \exists i \in \{1, ..., k\} : \alpha_i \neq \sigma_i$. Следовательно соответствующее слагаемое имеет вид: $\underbrace{\alpha_1^{\sigma_1}}_{=0} \cdot ... \cdot \underbrace{\alpha_k^{\sigma_k}}_{=0} \cdot f(\sigma_1, ..., \sigma_k, \alpha_{k+1}, ..., \alpha_n) = 0$.

Итак, правая часть имеет на наборе $\tilde{\alpha}$ имеет вид $0 \vee 0 \vee ... \vee 0 \vee f(\tilde{\alpha}) \vee 0 \vee ... \vee 0$, т.е. равна $f(\tilde{\alpha})$, ■.

Теорема 3: (о разложении булевых функций по переменной) Для любой булевой функции $f(\tilde{x}^n)$ имеет место равенство:

$$f(x_1, x_2, ..., x_n) = \bar{x}_1 \cdot f(0, x_2, ..., x_n) \vee x_1 \cdot f(1, x_2, ..., x_n).$$

Доказательство: Тривиально следует из теоремы 2, ■.

Из доказательства теоремы 2 следует, что каждом наборе $\tilde{\alpha}$ количество равных 1 слагаемых в правой части тождества теоремы 2 не больше 1, поэтому верна теорема 4.

Теорема 4: $\forall f(\tilde{x}^n), \forall k \in \{1, ..., n\}$:

$$f(\tilde{x}^n) = \sum_{(\sigma_1, ..., \sigma_k) \in E_2^k} x_1^{\sigma_1} \cdot x_2^{\sigma_2} \cdot ... \cdot x_k^{\sigma_k} \cdot f(\sigma_1, ..., \sigma_k, x_{k+1}, ..., x_n)$$

Теорема 5: (о совершенной ДНФ) Для любой булевой функции $f(\tilde{x}^n)$, $f(\tilde{x}^n) \not\equiv 0$ имеем место представление:

$$f(\tilde{x}^n) = \bigvee_{\substack{(\sigma_1, ..., \sigma_n) \in E_2^n \\ f(\sigma_1, ..., \sigma_n) = 1}} x_1^{\sigma_1} \cdot x_2^{\sigma_2} \cdot ... \cdot x_n^{\sigma_n} \text{ - совершенная ДНФ}$$

Доказательство: Следует из теоремы 2, ■.

Теорема 6: (о совершенной КНФ) Для любой булевой функции $f(\tilde{x}^n)$, $f(\tilde{x}^n) \not\equiv 1$ имеем место представление:

$$f(\tilde{x}^n) = \&_{\substack{(\sigma_1, ..., \sigma_n) \in E_2^n \\ f(\sigma_1, ..., \sigma_n) = 0}} x_1^{\bar{\sigma}_1} \vee x_2^{\bar{\sigma}_2} \vee ... \vee x_n^{\bar{\sigma}_n} \text{ - совершенная КНФ}$$

Определение: Совершенная ДНФ для функции $f(x^n)$ - такая ДНФ, в которой всякий элемент конъюнкции имеет ранг n (и которая реализует функцию f).

Пример:

x_1	x_2	x_3	f
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

Совершенная ДНФ: $D_f^{\text{сов}}(x_1, x_2, x_3) = x_1^0 x_2^0 x_3^1 \vee x_1^0 x_2^1 x_3^1 \vee x_1^1 x_2^0 x_3^1 \vee x_1^1 x_2^1 x_3^0 = \bar{x}_1 \bar{x}_2 x_3 \vee \bar{x}_1 x_2 x_3 \vee x_1 \bar{x}_2 x_3 \vee x_1 x_2 \bar{x}_3$
Совершенная КНФ: $K_f^{\text{сов}}(x_1, x_2, x_3) = (x_1 \vee x_2 \vee x_3) \cdot (x_1 \vee \bar{x}_2 \vee x_3) \cdot (\bar{x}_1 \vee x_2 \vee \bar{x}_3) \cdot (\bar{x}_1 \vee \bar{x}_2 \vee \bar{x}_3)$

Геометрическая интерпретация ДНФ

Пусть $\tilde{\alpha} = (\alpha_1, ..., \alpha_n) \in E_2^n$ $(B^n = E_2^n)$.

Определение: Вес $\tilde{\alpha}$ - это количество $||\tilde{\alpha}||$ единиц в наборе $\tilde{\alpha}$.

Определение: Множество $B_k^n = \{\tilde{\alpha} | \tilde{\alpha} \in B^n, ||\tilde{\alpha}|| = k\}$ называется k-м слоем булевого куба, где $k \in \{0, 1, ..., n\}$.

Пусть $\tilde{\alpha} = (\alpha_1, ..., \alpha_n)$, $\tilde{\beta} = (\beta_1, ..., \beta_n)$ - наборы из B^n.

Определение: Расстояние Хеминга между $\tilde{\alpha}$ и $\tilde{\beta}$ - это количество координат в которых $\tilde{\alpha}$ и $\tilde{\beta}$ отличаются друг от друга:

$$\rho(\tilde{\alpha}, \tilde{\beta}) = \sum_{i=1}^{n} |\alpha_i - \beta_i|$$

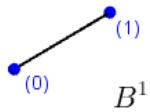
Если $\rho(\tilde{\alpha}, \tilde{\beta}) = 1$, то $\tilde{\alpha}$ и $\tilde{\beta}$ - соседние наборы.
Если $\rho(\tilde{\alpha}, \tilde{\beta}) = 0$, то $\tilde{\alpha}$ и $\tilde{\beta}$ - противоположные наборы.
Будем говорить, что $\tilde{\alpha}$ предшествует набору $\tilde{\beta}$ $(\tilde{\alpha} \preceq \tilde{\beta})$ тогда и только тогда, когда:

$$\alpha_1 \leq \beta_1; \alpha_2 \leq \beta_2; ...; \alpha_n \leq \beta_n$$

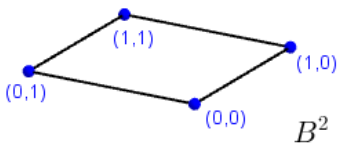
Если $\tilde{\alpha} \preceq \tilde{\beta}$ или $\tilde{\beta} \preceq \tilde{\alpha}$, то $\tilde{\alpha}$ и $\tilde{\beta}$ - сравнимые наборы $(\tilde{\alpha}, \tilde{\beta} \in B^n)$, иначе - несравнимые наборы.

Пример: $(0, 1)$ и $(1, 0)$ - несравнимые наборы.

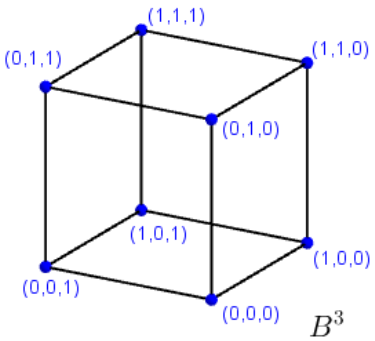
Будем изображать булев куб B^n геометрически, считая каждый набор $\tilde{\alpha}$ из B^n вершиной (точкой) и соединяя два набора $\tilde{\alpha}$ и $\tilde{\beta}$ из B^n отрезком несамопересекающейся гладкой кривой (наборы $\tilde{\alpha}$ и $\tilde{\beta}$ - соседние).



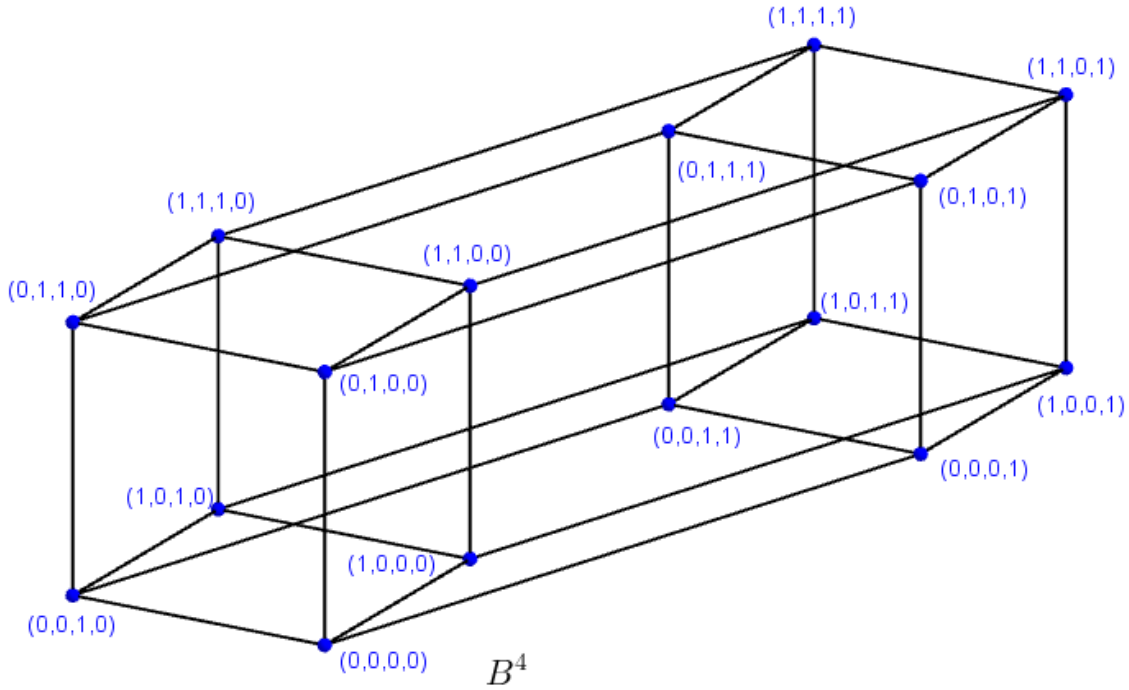
B^1



B^2



B^3



Пусть $f(\tilde{x}^n)$ - булева функция. $N_f = \{\tilde{\alpha} | \tilde{\alpha} \in B^n, f(\tilde{\alpha}^n) = 1\}$. Тогда булеву функцию $f(\tilde{x}^n)$ можно задать на кубе, выделив жирно те вершины, которые лежат в N_f.

$f = f_1 \cdot f_2 \Longleftrightarrow N_f = N_{f_1} \cap N_{f_2}$
$f = f_1 \cup f_2 \Longleftrightarrow N_f = N_{f_1} \cup N_{f_2}$
$f = \bar{f}_1 \Longleftrightarrow N_f = B^n \backslash N_{f_1}$

Определение: Пусть M - множество, и $\{M_1, M_2, ..., M_s\}$ - семейство всех подмножеств множества M. Это семейство образует покрытие множества M тогда и только тогда, когда $M = \bigcup_{i=1}^{s} M_i$.

Определение: Пусть $K(\tilde{x}^n)$ - элементарная конъюнкция от $x_1, ..., x_n$ ранга r. Тогда множество $N_{K(\tilde{x}^n)}$ называется гранью $\Gamma_{K(\tilde{x}^n)}$ размерности $n - r$ в булевом кубе B^n.

$$K(\tilde{x}^n) = x_{i_1}^{\sigma_1} \cdot x_{i_2}^{\sigma_2} \cdot ... \cdot x_{i_r}^{\sigma_r} \Rightarrow$$
$$\Rightarrow \Gamma_{K(\tilde{x}^n)} = \{(\alpha_1, ..., \alpha_{i_1-1}, \sigma_1, \alpha_{i_1+1}, ..., \alpha_{i_2-1}, \sigma_2, \alpha_{i_2+1}, ..., \alpha_{i_r-1}, \sigma_r, \alpha_{i_r+1}, ..., \alpha_n) |$$
$$\alpha_i \in B, i \in \{1, ..., n\} \ \{i_1, ..., i_r\}\}.$$

Эта грань может быть задан кодом вида:

$$(\underbrace{-}_{1} ... - \underbrace{\sigma_1}_{i_1} - ... - \underbrace{\sigma_2}_{i_2} - ... - \underbrace{\sigma_r}_{i_r} - ... \underbrace{-}_{n})$$

и является подкубом размерности $n - r$ в B^n.

Пусть $f(\tilde{x}^n) \not\equiv const$ - булева функция, отличная от константы. Пусть, далее, $K = K(\tilde{x}^n) = x_{i_1}^{\sigma_1} \cdot x_{i_2}^{\sigma_2} \cdot ... \cdot x_{i_r}^{\sigma_r}$ - элементарная конъюнкция, Γ_K - соответствующая ей грань, код которой имеет вид: $(-...-\sigma_1-...-\sigma_2-...-\sigma_r-...-)$.

Определение: Если $\Gamma_K \subseteq N_f$, то Γ_K называется гранью функции $f(\tilde{x}^n)$, а элементарная конъюнкция K называется импликантой булевой функции $f(\tilde{x}^n)$.
Если для любой грани Γ булева куба B^n такой, что $\Gamma_K \subset \Gamma$ выполнено условие $\Gamma \not\subseteq N_f$, то Γ_K называют максимальной гранью функции f, а K - простой импликантой функции f.

Любая ДНФ D, реализующая функцию f и имеющая вид $D(\tilde{x}^n) = K_1 \vee K_2 \vee ... \vee K_s$, соответствует покрытию множества N_f гранями $\Gamma_{K_1}, \Gamma_{K_2}, ..., \Gamma_{K_s}$ функции $f(\tilde{x}^n)$.

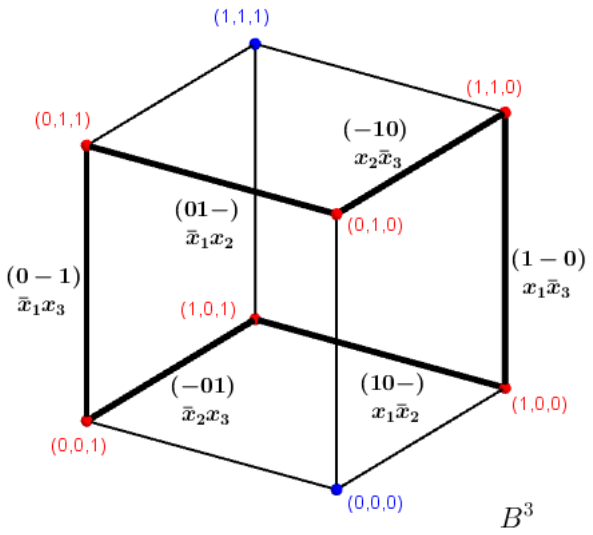
Замечание: Совершенная ДНФ соответствует покрытию множества N_f нульмерными гранями функции $f(\tilde{x}^n)$ (в кубе B^n).

Определение: Сокращенная ДНФ функции $f(\tilde{x}^n)$ - ДНФ, являющаяся дизъюнкцией всех простых импликант функции f.

Построение сокращенной ДНФ

Пример: $n = 3$

x_1	x_2	x_3	f
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	0



Представление булевой функции на кубе: вершины, соответствующие наборам из N_f - красные. Коды граней (выделены жирным) указаны жирным. $D_f^{\text{сокр}}(x_1, x_2, x_3) = \bar{x}_1x_2 \vee \bar{x}_1x_3 \vee \bar{x}_2x_3 \vee x_1\bar{x}_3 \vee x_1\bar{x}_3 \vee x_2\bar{x}_3$.

Пусть A - формула, представляющая собой конъюнкцию двух ДНФ. В результате раскрытия скобок, приведения подобных и поглощения из формулы A будет получена такая формула A', в которой:

1. нет одинаковых слагаемых (с точностью до перестановки);
2. нет слагаемых, получаемые другими слагаемыми (по формуле $K \vee KK' = K$) - с точностью до перестановки сомножителей;
3. A' есть дизъюнкция конъюнкций;
4. в каждом слагаемом в A' нет одинаковых сомножителей;
5. в A' нет слагаемых, содержащих множителей вида $x_i \cdot \bar{x}_i$б за исключением случая, когда функция, реализуемая формулой A есть константа 0, тогда $A' = x_i \cdot \bar{x}_i$.

Ясно, что A' может быть получена из A с помощью основных тождеств.

Пример:

$$A = (x_1\bar{x}_2 \vee x_3) \cdot (\bar{x}_1 x_3 \vee x_1 x_2) = x_1\bar{x}_2\bar{x}_1 x_3 \vee x_1 x_1 x_2 \bar{x}_2 \vee x_3 x_3 \bar{x}_1 \vee x_1 x_2 x_3 = x_3\bar{x}_1 \vee x_1 x_2 x_3 = A'$$

Лемма 1: Формула, полученная из конъюнкции двух сокращенных ДНФ путем раскрытия скобок, приведения подобных и поглощения, является сокращенной ДНФ.

Доказательство: Пусть $f = f_1 \cdot f_2$, $D_{f_1}^{\text{сокр}}$ и $D_{f_2}^{\text{сокр}}$ - сокращенные ДНФ f_1 и f_2, $A = D_{f_1}^{\text{сокр}} \cdot D_{f_2}^{\text{сокр}}$.

Достаточно доказать, что в формуле A', полученной из A так, как указано в условии леммы, встретится любая простая импликанта K формулы f.

Пусть K - простая импликанта f, тогда грань $\Gamma_K \subseteq N_f = N_{f_1} \cap N_{f_2}$. Следовательно

$$\exists K_1, K_2 : \Gamma_{K_1} \subseteq N_{f_1}, \Gamma_{K_2} \subseteq N_{f_2}, \Gamma_{\text{К}} \subseteq \Gamma_{K_1}, \Gamma_{\text{К}} \subseteq \Gamma_{K_2}$$

и K_1, K_2 - простые импликанты функций f_1, f_2 (соответственно). Тогда при раскрытии скобок в A получится элементарная конъюнкция, эквивалентная $K_1 \cdot K_2 = \hat{K}$.

Ясно, что $\Gamma_K \subseteq \Gamma_{\hat{K}}$. Если $\Gamma_K \subset \Gamma_{\hat{K}}$б то K - не простая импликанта функции f (т.к. Γ_K - не максимальная грань) - этот случай невозможен. Значит, $\Gamma_K = \Gamma_{\hat{K}}$, ■.

Теорема 7: (метод Нельсона построения сокращенной ДНФ по КНФ) Пусть функция f ($f \not\equiv const$) представлена какой-то КНФ. Тогда, последовательно раскрывая скобки (по парам), проводя приведение подобны и поглощения (после каждого раскрытия пары скобок), в конце концов будет построена сокращенная ДНФ функции f.

Пример:

$$\begin{gathered} f = (x_1 \vee \bar{x}_2)(x_1 \vee x_3)(x_1 \vee \bar{x}_2) = \\ = (x_1 x_1 \vee x_1 x_3 \vee x_1\bar{x}_2 \vee \bar{x}_2 x_3)(x_1 \vee \bar{x}_2) = \\ = (x_1 \vee \bar{x}_2 x_3)(x_1 \vee \bar{x}_2) = x_1 \vee \bar{x}_2 x_3 \end{gathered}$$

Полные системы в P_2

Определение: Система функций $Q(Q \subseteq P_2)$ называется полной в P_2 системой тогда и только тогда, когда любая булева функция может быть реализована формулой над Q.

Теорема 8: Пусть Q' - полная в P_2 система, каждая функция которой реализуется формулой над системой Q''. Тогда Q'' - полная в P_2 система.

Доказательство: Рассмотрим произвольную $f \in P_2$. Q' - полна в P_2, следовательно существует формула $A = A[Q']$ над Q', реализующая f. В A встречается конечное число функций из Q'. Каждая такая функция g_i реализуется формулой над $B_i[Q'']$ над Q''. Заменим (в порядке выполнения действий в формуле A) функции g_i на реализующие их формулы $B_i[Q'']$ - получим формулу $C[Q'']$ над Q'', реализующую f. Тогда, в силу произвольности выбора f, система Q'' полна в P_2, ■.

Примеры полных в P_2 систем

1. $Q_1 = P_2$ - полная в P_2 система;
2. $Q_2 = \{x_1 \& x_2, x_1 \vee x_2, bar x_1\}$ - полная в P_2 система.
   ► Рассмотрим произвольную булеву функцию $f(f \in P_2)$. Если $f \not\equiv 0$, то ее можно реализовать совершенной ДНФ, являющейся формулой над Q_2. Если $f \equiv 0$, то $f = x_i \cdot \bar{x}_i$, ■.
3. $Q_3 = \{x_1 \cdot x_2, \bar{x}_1\}$: сведем к Q_2 по теореме 8, т.к. $x_1 \vee x_2 = \overline{\bar{x}_1 \cdot \bar{x}_2}$;
4. $Q_4 = \{x_1 \vee x_2, \bar{x}_1\}$: аналогично $x_1 \cdot x_2 = \overline{\bar{x}_1 \vee \bar{x}_2}$;
5. $Q_5 = \{x_1|x_2\}$: сведем к Q_3 по теореме 8, т.к. $\bar{x}_1 = x_1|x_1$; $x_1 \cdot x_2 = (x_1|x_2)|(x_1|x_2)$;
6. $Q_6 = \{x_1 \downarrow x_2\}$: сведем к Q_4 по теореме 8, т.к. $\bar{x}_1 = x_1 \downarrow x_1$; $x_1 \vee x_2 = (x_1 \downarrow x_2) \downarrow (x_1 \downarrow x_2)$;
7. $Q_7 = \{x_1 \cdot x_2, x_1 \oplus x_2, 1, \underbrace{0}_{\text{не обяз.}}\}$: сведем к Q_3 по теореме 8, т.к. $\bar{x}_1 = x_1 \oplus 1$;

Замечание: Полином Жегалкина - формула над Q_7.

Теорема 9: У любой булевой функции f существует, и притом единственный, полином Жегалкина.

Доказательство:

1) Существование: Q_7 полна в P_2, следовательно для f существует реализующая ее формула над Q_7. Раскроем скобки, приведем подобные - получим полином Жегалкина.

Пример:

$$(x \oplus yz)(x \oplus y)(1 \oplus xz) = (x \oplus xy \oplus xyz \oplus yz)(1 \oplus xz) =$$
$$= x \oplus xy \oplus xyz \oplus yz \oplus xz \oplus xyz \oplus xyz \oplus xyz =$$
$$= x \oplus xy \oplus yz \oplus xz$$

2) Единственность: Каждый полином от $x_1, ..., x_n$ может быть представлена в виде:

$$P_f(\tilde{x}^n) = \underbrace{a_\varnothing \oplus \bigoplus_{k=1}^{n} \bigoplus_{1 \le i_1 < ... < i_k \le n} a_{\{i_1,...,i_k\}}}_{\text{коэффициенты из } \{0;1\}} \cdot x_{i_1} \cdot ... \cdot x_{i_k}$$

Таких наборов столько же, сколько наборов коэффициентов $\underbrace{(a_{\varnothing}, a_{\{1\}}, ..., a_{\{n\}}, a_{\{1,2\}}, ..., a_{\{1,2,...,n\}})}_{2^n \text{координат}}$, но таких векторов 2^{2^n} по лемме 0, следовательно число неэквивалентных полиномов есть 2^{2^n} (полиномов от $x_1, ..., x_n$).

Но по тереме 1 имеем $|P_2(n)| = 2^{2^n}$, следовательно, если бы при некотором n нашлась булева функция f, обладающая более чем 1 полиномом, то число полиномов для этого n было бы больше, чем 2^{2^n}, что не так, ■.

Нумерация монотонных конъюнкций

от $x_1, ..., x_n$

1. Пусть $(\alpha_1, ..., \alpha_n) = (0, 0, ..., 0)$, следовательно $\nu(\alpha_1, ..., \alpha_n) = 0$, и тогда $K_0^+(\tilde{x}^n) = 1$.
2. Пусть $(\alpha_1, ..., \alpha_n) = (0, ..., 0, \underbrace{1}_{i_1}, 0, ..., 0, \underbrace{1}_{i_2}, 0, ..., 0, \underbrace{1}_{i_r}, 0, ..., 0)$
   ($'1'$ - в позициях $i_1, i_2, ..., i_r$ $(r \geq 1)$, в остальных позициях - $'0'$),
   и пусть $j = \nu(\alpha_1, ..., \alpha_n), j \in \{1, ..., 2^n - 1\}$, тогда $K_j^+(\tilde{x}^n) = x_{i_1} \cdot x_{i_2} \cdot ... \cdot x_{i_r}$.

Пример: n = 2

$j = \nu(x_1, x_2)$	x_1	x_2	$K_j^+(x_1, x_2)$
0	0	0	1
1	0	1	x_2
2	1	0	x_1
3	1	1	$x_1 \cdot x_2$

Любой полином Жегалкина от $x_1, ..., x_n$ можно представить в виде:

$$f(\tilde{x}^n) = P(\tilde{x}^n) = \sum_{j=0}^{2^n-1} \beta_j \cdot K_j^+(\tilde{x}^n).$$

Вектор коэффициентов полинома Жегалкина от функции $f(\tilde{x}^n)$:

$$\beta_{f(\tilde{x}^n)} = (\beta_0, \beta_1, ..., \beta_{2^n-1}).$$

Определение: Операция T (индуктивное по n).
Базис: $n = 1$, $T(\alpha_0, \alpha_1) = (\alpha_0, \alpha_0 \oplus \alpha_1)$
Шаг: Пусть

$$T(\alpha_0^{(0)}, ..., \alpha_{2^n-1}^{(0)}) = (\beta_0^{(0)}, ..., \beta_{2^n-1}^{(0)}),$$
$$T(\alpha_0^{(1)}, ..., \alpha_{2^n-1}^{(1)}) = (\beta_0^{(1)}, ..., \beta_{2^n-1}^{(1)}),$$

тогда:

$$T(\alpha_0^{(0)}, ..., \alpha_{2^n-1}^{(0)}, \alpha_0^{(1)}, ..., \alpha_{2^n-1}^{(1)}) = (\beta_0^{(0)}, ..., \beta_{2^n-1}^{(0)}, \beta_0^{(0)} \oplus \beta_0^{(1)}, ..., \beta_{2^n-1}^{(0)} \oplus \beta_{2^n-1}^{(1)}).$$

Теорема 10: Для любой булевой функции $f(\tilde{x}^n)$ (при $n \in \mathbb{N}$):

$$\tilde{\beta}_{f(\tilde{x}^n)} = T(\tilde{\alpha}_{f(\tilde{x}^n)}),$$

где $\tilde{\beta}_{f(\tilde{x}^n)}$ - вектор коэффициентов; $\tilde{\alpha}_{f(\tilde{x}^n)}$ - вектор значений f.

Доказательство: (индукция по n). Пусть $\tilde{\alpha}_{f(\tilde{x}^n)} = (\alpha_0, \alpha_1)$.
Базис: $n = 1$

x_1	f
0	α_0
1	α_1

По теореме 4 при $k = 1$:

$$f(x_1) = \bar{x}_1 \cdot f(0) \oplus x_1 \cdot f(1) = \bar{x}_1 \cdot \alpha_0 \oplus x_1 \cdot \alpha_1 = (x_1 \oplus 1) \cdot \alpha_0 \oplus x_1 \cdot \alpha_1 = \alpha_0 \cdot 1 \oplus (\alpha_0 \oplus \alpha_1) \cdot x_1 =$$
$$= \underbrace{\alpha_0}_{\beta_0} \cdot K_0^+(x_1) \oplus \underbrace{\alpha_0 \oplus \alpha_1}_{\beta_1} \cdot K_1^+(x_1).$$

Т.е. $(\beta_0, \beta_1) = T(\alpha_0, \alpha_1)$ - базис доказан.

Шаг: Пусть верно для n, докажем для $n+1$. Пусть,

$$f_0(x_2, ..., x_{n+1}) = f(0, x_2, ..., x_{n+1}),$$
$$f_1(x_2, ..., x_{n+1}) = f(1, x_2, ..., x_{n+1}),$$
$$T(\tilde{\alpha}_{f_0(x_2,...,x_{n+1})}) = \tilde{\beta}_{f_0(x_2,...,x_{n+1})} = (\beta_0^{(0)}, ..., \beta_{2^n-1}^{(0)}),$$
$$T(\tilde{\alpha}_{f_1(x_2,...,x_{n+1})}) = \tilde{\beta}_{f_1(x_2,...,x_{n+1})} = (\beta_0^{(1)}, ..., \beta_{2^n-1}^{(1)}).$$

По теореме 4 при $k = 1$:

$$f(x_1, x_2, ..., x_{n+1}) = \bar{x}_1 \cdot f_0(x_2, ..., x_{n+1}) \oplus x_1 \cdot f_1(x_2, ..., x_{n+1}) =$$
$$= \bar{x}_1 \cdot \sum_{j=0}^{2^n-1} \beta_j^{(0)} \cdot \hat{K}_j^+(x_2, ..., x_{n+1}) \oplus x_1 \cdot \sum_{j=0}^{2^n-1} \beta_j^{(1)} \cdot \hat{K}_j^+(x_2, ..., x_{n+1}) =$$
$$= \sum_{j=0}^{2^n-1} \beta_j^{(0)} \cdot \underbrace{\hat{K}_j^+(x_2, ..., x_{n+1})}_{K_j^+(x_1,...,x_{n+1})} \oplus \sum_{j=0}^{2^n-1} (\beta_j^{(0)} \oplus \beta_j^{(1)}) \cdot x_1 \cdot \underbrace{\hat{K}_j^+(x_2, ..., x_{n+1})}_{K_{2^n+j}^+(x_1,...,x_{n+1})} \Rightarrow$$
$$\Rightarrow \tilde{\beta}_{f(x_1,...,x_{n+1})} = (\beta_0^{(0)}, ..., \beta_{2^n-1}^{(0)}, \beta_0^{(0)} \oplus \beta_0^{(1)}, ..., \beta_{2^n-1}^{(0)} \oplus \beta_{2^n-1}^{(1)}).$$

Но т.к. $\tilde{\alpha}_{f(x_1,...,x_{n+1})} = (\tilde{\alpha}_{f_0(x_2,...,x_{n+1})}, \tilde{\alpha}_{f_1(x_2,...,x_{n+1})})$, то:

$$T(\tilde{\alpha}_{f(x_1,...,x_{n+1})}) = \tilde{\beta}_{f(x_1,...,x_{n+1})}, \blacksquare.$$

<Здесь должна быть табличка, отражающая суть наборов>

Замыкания. Важнейшие замкнутые классы

Пусть Q - система булевых функций ($Q \subseteq P_2$)

Определение: Замыканием Q называется множество $[Q]$ всех булевых функций, реализуемых формулами над Q.

Свойства замыканий:

1. $Q_1 \subseteq Q_2 \Rightarrow [Q_1] \subseteq [Q_2]$
2. $Q \subseteq [Q]$
3. $[[Q]] = [Q]$
4. $[Q_1 \cap Q_2] \subseteq [Q_1] \cap [Q_2]$
5. $[Q_1 \cup Q_2] \supseteq [Q_1] \cup [Q_2]$

Определение: Система булевых функций Q называется замкнутым классом тогда и только тогда, когда $[Q] = Q$.

I. Классы, сохраняющие 0 и 1

Пусть $\sigma \in \{0,1\}$. Функция $f(x_1,...,x_n)$ сохраняет σ тогда и только тогда, когда $f(\sigma,...,\sigma)=\sigma$. Сумма всех булевых функций, сохраняющий σ обозначается T_σ.

Лежат в T_0: $0, x, xy, x \vee y, x \oplus y, m(x,y,z) = xy \vee yz \vee xz$;
Не лежат в T_0: $1, \bar{x}, x \sim y, x \to y, x|y, x \downarrow y$.
Лежат в T_1: $1, x, xy, x \vee y, x \sim y, x \to y, m(x,y,z)$;
Не лежат в T_1: $0, \bar{x}, x \oplus y, x|y, x \downarrow y$.

Лемма 2: $T_\sigma = [T_\sigma], \sigma \in \{0,1\}$. ($T_\sigma, T_0, T_1$ - замкнутые классы)

Доказательство: Т.к. $x \in T_\sigma$, то достаточно доказать, что если $f_0, f_1, ..., f_t \in T_\sigma$, то $\Phi = f_0(f_1,...,f_t) \in T_\sigma$.

$$\Phi(\sigma,...,\sigma) = f_0(f_1(\sigma,...,\sigma),...,f_t(\sigma,...,\sigma)) = f_0(\sigma,...,\sigma) = \sigma, \blacksquare.$$

II. Класс самодвойственных функций

Определение: Двойственной к функции $f(x_1,...,x_n)$ называется функция $f^*(x_1,...,x_n) = \bar{f}(\bar{x}_1,...,\bar{x}_n)$. Ясно, что $(f^*)^* = f$, из того, что $g = f^*$, следует, что $f = g^*$.

Если $\tilde{\alpha}_{f(\tilde{x}^n)} = (\alpha_0,...,\alpha_{2^n-1})$, то $\tilde{\alpha}_{f^*(\tilde{x}^n)} = (\bar{\alpha}_{2^n-1},...,\bar{\alpha}_0)$.

1. $(x)^* = x$;
2. $(\bar{x})^* = \bar{x}$;
3. $0^* = 1$;
4. $(x \cdot y)^* = x \vee y$;
5. $(x \oplus y)^* = x \sim y$;
6. $m^*(x,y,z) = m(x,y,z)$;
7. $(x|y)^* = x \downarrow y$

Теорема 11: (принцип двойственности) Пусть

$$\Phi(x_1,...,x_n) = f_0(f_1(x_1^{(1)},...,x_{t_1}^{(1)}),...,f_s(x_1^{(s)},...,x_{t_s}^{(s)})),$$

где $\bigcup_{i=1}^{s}\{x_1^{(i)},...,x_{t_i}^{(i)}\} \subseteq \{x_1,...,x_n\}$. Тогда

$$\Phi^*(x_1,...,x_n) = f_0^*(f_1^*(x_1^{(1)},...,x_{t_1}^{(1)}),...,f_s^*(x_1^{(s)},...,x_{t_s}^{(s)})).$$

Доказательство:

$$\Phi^*(x_1,...,x_n) = \bar{\Phi}(\bar{x}_1,...,\bar{x}_n) =$$
$$= \bar{f}_0(\overline{f_1}(\bar{x}_1^{(1)},...,\bar{x}_{t_1}^{(1)}),...,\overline{f_s}(\bar{x}_1^{(s)},...,\bar{x}_{t_s}^{(s)})) =$$
$$= \bar{f}_0(\bar{f}_1^*(x_1^{(1)},...,x_{t_1}^{(1)}),...,\bar{f}_s^*(x_1^{(s)},...,x_{t_s}^{(s)})) =$$
$$= f_0^*(f_1^*(x_1^{(1)},...,x_{t_1}^{(1)}),...,f_s^*(x_1^{(s)},...,x_{t_s}^{(s)})), \blacksquare.$$

Определение: Функция $f(\tilde{x}^n)$ называется самодвойственной тогда и только тогда, когда

$$f^*(\tilde{x}^n) = f(\tilde{x}^n).$$

Система всех самодвойственных функций обозначается S.

Лежат в S: $x, \bar{x}, x \oplus y \oplus z \oplus const, m(x,y,z)$;
Не лежат в S: $0, 1, x \cdot y, x \vee y, x \oplus y, x \sim y, x \to y, x|y, x \downarrow y$.

Лемма 3: $[S] = S$. (S - замкнутый класс)

Доказательство: Т.к. $x \in S$, то достаточно доказать, что если $f_0, f_1, ..., f_s \in S$, то $\Phi = f_0(f_1, ..., f_s) \in S$. Но по теореме 11:

$$\Phi^* = f_0^*(f_1^*, ..., f_s^*) = f_0(f_1, ..., f_s) = \Phi, \text{ тогда } \Phi \in S, \blacksquare.$$

III. Класс линейных функций

Определение: Функция $f(\tilde{x}^n)$ называется линейной тогда и только тогда, когда

$$f(\tilde{x}^n) = a_0 \oplus a_1 \cdot x_1 \oplus ... \oplus a_n \cdot x_n,$$

где $a_0, a_1, ..., a_n$ лежат в $\{0, 1\}$. (Т.е. в полиноме линейной функции нет монотонных конъюнкций ранга ≥ 2.)

Система всех линейных функций обозначается L.

Лежат в L: $0, 1, x, \bar{x}, x \oplus y, x \sim y$;
Не лежат в L: $x \cdot y, x \vee y, x \to y, x|y, x \downarrow y, m(x,y,z)$.

Лемма 4: $[L] = L$. (L - замкнутый класс)

Доказательство: Т.к. $x \in L$, то достаточно доказать, что если $f_0, f_1, ..., f_s \in L$, то $\Phi = f_0(f_1, ..., f_s) \in L$. Но это следует из определения линейной функции и основных тождеств (дистрибутивность & относительно $\oplus$; коммутативность $\oplus$ и &; $x \cdot x = x$; $x \oplus 0 = x$; $x \oplus x = 0$), $\blacksquare$.

IV. Класс монотонных функций

Определение: Булева функция $f(\tilde{x}^n)$ называется монотонной тогда и только тогда, когда для любых наборов $\tilde{\alpha}$, $\tilde{\beta}$ из B^n таких, что $\tilde{\alpha} \preceq \tilde{\beta}$, справедливо неравенство $f(\tilde{\alpha}) \preceq f(\tilde{\beta})$.

Через M обозначается система всех монотонных булевых функций.

Лежат в M: $0, 1, x, xy, x \vee y, m(x,y,z) = xy \vee yz \vee xz$;
Не лежат в M: $\bar{x}, x \oplus y, x \sim y, x \to y, x|y, x \downarrow y$.

Лемма 5: $[M] = M$ (M - замкнутый класс).

Доказательство: т.к. $x \in M$, то достаточно доказать, что, если $f_0, f_1, ..., f_n$ лежит в M, то $\Phi = f_0(f_1, f_2, ..., f_t) \in M$. $\Phi(x_1, ..., x_n) = f_0(f_1(x_1^{(1)}, ..., x_{q_1}^{(1)}), ..., f_t(x_1^{(t)}, ..., x_{q_t}^{(t)}))$.
Рассмотрим произвольные $\tilde{\alpha}$, $\tilde{\beta}$ из B^n такие, что $\tilde{\alpha} \preceq \tilde{\beta}$, при этом $\tilde{\alpha} = (\alpha_1, ..., \alpha_n)$, $\tilde{\beta} = (\beta_1, ..., \beta_n)$.
Так как $f_0, f_1, ..., f_n$ из M, то

$$f_1(\alpha_1^{(1)}, ..., \alpha_{q_1}^{(1)}), ..., f_t(\alpha_1^{(t)}, ..., \alpha_{q_t}^{(t)}) \preceq f_1(\beta_1^{(1)}, ..., \beta_{q_1}^{(1)}), ..., f_t(\beta_1^{(t)}, ..., \beta_{q_t}^{(t)})$$

Но $f_0 \in M$, тогда

$$f_0(f_1(\alpha_1^{(1)}, ..., \alpha_{q_1}^{(1)}), ..., f_t(\alpha_1^{(t)}, ..., \alpha_{q_t}^{(t)})) \preceq f_0(f_1(\beta_1^{(1)}, ..., \beta_{q_1}^{(1)}), ..., f_t(\beta_1^{(t)}, ..., \beta_{q_t}^{(t)})),$$

т.е.

$$\Phi(\tilde{\alpha}) \leq \Phi(\tilde{\beta}), \blacksquare.$$

Три леммы

Лемма 6: (о несамодвойственной функции) Из любой булевой функции $f(\tilde{x}^n)$, не лежащей в классе S, можно с помощью подстановок вместо переменных $x_1, ..., x_n$ функций $x, \bar{x}$ получить константу.

Доказательство: $f \notin S$, тогда существуют наборы $\alpha_1, \alpha_2, ..., \alpha_n$ из E_2 (из $B = \{0,1\}$):

$$f(\alpha_1, \alpha_2, ..., \alpha_n) = f(\bar{\alpha}_1, \bar{\alpha}_2, ..., \bar{\alpha}_n).$$

Рассмотрим функцию $\varphi(x) = f(x^{\alpha_1}, x^{\alpha_2}, ..., x^{\alpha_n})$.

$$\varphi(0) = f(\bar{\alpha}_1, \bar{\alpha}_2, ..., \bar{\alpha}_n) = f(\alpha_1, \alpha_2, ..., \alpha_n) = \varphi(1),$$

следовательно $\varphi(x) \equiv const$, $\blacksquare$.

Лемма 7: (о немонотонной функции) Из любой булевой функции $f(\tilde{x}^n)$, не лежащей в классе M, можно с помощью подстановок вместо переменных $x_1, ..., x_n$ функций $0, 1, x$ получить функцию $\bar{x}$.

Доказательство: $f \notin M$, тогда существуют наборы $\alpha_1, \alpha_2, ..., \alpha_n$ из E_2 (из $B = \{0,1\}$), такие что $\tilde{\alpha} \preceq \tilde{\beta}$, но $f(\tilde{\alpha}) > f(\tilde{\beta})$, т.е. $f(\tilde{\alpha}) = 1$, а $f(\tilde{\beta}) = 0$. Не ограничивая общности, будем считать что:

$$\tilde{\alpha} = (\underbrace{0, 0, ..., 0}_{l \geq 0}, \underbrace{0, 0, ..., 0}_{m \geq 1}, \underbrace{1, 1, ..., 1}_{r \geq 0})$$
$$\tilde{\beta} = (\underbrace{0, 0, ..., 0}_{l \geq 0}, \underbrace{1, 1, ..., 1}_{m \geq 1}, \underbrace{1, 1, ..., 1}_{r \geq 0})$$

Рассмотрим функцию $\varphi(x) = f(\underbrace{0, 0, ..., 0}_{l \geq 0}, \underbrace{x, x, ..., x}_{m \geq 1}, \underbrace{1, 1, ..., 1}_{r \geq 0})$.

$$\varphi(0) = f(\tilde{\alpha}) = 1 \text{ и } \varphi(1) = f(\tilde{\beta}) = 0,$$

следовательно $\varphi(x) = \bar{x}$, $\blacksquare$.

Утверждение: Если функция $f(\tilde{x}^n) \notin M$, то существуют два соседних набора $\tilde{\alpha}'$, $\tilde{\beta}'$, на которых нарушается монотонность булевой функции $f(\tilde{x}^n)$.

Доказательство: Пусть наборы $\tilde{\alpha}$, $\tilde{\beta}$: $\tilde{\alpha} \preceq \tilde{\beta}$, $f(\tilde{\alpha}) = 1$, $f(\tilde{\beta}) = 0$ - такие же как доказательстве леммы 7. Построим последовательность наборов:

$\tilde{\alpha}^{(i)}$	f				
$\tilde{\alpha} = \tilde{\alpha}^{(0)} = (\overbrace{0,0,...,0}^{l\geq 0},\overbrace{0,0,...,0,0,0}^{m\geq 1},\overbrace{1,1,...,1}^{r\geq 0})$	1	1	1	$\cdots$	1
$\tilde{\alpha}^{(1)} = (0,0,...,0,0,0,...,0,0,1,1,1,...,1)$	0	1			
$\tilde{\alpha}^{(2)} = (0,0,...,0,0,0,...,0,1,1,1,1,...,1)$		0	1		
$\vdots$				$\ddots$	
$\tilde{\alpha}^{(m-1)} = (0,0,...,0,0,1,...,1,1,1,1,1,...,1)$					1
$\tilde{\alpha}^{(m)} = (0,0,...,0,1,1,...,1,1,1,1,1,...,1)$	0	0	0	$\cdots$	0

В цепочке найдутся последовательные наборы $\tilde{\alpha}^{(j)} = \tilde{\alpha}'$ и $\tilde{\alpha}^{(j+1)} = \tilde{\beta}'$ - соседние, нарушается монотонность функции f, ■.

Следствие: Для распознавания монотонности булевой функции $f(\tilde{x}^n)$ достаточно сравнить ее значения на всех парах соседних наборов.

Замечание: Если булева функция $f(\tilde{x}^n)$ задана вектором значений, то то длина входа для распознавания монотонности $f(\tilde{x}^n)$ есть $N = 2^n$, и вычислительная сложность алгоритма распознавания монотонности f есть:

$$O(n \cdot 2^n) = O(N \cdot \log_2 N).$$

Аналогично, вычислительная сложность построения $\tilde{\beta}_f$, как $T(\tilde{\alpha}_f)$, есть $O(N \cdot \log_2 N)$.

Лемма 8: (о нелинейной функции) Из любой булевой функции $f(\tilde{x}^n)$, не лежащей в классе L, можно с помощью подстановок вместо переменных $x_1, ..., x_n$ функций $0, 1, x, \bar{x}, y, \bar{y}$ получить одну из функций $x \cdot y$ или $\overline{x \cdot y}$.

Доказательство: $f \notin L$, тогда в полиноме Жегалкина функции f есть конъюнкция двух (или большего числа) переменных. Не ограничивая общности, будем считать, что там есть конъюнкция, соединяющая $x_1 \cdot x_2$. Преобразуем P к виду:

$$P = x_1 \cdot x_2 \cdot P_0(x_3, ..., x_n) \oplus x_1 \cdot P_1(x_3, ..., x_n) \oplus x_2 \cdot P_2(x_3, ..., x_n) \oplus P_3(x_3, ..., x_n).$$

Ясно, что по теореме о единственности полинома $P_0(x_3, ..., x_n) \not\equiv 0$. Следовательно существуют $\alpha_3, ..., \alpha_n$ (из $\{0, 1\}$) такие, что $P_0(x_3, ..., x_n) = 1$.
Рассмотрим $\psi_1(x, y) = f(x, y, \alpha_3, ..., \alpha_n) = xy \oplus ax \oplus by \oplus c$.
Теперь рассмотрим $\psi(x, y)$:

$$\psi(x, y) = \psi_1(x \oplus b, y \oplus a) = (x \oplus b)(y \oplus a) \oplus a(x \oplus b) \oplus b(y \oplus a) \oplus c =$$
$$= xy \oplus \underline{ax} \oplus \underline{\underline{by}} \oplus \underbrace{ab} \oplus \underline{ax} \oplus \underbrace{ab} \oplus \underline{\underline{by}} \oplus ab \oplus c =$$
$$= xy \oplus (ab \oplus c) = \begin{cases} x \cdot y, & ab \oplus c = 0; \\ \overline{x \cdot y}, & ab \oplus c = 1. \end{cases}, \blacksquare.$$

Теорема 12: (теорема Поста о полноте *или* критерий полноты в P_2) Система булевых функций Q полна в P_2 тогда и только тогда, когда Q целиком **не** содержится ни в одном из пяти замкнутых классов T_0, T_1, L, M, S.

Доказательство: Необходимость: Если $Q \subseteq K$, где $K = \{T_0, T_1, L, M, S\}$, то $[Q] \subseteq [K] =$ $= \{\text{по леммам 2 - 5}\} = K \subset P_2$, т.е. $[Q] \neq P_2$, Q - неполная система.

Достаточность: Пусть Q не содержится ни в одном 5 классов T_0, T_1, L, M, S, тогда в Q имеется 5 (не обязательно неравных друг другу) функций: $f_0 \notin T_0, f_1 \notin T_1, f_l \notin L, f_m \notin M, f_s \notin S$. Докажем полноту Q в P_2, сведя по теореме 8 подсистему $\{f_0, f_1, f_l, f_m, f_s\} = \hat{Q}$ системы Q к полной системе $Q_3 = \{xy, \bar{x}\}$.

I этап. Получение констант: Рассмотрим $f_0 \notin T_0$. Положим, $\varphi_0(x) = f_0(x, x, ..., x)$. Ясно, что $\varphi_0(0) = f_0(0, 0, ..., 0) = 1$.

Случай 1). Пусть $f_0(1, 1, ..., 1) = 0$, тогда $\varphi_0(1) = 0$, следовательно $\varphi(x) \equiv \bar{x}$. Но по лемме 6 о несамодвойственной функции из $f_s \notin S$ с помощью подстановок $x, \bar{x} = \varphi_0(x)$ можно получить какую-то константу $\sigma \in \{0, 1\}$. Следовательно, $\varphi_0(\sigma) = \bar{\sigma}$ - получены обе константы.

Случай 2). Пусть $f_0(1, 1, ..., 1) = 1$, тогда $\varphi_0(1) = 1$, следовательно $\varphi(x) \equiv 1x$. Тогда $f_1(\varphi_0(x), ..., \varphi_0(x)) \equiv$ $f_1(1, 1, ..., 1) \equiv 0$, т.к. $f_1 \notin T$.

II этап. Получение $\bar{x}$: По лемме 7 о немонотонной функции из $f_m \notin M$ с помощью $0, 1, x$.

III этап. Получение $x \cdot y$: По лемме 8 о нелинейной функции из $f_l \notin L$ с помощью $0, 1, x, \bar{x}, y, \bar{y}$ получим $x \cdot y$ или $\overline{x \cdot y}$, в последнем случае $x \cdot y = (\overline{\overline{x \cdot y}})$.

Теорема доказана, ■.

Предполные классы

Определение: Система функций Q ($Q \subseteq P_2$) - предполный класс тогда и только тогда, когда:

1. $[Q] \subset P_2$;
2. $\forall f, f \notin Q : [Q \cup \{f\}] = P_2$.

Лемма #: Каждый из 5 замкнутых классов T_0, T_1, L, M, S целиком не содержится ни в одном из 4 остальных.

Доказательство:

$f \notin K$ / $f \in K$	T_0	T_1	L	M	S
T_0	$\times$	0	$x \cdot y$	$x \oplus y$	0
T_1	1	$\times$	$x \cdot y$	$x \sim y$	1
L	1	0	$\times$	$x \oplus y$	1
M	1	0	$x \cdot y$	$\times$	1
S	$\bar{x}$	$\bar{x}$	m	$\bar{x}$	$\times$

Пример построен, ■.

Теорема 13: (о предполных классах) В P_2 имеется ровно 5 предполных классов: T_0, T_1, L, M, S.

Доказательство: Пусть $K \in \{T_0, T_1, L, M, S\}$. Докажем, что K - предполный класс.

а) по лемме # и леммам 2 - 5 имеем, что [K] $= K \subset P_2$.

б) по лемме # K не содержится ни в одном из 4 остальных классов из множества $\{T_0, T_1, L, M, S\}$, тогда для любой $f, f \notin K$ система $K \cup \{f\}$ не содержится ни в одном из 5 классов T_0, T_1, L, M, S, следовательно по теореме Поста эта система полна в P_2, т.е. $[K \cup \{f\}] = P_2$.

Теперь докажем, что других предполных классов нет. От противного: пусть K' - предполный класс, отличающий от 5 остальных. Возможны два случая:

Случай 1: K' целиком содержится в K ($K' \subset K$), где $K \in \{T_0, T_1, L, M, S\}$, тогда существует $f : f \in K \backslash K'$, тогда $[K' \cup \{f\}] \subseteq [K] =$ по леммам 2-5 $= K \subset P_2$, следовательно K' - не предполный класс.

Случай 2: K' целиком не содержится ни в одном из 5 классов T_0, T_1, L, M, S. Тогда по теореме Поста $[K'] = P_2$, это означает, что K' - не предполный класс, ■.

Базисы в P_2

Определение: Система булевых функций Q ($Q \subseteq P_2$) называется *[функциональным]* базисом в P_2 тогда и только тогда, когда:

1. $[Q] = P_2$;
2. $\forall Q', Q' \subset Q : [Q'] \neq P_2$.

Теорема 14: (о максимальном числе функций в базисе алгебры логики) Максимальное число функций в базисе в P_2 равно 4.

Доказательство: Из теоремы Поста следует, что из любой полной в P_2 системы булевых функций Q можно выделить полную подсистему из не более, чем 5 функций:

$$f_0 \notin T_0; f_1 \notin T_1; f_l \notin L; f_m \notin M; f_s \notin S.$$

1. Верхняя оценка: Рассмотрим $f_0 \notin T_0$. $f_0(0,0,...,0) = 1$. Возможны два случая:

Случай 1: $f_0(1,1,...,1) = 0$, следовательно $f_0 \notin M$ и $f_0 \notin T_1$, тогда по теореме Поста система $\{f_0, f_l, f_s\}$ полна в P_2.

Случай 2: $f_0(1,1,...,1) = 1$, следовательно $f_0 \notin S$, тогда по теореме Поста система $\{f_0, f_1, f_l, f_m\}$ полна в P_2.

2. Нижняя оценка: Рассмотрим систему функций $\hat{Q} = \{x \cdot y, x \oplus y \oplus z, 0, 1\}$
Критериальная таблица:

f \ K	T_0	T_1	L	M	S
$x \cdot y$	+	+	−	+	−
$x \oplus y \oplus z$	+	+	+	−	+
0	+	−	+	+	−
1	−	+	−	+	−

"+" показывает, что $f \in K$, "−" показывает, что $f \notin K$.
По теореме Поста система $\hat{Q}$ полна так как:

$$x \cdot y \notin L; x \oplus y \oplus z \notin M; 0 \notin T_1 \cup S; 1 \notin T_0.$$

Кроме этого:

$$\hat{Q} \backslash \{1\} \subseteq T_0; \hat{Q} \backslash \{0\} \subseteq T_1; \hat{Q} \backslash \{x \oplus y \oplus z\} \subseteq M; \hat{Q} \backslash \{x \cdot y\} \subseteq L.$$

Следовательно, $\hat{Q}$ - базис из 4 функций в P_2, ■.

Функции k-значной логики (k-значные функции)

Определим, что $k \geq 3$. $E_k = \{0, 1, ..., k-1\}$.

Определение: k-значной функцией называется всякая функция следующего вида:

$$f(x_1, ...x_n) : E_k^n \to E_k$$

Как и в случае с алгеброй логики определяются: лексикографический порядок, формула над Q, таблица функции f, замыкание, замкнутые классы, полная система, существенные и фиктивные переменные, предполный класс, базис и др.

P_k - множество k-значных функций.
$P_k(n)$ - множество k-значных функций от переменных $x_1, x_2, ..., x_n$.

Теорема 15: $|P_k(n)| = k^{k^n}.(n \in \mathbb{N})$.

Доказательство: Аналогично доказательству теоремы 1, ■.

Обозначение: $a_1 \equiv a_2(mod\ k) \Leftrightarrow a_1 - a_2 \vdots k$.

Пусть $a \in \mathbb{N}, k \in \mathbb{N}$. Тогда $r = \underbrace{(a\ mod\ k)}_{\substack{\text{остаток от} \\ \text{деления a на k}}}$ тогда и только тогда, когда: $\begin{cases} r \in \{0, 1, ..., k\} \\ r \equiv a(mod\ k) \end{cases}$

Элементарные k-значные функции

1. $0, 1, ..., k-1$ - константы;
2. x - тождественная функция;
3. $g_i^n(x_1, ..., x_i, ...x_n) = x_i$ - селекторная функция;
4. $\bar{x} = ((x+1)\ mod\ k)$ - отрицание Поста;
5. $\sim x = N_x = (k-1) - x$ - отрицание Лукасевича;
6. $min(x, y)$; (является аналогом конъюнкции в P_2)
7. $max(x, y)$; (является аналогом дизъюнкции в P_2)
8. $x + y; x \cdot y$ - сложение и умножение по модулю k;
9. $j_\sigma(x) = \begin{cases} 1, & \text{при } x = \sigma \\ 0, & \text{при } x \neq \sigma \end{cases}$
10. $J_\sigma(x) = \begin{cases} k-1, & \text{при } x = \sigma \\ 0, & \text{при } x \neq \sigma \end{cases}$
11. $x - y = \begin{cases} x - y, & \text{при } 0 \leq y \leq x \leq k-1 \\ 0, & \text{при } 0 \leq x < y \leq k-1 \end{cases}$ - усеченная разность;
12. $x \supset y = (k-1) - (x - y)$ - импликация;
13. $V_k(x, y) = \overline{max(x, y)}$ - функция Вебба.

Простейшие тождества

1. Коммутативность $min, max, +, \cdot$;
2. Ассоциативность $min, max, +, \cdot$ (поэтому будут допустимы многоместные функции min и max, а также суммы и произведения);
3. Дистрибутивность min относительно max, max относительно min, $\cdot$ относительно $+$;
4. $\sim max(x, y) = min(\sim x, \sim y)$;
   $\sim min(x, y) = max(\sim x, \sim y)$;

Лемма 9: Пусть $a_1 = q_1k + r_1$, $a_2 = q_2k + r_2$, где $a_1, a_2, q_1, q_2 \in \mathbb{Z}$, $k \in \mathbb{N}$, $r_1, r_2 \in \{0, 1, ..., k-1\}$. Тогда:

$$a_1 \pm a_1 \equiv r_1 \pm r_2 (mod\ k);$$

$$a_1 \cdot a_1 \equiv r_1 \cdot r_2 (mod\ k).$$

Доказательство: 1) $(a_1 \pm a_2) - (r_1 \pm r_2) = k(q_1 \pm q_2) \vdots k \Rightarrow a_1 \pm a_1 \equiv r_1 \pm r_2 (mod\ k)$

2) $a_1 \cdot a_2 - r_1 \cdot r_2 = (q_1k + r_1) \cdot (q_2k + r_2) - r_1 \cdot r_2 = k(q_1q_2k + q_1r_2 + q_2r_1) \vdots k \Rightarrow a_1 \cdot a_1 \equiv r_1 \cdot r_2 (mod\ k)$

Теорема 16: (разложение функции из P_k в I форму) Пусть $f(\tilde{x}^n) \in P_k$. Тогда:

$$f(\tilde{x}^n) = \max_{\tilde{\sigma}=\{\sigma_1,...,\sigma_n\} \in E_k^n} \min(J_{\sigma_1}(x_1), J_{\sigma_2}(x_2), ..., J_{\sigma_n}(x_n), f(\tilde{\sigma})) \text{ - I форма.} \quad (*)$$

Доказательство: Рассмотрим произвольный набор $\tilde{\alpha}^n = (\alpha_1, \alpha_2, ..., \alpha_n) \in E_2^k$.
В левой части $(*)$ на $\tilde{\alpha} : f(\tilde{\alpha})$. Теперь рассмотрим правую часть $(*)$ на $\tilde{\alpha}$:

Случай 1: $\tilde{\sigma} = \tilde{\alpha} \Rightarrow \sigma_1 = \alpha_1, ..., \sigma_n = \alpha_n$, тогда $J_{\sigma_i}(\alpha_i) = k - 1$, где $i = \overline{1, n}$, следовательно

$$\min(J_{\sigma_1}(\alpha_1), ..., J_{\sigma_n}(\alpha_n), f(\tilde{\sigma})) = f(\tilde{\alpha})$$

Случай 2: $\tilde{\sigma} \neq \tilde{\alpha} \Rightarrow \exists i \in \{1, ..., n\} : \sigma_i \neq \alpha_i$, тогда $J_{\sigma_i}(\alpha_i) = 0$, следовательно

$$\min(J_{\sigma_1}(\alpha_1), ..., J_{\sigma_n}(\alpha_n), f(\tilde{\sigma})) = 0$$

Итак, правая часть $(*)$ на $\tilde{\alpha}$:

$$\max(0, ..., 0, f(\tilde{\alpha}), 0, ..., 0) = f(\tilde{\alpha})$$

и в силу произвольности выбора $\tilde{\alpha}$ теорема доказана, ■.

Теорема 17: (разложение функции из P_k в II форму) Пусть $f(\tilde{x}^n) \in P_k$. Тогда:

$$f(\tilde{x}^n) = \sum_{\tilde{\sigma}=\{\sigma_1,...,\sigma_n\} \in E_k^n} j_{\sigma_1}(x_1) \cdot j_{\sigma_2}(x_2) \cdot ... \cdot j_{\sigma_n}(x_n) \cdot f(\tilde{\sigma}) \text{ - II форма.} \quad (**)$$

Доказательство: Рассмотрим произвольный набор $\tilde{\alpha}^n = (\alpha_1, \alpha_2, ..., \alpha_n) \in E_2^k$.
В левой части $(**)$ на $\tilde{\alpha} : f(\tilde{\alpha})$. Теперь рассмотрим правую часть $(**)$ на $\tilde{\alpha}$:

Случай 1: $\tilde{\sigma} = \tilde{\alpha} \Rightarrow \sigma_1 = \alpha_1, ..., \sigma_n = \alpha_n$, тогда $j_{\sigma_i}(\alpha_i) = 1$, где $i = \overline{1, n}$, следовательно

$$j_{\sigma_1}(x_1) \cdot j_{\sigma_2}(x_2) \cdot ... \cdot j_{\sigma_n}(x_n) \cdot f(\tilde{\sigma}) = f(\tilde{\alpha})$$

Случай 2: $\tilde{\sigma} \neq \tilde{\alpha} \Rightarrow \exists i \in \{1, ..., n\} : \sigma_i \neq \alpha_i$, тогда $j_{\sigma_i}(\alpha_i) = 0$, следовательно

$$j_{\sigma_1}(x_1) \cdot j_{\sigma_2}(x_2) \cdot ... \cdot j_{\sigma_n}(x_n) \cdot f(\tilde{\sigma}) = 0$$

Итак, правая часть $(**)$ на $\tilde{\alpha}$:

$$0 + ... + 0 + f(\tilde{\alpha}) + 0 + ... + 0 = f(\tilde{\alpha})$$

и в силу произвольности выбора $\tilde{\alpha}$ теорема доказана, ■.

Из теорем 16, 17 вытекает следующее утверждение:

Теорема 18: (о существовании в P_k конечных полных систем) Каждая из систем функций:

$$\{0, 1, ..., k-1, J_0(x), ..., J_{k-1}(x), \min(x, y), \max(x, y)\} \text{ (система Россера-Туркетта)}$$
$$\text{и } \{0, 1, ..., k-1, j_0(x), ..., j_{k-1}(x), x + y(mod;\ k), x \cdot y(mod;\ k)\}$$

является полной системой в P_k $(k \geq 3)$.

$x^s = x \cdot ... \cdot x (mod\ k)$ - s-ая степень переменной.

Определение: Моном - выражение вида:

$$a \cdot x_{i_1}^{s_1} \cdot x_{i_2}^{s_2} \cdot ... \cdot x_{i_t}^{s_t} (mod\ k),$$

где $i_j \neq i_l$ при $j \neq l$ и $a \in E_k$.

Определение: Полином (по $mod\ k$) - сумма по $mod\ k$ различных (без учета коэффициентов) мономов.

Вопрос: при каких k ($k \geq 3$) полна в P_k система полиномов?
Можно сформулировать вопрос иначе: когда $[\{0, 1, ..., k-1, x + y (mod\ k), x \cdot y (mod\ k)\}] = P_k$?

Лемма 10: Пусть $l, p \in \mathbb{N}$, p - простое, НОД$(l, p) = 1$. Тогда числа $l, 2l, ..., (p-1)l$ принимают по $(mod\ p)$ все $p-1$ различных остатков из множества $\{1, 2, ..., p-1\}$.

Доказательство: Ясно, что при любом $j \in \{1, 2, ..., p-1\}$ число $j \cdot l$ не кратно p, следовательно среди искомых остатков нет 0.
Осталось доказать, что все остатки по $mod\ p$ чисел $1, 2, ..., p-1$ попарно различны. Пусть, это не так, и существуют j_1, j_2 ($1 \leq j_1 < j_2 \leq p-1$) такие, что $j_1 \cdot l \equiv j_2 \cdot l (mod\ p)$, тогда $(j_2 - j_1)l \vdots p$, что невозможно, т.к. $j_2 - j_1 \in \{1, ..., p-1\}$, p - простое и НОД$(p, l) = 1$, ■.

Теорема 19: (малая теорема Ферма) Пусть $l, p \in \mathbb{N}$, p - простое, НОД$(l, p) = 1$. Тогда

$$l^{(p-1)} \equiv 1 (mod\ p).$$

Доказательство: По леммам 9 и 10 получается, что

$$l \cdot (2l) \cdot (3l) \cdot ... \cdot ((p-1)^l) \equiv 1 \cdot 2 \cdot ... \cdot (p-1) (mod\ p)$$

$$l^{(p-1)} \cdot (p-1)! \equiv (p-1)! (mod\ p) \Rightarrow (l^{(p-1)} - 1) \cdot (p-1)! \vdots p \overset{p \text{ - простое}}{\Rightarrow}$$
$$\overset{p \text{ - простое}}{\Rightarrow} (l^{(p-1)} - 1) \vdots p \Rightarrow l^{(p-1)} \equiv 1 (mod\ p),\ ■.$$

Теорема 20: Система всех полиномов полна в P_k тогда и только тогда, когда k ($k \geq 3$) - простое число. (при $k = 2$ также верно.)

Доказательство: **1.** $k = p$, где p - простое число, $p \geq 3$. По теореме 17 достаточно доказать, что все функции $j_0(x), j_1(x), ..., j_{p-1}(x)$ представимы полиномами по $mod\ p$.

Заметим, что $j_\sigma(x) = j_0(x - \sigma)$, тогда, т.к. $(x - \sigma)$ - полином, достаточно доказать, что $j_0(x)$ представимо полиномом. По малой теореме Ферма $j_0(x) = 1 = 1 - 0^{(p-1)}$.

Действительно, $j_0(0) = 1 = 1 - 0^{(p-1)}$ - верно, а при $x = l$, $l \in \{1, ..., p-1\}$ (т.к. НОД$(l, p) = 1$): $j_0(x) = 1 = 1 - 0^{(p-1)}$ - верно.

Т.е. при $k = p$, где p - простое,

$$[\{0, 1, ..., k-1, x + y (mod\ k), x \cdot y (mod\ k)\}] = P_k,$$

и каждая функция f $(f_{\in}P_k)$ представима полиномом.

2. k - составное число, тогда пусть k представимо в виде: $k = k_1 \cdot k_2$, где $1 < k_1 < k, k_1 \in \mathbb{N}$. Докажем, что функция $j_0(x)$ не представима в полиномом по $mod\ k$.

Пусть, это не так, тогда $j_0(x) = b_0 + b_1x + b_2x^2 + ... + b_sx^s(mod\ k)$, где $b_i \in E_k$ при $j = \overline{0,s}, s \in \mathbb{N} \cup \{0\}$. При $x = 0$ имеем: $b_0 = 1$. Подставим $x = k_1$: $0 = j_0(k_1) = 1 + b_1k_1 + b_2k_1^2 + ... + b_sk_1^s(mod\ k)$. Тогда $k - 1 \equiv k_1 \cdot \underbrace{(b_1 + b_2k_1 + ... + b_sk_1^{s-1})}_{A}(mod\ k) \Rightarrow ((k-1) - k_1A) \vdots k \Rightarrow ((k-1) - k_1A) \vdots k_1 \Rightarrow (k-1) \vdots k$,

но и $k \vdots k_1$, $k_1 > 1$, противоречие (?!), $\blacksquare$.

Глава 2

Введение в теорию графов

Определение: Псевдограф (граф общего вида) есть пара объектов (V, E), где V - множество, элементы которого называются вершинами (*vertex*) псевдографа, а E - совокупность пар элементов из V, называемых ребрами (*edge*) псевдографа.

Обычно пишут: $G = (V, E)$. Будем использовать запись $V(G)$, $E(G)$, если требуется уточнить, что V и E - для G.

Определение: Если все ребра - неупорядоченные пары вершин, то псевдограф G - неориентированный. О ребре $e = (v, w)$ говорят, что e соединяет вершины v и w; v и w - концы ребра e.

Определение: Ребра вида (v, v) называют петлей.

Определение: Одинаковые ребра в E называют кратными.

Определение: Если все ребра - упорядоченные пары вершин, то псевдограф G - ориентированный (псевдоорграф). Каждое ребро называется дугой. О дуге $e = (v, w)$ говорят, что e ведет из v в w; исходит из v и заходит в w; v - начало дуги e, w - конец дуги e.

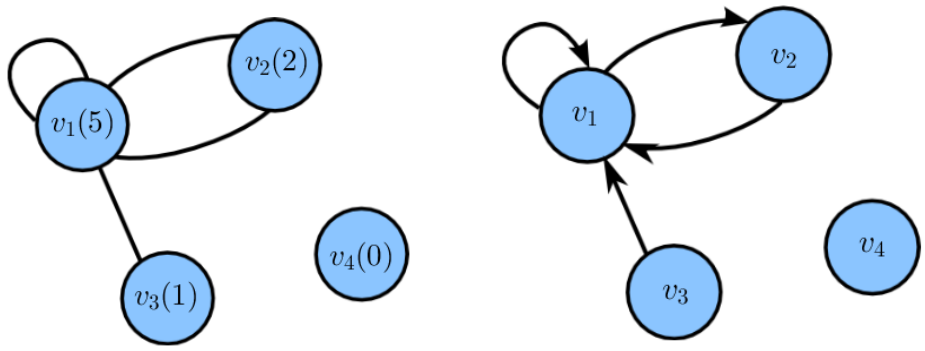
Определение: Мультиграфы - псевдографы, в которых не допускаются петли.

Определение: Простые графы - мультиграфы, в которых не допускаются кратные ребра.

Определение: Псевдограф называется конечным, если $V(G)$ и $E(G)$ - конечные.

Определение: Степень вершины v в G - число $\deg v$ концов ребер, сосредоточенных в v (т.е. каждое смежное с v, отличное от петли, ребро учитывается 1 раз, а каждая петля - 2 раза).

Пример: $G = (V, E)$ $V = \{v_1, v_2, v_3, v_4\}$ $E = \{(v_1, v_2), (v_1, v_1), (v_2, v_1), (v_3, v_1)\}$



Определение: Полустепень исхода (захода) вершины v в псевдограф G - число $\deg^+ v$ ($\deg^- v$) дуг, исходящих из v (заходящих в v).

$$\deg v = \deg^+ v + \deg^- v$$

Теорема 1: (теорема Эйлера о степенях вершин *или* лемма о рукопожатиях) Пусть $G = (V, E)$ - конечный псевдограф; $V = \{v_1, ..., v_p\}$. Тогда

$$\sum_{i=1}^{p} \deg v_i = 2|E|$$

Доказательство: следует из того, что в этом равенстве слева и справа подсчитываются концы ребер в G, ■.

Следствие: В любом псевдографе число вершин нечетной степени четно.

Определение: Пусть $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$ - псевдографы. Говорят, что G_1 и G_2 изоморфные (обозначение: $G_1 \cong G_2$) тогда и только тогда, когда существуют такие взаимооднозначные отображения

$$\varphi : V_1 \to V_2 \text{ и } \psi : E_1 \to E_2,$$

что для любого ребра e (пусть $e = (v, w)$) из E_1 имеет место равенство:

$$\psi(e) = (\varphi(v), \varphi(w)).$$

Пусть $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$ - простые графы. $G_1 \cong G_2$ тогда и только тогда, когда существует взаимнооднозначное отображение $\varphi : V_1 \to V_2$, сохраняющее смежность и несмежность вершин.

Определение: Отображение φ называется изоморфизмом G_1 и G_2.

Определение: Изоморфизм псевдографа на себя называется автоморфизмом.

Определение: Пусть $G = (V, E)$ - конечный псевдограф; $V = \{v_1, v_2, ..., v_p\}$. Матрицей смежности называется матрица $A(G) = [a_{ij}]_{p \times p}$, где a_{ij} - число ребер, концами которых являются v_i и v_j.

Определение: Путем в псевдографе G называется всякая последовательность вида:

$$P = v_{i_0}, (v_{i_0}, v_{i_1}), v_{i_1}, (v_{i_1}, v_{i_2}), ..., v_{i_{e-1}}, (v_{i_{e-1}}, v_{i_e}), v_{i_e}.$$

P состоит из вершин и ребер G. Говорят, что путь P, указанного вида, соединяет v_{i_0} и v_{i_e}.

Определение: Длиной пути P называется число $l(P)$ ребер в нем.

Определение: Путь P называется незамкнутым тогда и только тогда, когда $v_{i_0} \neq v_{i_e}$.

Определение: Незамкнутый путь без повторов ребер - цепь, без повторов вершин - простая цепь.

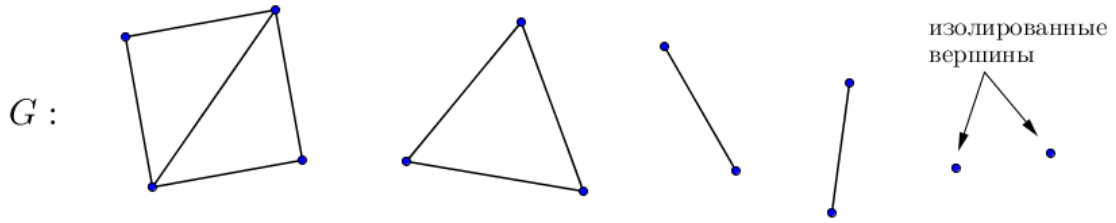
Определение: Замкнутый путь без повторов ребер - цикл, без повторов вершин, за исключением совпадения концов пути, - простой цикл.

Определение: Псевдограф G - связный тогда и только тогда, когда любые две его вершины можно соединить в G.

Определение: Пусть $G = (V, E)$, $G' = (V', E')$ - псевдографы. Говорят, что псевдограф G' - подграф псевдографа G тогда и только тогда, когда $V' \subseteq V$ и $E' \subseteq E$.

Определение: Компонента связности псевдографа G - всякий из максимальных по включению вершин и ребер связных подграфов псевдографа G (*иными словами:* некоторый подграф такой, что для любых двух вершин этого подграфа существует путь из одной в другую, и не существует пути из вершины этого подграфа в вершину не из этого подграфа).

Пример:



6 компонент связности

Число вершин, ребер, компонент связности псевдографа G будем обозначать $p(G)$, $q(G)$, $c(G)$ соответственно.

Теорема 2: Пусть $G = (V, E)$ - псевдограф; $V = \{v_1, v_2, ..., v_p\}$; $A = A(G)$ - его матрица смежности. Тогда для любого $l \in \mathbb{N}$ и любых $i, j \in \{1, ..., p\}$ элемент $a_{ij}^{(l)}$ матрицы $A^l = [a_{ij}^{(l)}]_{p \times p}$ равен числу путей длины l, соединяющих вершины v_i и v_j в G.

Доказательство: индукция по l
Базис: $l = 1$ - очевидно
Предположение: Пусть верно для l. Докажем для $l + 1$.
Шаг: $a_{ij}^{(l+1)} = \sum_{r=1}^{p} \underbrace{a_{ir}^{(l)}}_{(*)} \underbrace{a_{rj}}_{(**)}$ - число путей длины $l + 1$, соединяющие v_i и v_j
$(*)$ - число путей длины l, соединяющие v_i и v_r
$(**)$ - число путей длины 1, соединяющие v_j и v_r, ■.

Следствие: Пусть в теореме 2 $l = p - 1$, а вместо суммы и произведения - дизъюнкция и конъюнкция, и пусть в матрице смежности факт смежности вершины отмечается 1 (кратные ребра не учитываются). Тогда $a_{ij}^{(p-1)} = 1$ тогда и только тогда, когда v_i и v_j лежат в одной компоненте связности.

Замечание: В последнем случае построение матрицы $A^{(p-1)}$ имеет сложность $O(p^3 \log p)$.

В этой части курса будем сокращать "конечный простой граф"до "граф".

Лемма 1: Пусть $G = (V, E)$ - граф, P - незамкнутый путь в G, соединяющий v и w. Тогда из P можно выделить простую цепь, соединяющую v и w.

Доказательство: Если P - простая цепь, то она - искомая (в частности, если $l(P) = 1$). В остальных случаях воспользуемся индукцией по $l(p)$. Базис очевидно верен. Пусть для $l(P) \leq l'$ утверждение верно, докажем его для P, отличных от простой цепи, и такого, что $l(p) = l' + 1$.

$P = vP'uP''uP'''w$, тогда пусть $\hat{P} = vP'uP'''w$, соединяющий v и w и удовлетворяющий предположению индукции. Следовательно, из $\hat{P}$ можно выделить искомую простую цепь, ■.

Лемма 2: Пусть $G = (V, E)$ - связный псевдограф, $e = (v, w) \notin E$, тогда при добавлении ребра e к графу G в полученном псевдографе будет цикл.

Доказательство: G - связный, тогда по лемме 1 существует простая цепь P, соединяющая v и w в G, следовательно при добавлении ребра e к цепи P получится простой цикл, ■.

Лемма 3: Пусть $G = (V, E)$ - связный псевдограф, $e = (v, w)$ - ребро, принадлежащее некоторому циклу в G, тогда при удалении ребра e из G получится связный псевдограф.

Доказательство: Рассмотрим произвольные вершины u', u'' из V. G - связный, тогда по лемме 1 существует простая цепь P в G, соединяющая u' и u''.

Случай 1: $e \notin P$, тогда в $G' = G - e$ вершины u' и u'' связаны путем.

Случай 2: $e \in P$, тогда т.к. e лежит в цикле Z, то заменим ребро e на дополняющую e часть цикла Z, следовательно в G' вершины u' и u'' связаны путем. Таким образом G' - связный, ■.

Лемма 4: Пусть $G = (V, E)$ - псевдограф с p вершинами, q ребрами и c компонентами связности. Тогда $c \geq p - q$, а если G без циклов, то $c = p - q$.

Доказательство: Пусть $G' = (V', E')$, $G'' = (V', E' \cup \{e\}) = G' + e$, где $e \notin E'$.

Случай 1: e соединяет вершины из одной компоненты связности в G', тогда $c(G'') = c(G')$.

Случай 2: e соединяет вершины из различных компонент в G', тогда $c(G'') = c(G') - 1$.

В любом случае $c(G'') \geq c(G') - 1$.

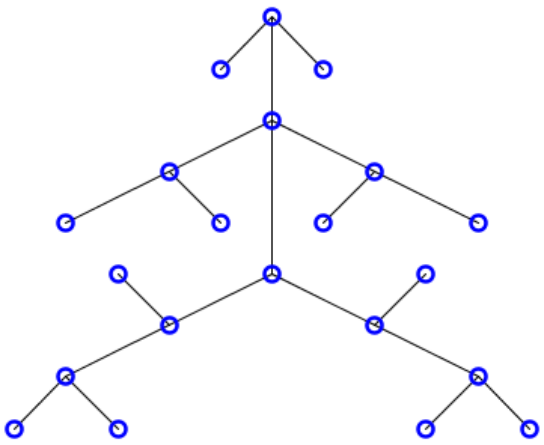
Граф G получается из $G_0 = (V, \varnothing)$ последовательным добавлением всех q ребер, тогда

$$c(G) \geq c(G_0) - q = p - q.$$

Если в G нет циклов, то случай 1 невозможен (по лемме 2). Тогда $c = p - q$, ■.

Деревья

Определение: Дерево - связный граф без циклов (в том числе $G = (\{v\}, \varnothing)$ - дерево).



Утверждение: (следствие из леммы 4) В дереве с p вершинами число ребер равно $p-1$.

Теорема 3: (об эквивалентных определениях) Пусть $G=(V,E)$ - конечный псевдограф. Тогда следующие утверждения эквивалентны:

1. G - дерево;
2. G - без циклов и $q=p-1$;
3. G - связный и $q=p-1$;
4. G - связный, но при удалении любого ребра связность теряется;
5. G - без циклов, но при добавлении одного ребра появляется цикл.

Доказательство: Схема доказательства: $1\Rightarrow 2\Rightarrow 3\Rightarrow 4\Rightarrow 5\Rightarrow 1$
$1\Rightarrow 2$: По лемме 4.
$2\Rightarrow 3$: По лемме 4 (2-ая часть): $1=p-q=c$.
$3\Rightarrow 4$: Пусть $e\in E$, $G'=G-e$, тогда $p(G')=p$, $q(G')=q-1$, и тогда по лемме 4
$c(G')\geq p(G')-q(G')=p-q+1$, следовательно G' - несвязный.
$4\Rightarrow 5$: Без циклов: от противного по лемме 3. $G+e$ содержит цикл по лемме 2.
$5\Rightarrow 1$: Пусть G - несвязный, тогда при добавлении ребра, соединяющего вершины из разных компонент, цикл не возникнет - противоречие, ■.

Определение: Граф $G'=(V',E')$ называется остóвным деревом (псевдо)графа $G=(V,E)$ тогда и только тогда, когда G' - дерево, $V'=V$ и G' - подграф G.

Теорема 4: В псевдографе G имеется хотя бы одно остовное дерево тогда и только тогда, когда G связный.

Доказательство: $\Rightarrow$: Пусть G несвязный, тогда очевидно, что нет остовных деревьев.
$\Leftarrow$: Пусть G связный. Положим $G''=G$. Если G'' - дерево, то утверждение доказано. Если нет, то G'' - связный граф с циклом Z, следовательно существует ребро $e\in Z$ и по лемме 3 $G'''=G''-e$ - связный. Положим $G''=G'''$, повторим рассуждения. Число таких рассуждений конечное, т.к. в G конечное число циклов, ■.

Пусть $w: E\to\mathbb{R}$, если $e\in E$, то $w(e)$ - вес ребра e.
Пусть $G(V,E)$ - конечный псевдограф, тогда вес G определяется как:

$$w(G)=\sum_{e\in E} w(e).$$

Задача: (о поиске минимального остовного дерева) Найти в связном конечном взвешенном (по ребрам) псевдографа G остовное дерево наименьшего веса.

Решение: На первом шаге выбираем пустой граф $G_0=(V,\varnothing)$, где $(V,E)=G$. Пусть за первые i шагов построим граф $G_{i-1}(V,E_{i-1})$ $(E_{i-1}\subseteq E, E_0=\varnothing, |E_{i-1}=i-1|)$. Опишем $i+1$ шаг:

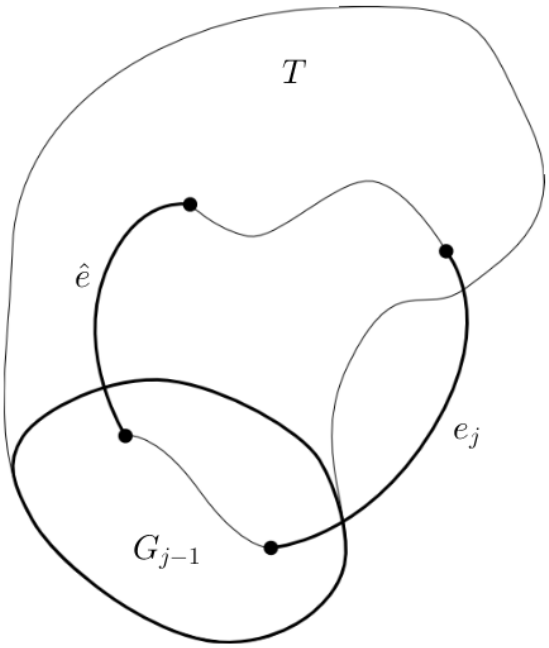
Стратегия 1: (алгоритм Крускала) добавляется ребро минимального веса, не порождающее циклов в графе $G_i=G_{i-1}+e$.

Стратегия 2: (алгоритм Прима) добавляется ребро минимального веса, не порождающее циклов в графе $G_i=G_{i-1}+e$ и такое, что все ребра G_i лежат в одной компоненте связности.

Теорема 5: Каждая отдельно взятая стратегия (1 или 2) приводит на шаге $i = |V|$ к подграфу, являющегося остовным деревом наименьшего веса.

Доказательство: Пусть это не так, тогда существует шаг j такой, что G_{j-1} содержится в некотором остовным деревом минимального веса, а G_j уже не содержится (G_0 содержится точно!).

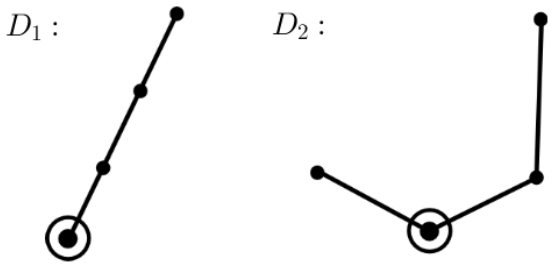
Пусть $G_j = G_{j-1} + e_j$ и пусть T - то остовное дерево G, подграфом которого является G_{j-1}. Рассмотрим $\hat{T} = T + e_j$ - в T точно имеется цикл по лемме 2 (ровно 1), следовательно в этому цикле имеется ребро $\hat{e}$, не лежащее в G_{j-1}, но смежное с о дним из ребер G_{j-1}. Но $w(e_j) \leq w(\hat{e})$ (в силу выбора e_j).



Рассмотрим $T' = T - \hat{e} + e_j$. T' - остовное дерево G, $w(T') = w(T) - w(\hat{e}) + w(e_j) \leq w(T)$, следовательно G_j содержится в остовном дереве T' минимального веса, противоречие (?!), ■.

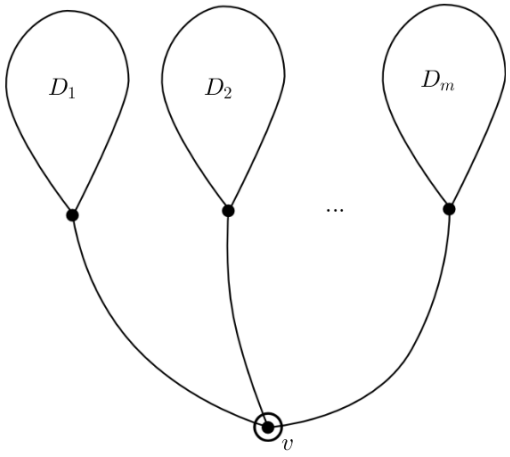
Корневые деревья

Определение: Корневое дерево - это дерево с выделенной вершиной, называемой корнем.
Обозначение: $D = (G, v_0)$, где $G(V, E)$ - дерево, $v_0 \in V$ - корень.



D_1 изоморфно D_2, как псевдограф, но не изоморфно, как корневое дерево.

Определение: (индуктивное) Корневое дерево:
Базис: ${}_v\odot$ - корневое дерево.
Шаг: Пусть $D_1, ..., D_m$ - корневые деревья, $D_i = (V_i, E_i)$ и $V_i \cap V_j = \varnothing$ $(i \neq j)$, с корнями $v_1, ..., v_m$ соответственно.

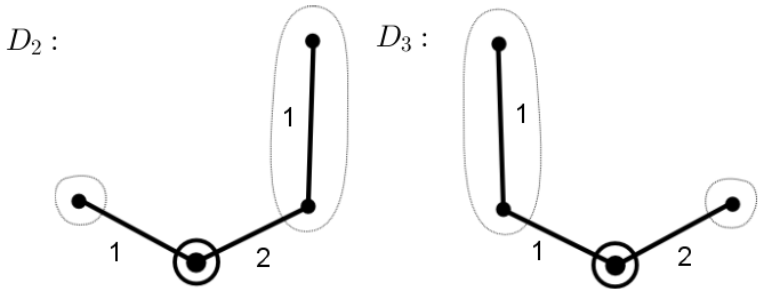


Тогда $D = (V, E)$, где

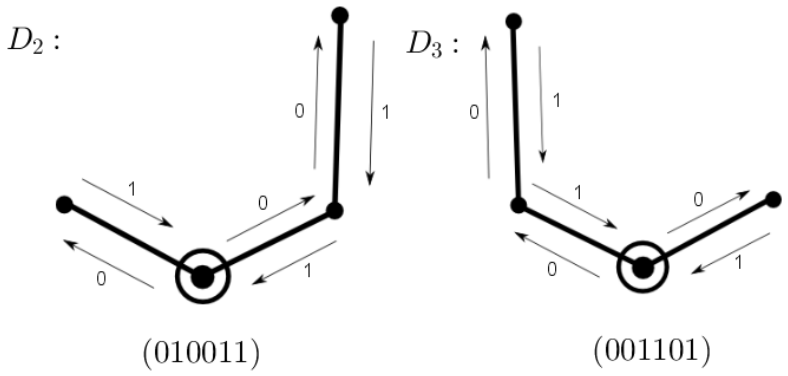
$$V = V_1 \cup V_2 \cup ... \cup V_m \cup \{v\}, \text{ а } v \notin V_i,\ i = \overline{1, n} \text{ и}$$
$$E = E_1 \cup E_2 \cup ... \cup E_m \cup \{(v, v_i) | i = \overline{1, m}\}$$

Других корневых деревьев нет.

Определение: Упорядоченное корневое дерево - корневое дерево, в котором задан порядок поддеревьев $D_1, D_2, ..., D_m$.



Определение: (индуктивное) Кодом упорядоченного корневого дерева $D = (V, E)$ называется вектор α_D:



(010011) (001101)

0 - первый проход ребра, 1 - второй проход ребра

Базис: Если D - корневое дерево, то $\alpha_D = \Lambda$ - пустое.
Шаг: Если D получено из деревьев $D_1, ..., D_m$ в указанном порядке присоединением корня и коды деревьев $\alpha_1, \alpha_2, ..., \alpha_m$, то код $\alpha_D = (0\alpha_1 10\alpha_2 1...0\alpha_m 1)$.

Замечание: Число координат в α_D равно $2|E|$.

Теорема 6: Число неизоморфных упорядоченных корневых деревьев с q ребрами $\leq 4^q$.

Доказательство: Поставим в соответствие каждому упорядоченному корневому дереву D его код α_D: $\alpha_D \in E_2^{2q}$. Так как упорядоченные корневые деревья D_1 и D_2 неизоморфны, то $\alpha_{D_1} \neq \alpha_{D_2}$. Т.е. число упорядоченных корневых деревьев не превосходит число векторов из E_2^{2q}. А число таких векторов $2^{2q} = 4^q$, ■.

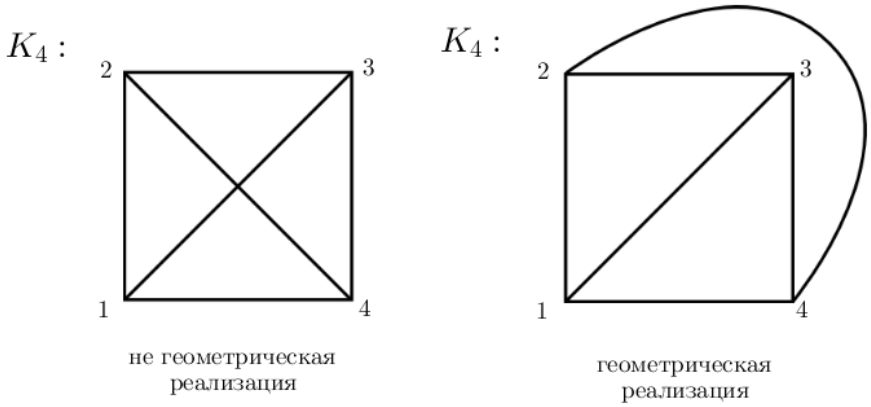
Следствия:

1. Число неизоморфных корневых деревьев с q ребрами не превосходит 4^q.
2. Число неизоморфных деревьев с q ребрами не превосходит 4^q.

Геометрическая реализация графов

Определение: Геометрическая реализация графа $G = (V, E)$ в пространстве $\mathbb{R}^n$ - фигура в $\mathbb{R}^n$:

1. Для любой вершины $v \in V$ сопоставлена точка $a_v \in \mathbb{R}^n$. $a_v \neq a_w$ при $v \neq w$; $v, w \in V$.
2. Для любого ребра $(v, w) \in E$ сопоставлена непрерывная несамопересекающаяся кривая, не проходящая через точки, сопоставленных вершинам (кроме концевых), соединяющая точки a_v и a_w.
3. Кривые, сопоставленные различным ребрам, не пересекаются (кроме концевых точек).

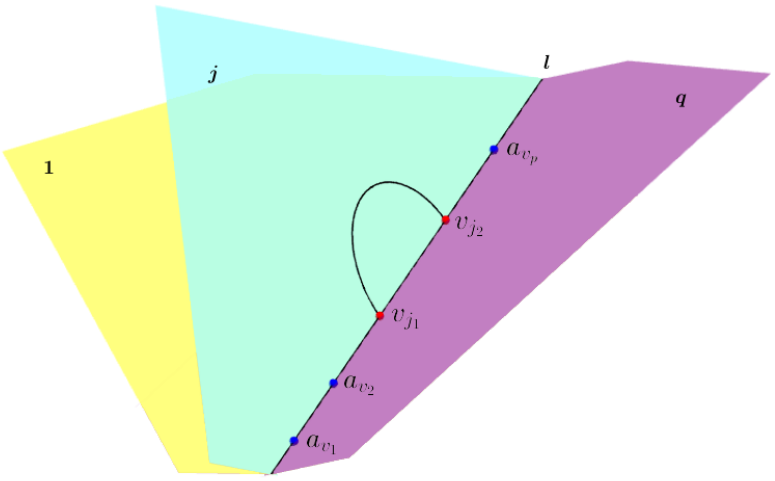


не геометрическая реализация

геометрическая реализация

Теорема 7: Любой граф допускает геометрическую реализацию в $\mathbb{R}^3$.

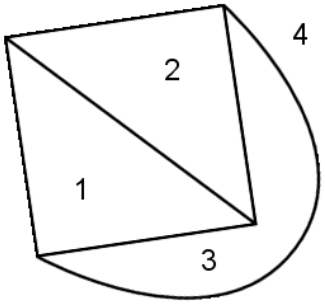
Доказательство: Рассмотрим произвольный граф $G = (V, E)$: $V = \{v_1, ..., v_p\}$; $E = \{e_1, ..., e_q\}$, $e_j = (v_{j_1}, v_{j_2})$.



, ■.

Определение: Граф называется планарным, если он допускает геометрическую реализацию на плоскости (в $\mathbb{R}^2$).

Определение: Пусть граф G геометрически реализован в $\mathbb{R}^2$. Каждая связная область $\mathbb{R}^2$ гранью этой геометрической реализации.



$1, 2, 3, 4$ - связные области.

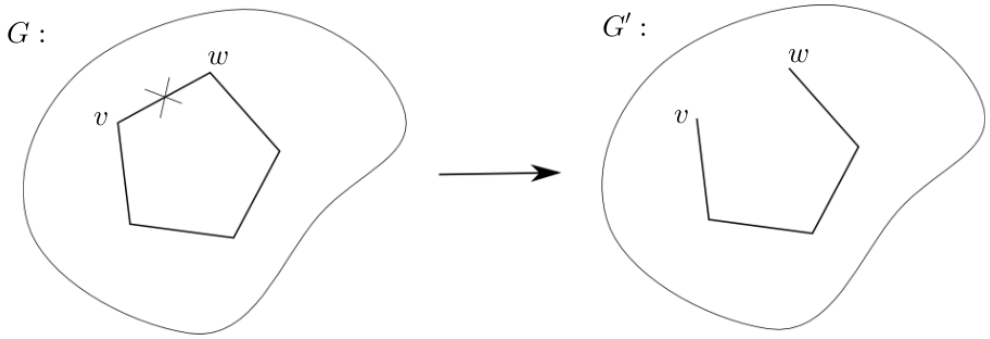
Подсказка: Представим, что граф изображен на листе бумаги. Возьмем ножницы и разрежем по всем линиям наш лист. Полученные кусочки и будут являться гранями.

Теорема 8: (формула Эйлера для планарных графов) Для каждой геометрической реализации планарного связного графа с p вершинами, q ребрами и r гранями верно следующее равенство:

$$p - q + r = 2$$

Доказательство: (индукция по $p - q$).
Базис: $p - q = 1$, т.е. $G = (V, E)$ - дерево. $\underbrace{p - q}_{1} + \underbrace{r}_{1} = 2$.

Шаг: Пусть утверждение теоремы верно для всех связных планарных графов таких, что $p - q \leq s_0$, $s_0 \geq 1$. Рассмотрим связный планарный граф такой, что $p - q = s_0 + 1$. Граф $G = (V, E)$ - связный и не является деревом. Значит в G есть цикл.

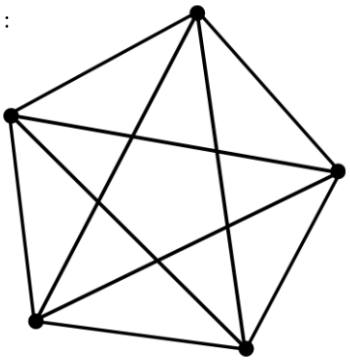


В G': p вершин, $q-1$ ребер. G' - связный, планарный. Для G' верно предположение индукции. Имеем $r - 1$ грань при геометрической реализации.

$$p - (q - 1) + (r - 1) = 2 \Rightarrow p - q + r = 2, \blacksquare.$$

Теорема 9: Граф K_5 не является планарным.

K_5 :



Доказательство: (от противного) Пусть K_5 планарен. Тогда для K_5 при любой его планарной реализации верна формула Эйлера:

$$p = 5;\ q = \tfrac{5\cdot 4}{2} = 10$$

По формуле Эйлера имеем: $5 - 10 + r = 2 \Rightarrow r = 7$.
Пусть в планарной реализации K_5 есть грани $1, 2, ..., r$, и i-ая грань ограничена циклом длины q_i.

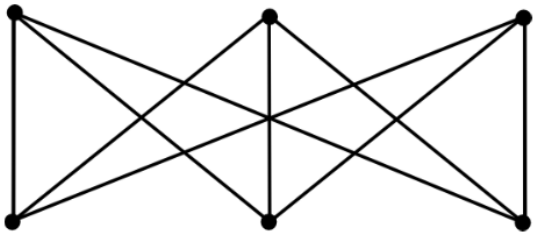
$$q_1 + q_2 + ... + q_r = 2q = 20$$

Заметим, что нет циклов длины 2 и циклов длины 1, поэтому $q_i \geq 3$, $i = \overline{1, r}$.

$$3r \leq 20 \Rightarrow r \leq \tfrac{20}{3}, \text{ противоречие (?!)}, \blacksquare.$$

Теорема 9: (задача о 3-х домах и 3-х колодцах) Граф $K_{3,3}$ не является планарным.

$K_{3,3}$:



Доказательство: (от противного) Пусть $K_{3,3}$ планарен. Тогда для $K_{3,3}$ при любой его планарной реализации верна формула Эйлера:

$$p = 6;\ q = 9$$

По формуле Эйлера имеем: $6 - 9 + r = 2 \Rightarrow r = 5$.
Занумеруем грани $1, 2, ..., r$, и i-ая грань ограничена циклом длины q_i.

$$q_1 + q_2 + ... + q_r = 2q = 20$$

Заметим, что нет циклов длины 2 и циклов длины 1, поэтому $q_i \geq 3$, $i = \overline{1, r}$.

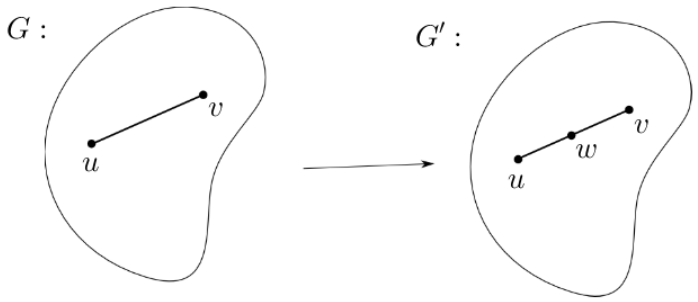
$$3r \leq 18 \Rightarrow r \leq 6.$$

Заметим так же, что в $K_{3,3}$ длина наименьшего цикла равна 4. Тогда $q_i \geq 4$.

$$4r \leq 18 \Rightarrow r \leq \tfrac{18}{4}, \text{ противоречие (?!)}, \blacksquare.$$

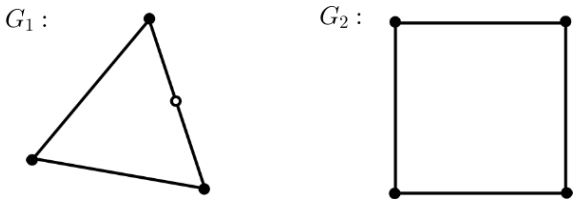
Определение: Пусть $G = (V, E)$ - граф. Операция подразделения ребра $(u, v) \in E$ - это преобразование графа G в граф $G' = (V', E')$, где

$$V' = V \cup \{w\}, w \notin V$$
$$E' = E \backslash \{(u, v)\} \cup \{(u, w), (w, v)\}$$



Определение: Граф G' является подразделением графа G, если граф G' получен из графа G конечным числом операций подразделения ребер.

Определение: Графы G_1 и G_2 называются гомеоморфными, если существуют их подразделения G_1' и G_2', которые изоморфны.

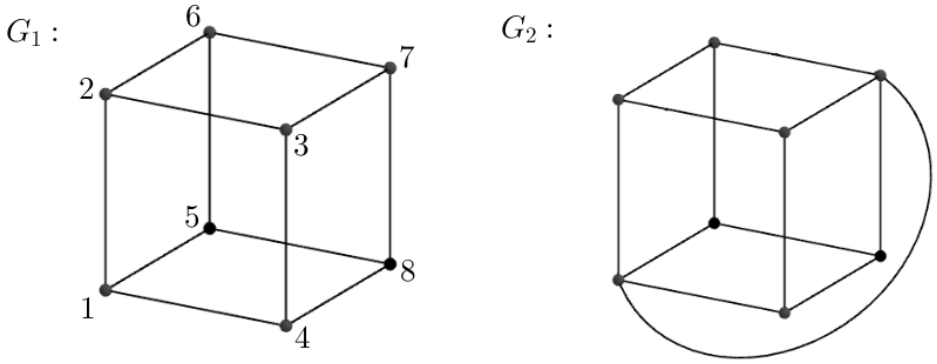


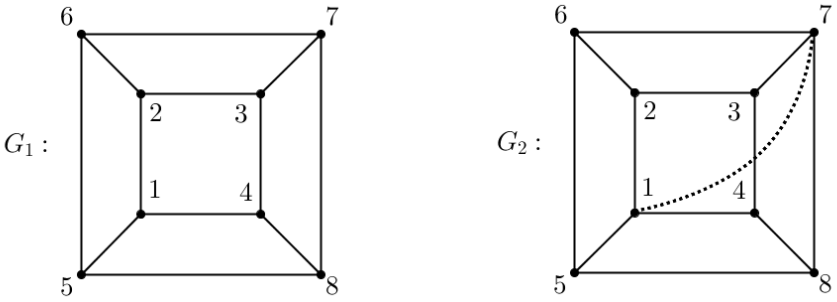
Теорема 11: (критерий планарности Понтрягина-Куратовского) Граф $G = (V, E)$ планарен тогда и только тогда, когда он не содержит ни одного подграфа гомеоморфного графу K_5 и $K_{3,3}$.

Доказательство: $\Rightarrow$: Пусть $G = (V, E)$ - планарен. От противного: пусть $G' = (V', E')$, где $V' \subseteq V, E' \subseteq E$, - подграф G, который гомеоморфен K_5 (или $K_{3,3}$). Построим планарную реализацию графа G. Удалив лишние ребра, получим планарную реализацию G', но K_5 (или $K_{3,3}$) не являются планарными, противоречие (?!).

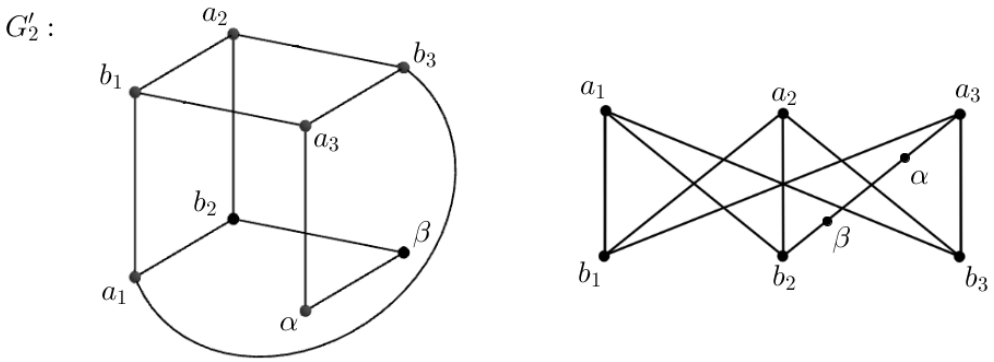
$\Leftarrow$: *Без доказательства,* ■.

Пример: Доказать, являются ли графы G_1 и G_2 планарными:





G_1 планарен. Докажем, что G_2 не является планарным.

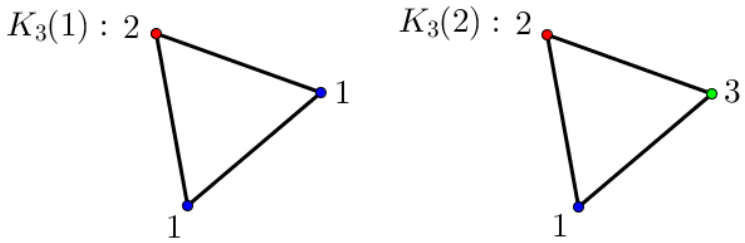


G_2 содержит подграф G_2', изоморфный $K_{3,3}$, и следовательно по теореме Понтрягина-Куратовского не является планарным, ■.

Раскраски графов

Определение: Пусть $C = \{c_1, c_2, ...\}$ - множество цветов. Раскраской вершин графа $G = (V, E)$ называется отображение $\rho : V \to C$ такое, что если $(u, v) \in E$, то $\rho(u) \neq \rho(v)$.

Пример: (1,2,3 - цвета)



Случай (1) не является раскраской.

Определение: Минимальное число цветов, в которое можно раскрасить вершины графа $G = (V, E)$ называется хроматическим числом графа G и обозначается $X(G)$.

Утверждение: Пусть дан граф $G = (V, E)$, $|V| = p$. Тогда выполняется условие: $X(G) \leq p$. Для полного графа K_p действует более сильное утверждение: $X(K_p) = p$.

Определение: Граф G называется двухцветным, если $X(G) = 2$.

Теорема 12: (критерий Кёнинга) Граф $G = (V, E)$ является двухцветным тогда и только тогда, когда в нем отсутствуют циклы нечетной длины.

Доказательство: $\Rightarrow$: $G = (V, E)$ - двухцветный граф, и ρ - раскраска вершин в цвета $\{1, 2\}$. От противного: пусть в G есть циклы нечетной длины. Не ограничивая общности будем считать, что все вершины цепи с четными индексами окрашены в цвет 1, нечетные - 2.

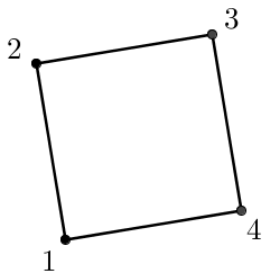
$$\begin{array}{cccccccc} C = & v_0 & v_1 & v_2 & \dots & v_{2k} & v_0 \\ & 1 & 2 & 1 & \dots & 1 & 1 \end{array}$$

Рассмотрим вершину v_{2k}: $\rho(v_{2k}) = 1$, $\rho(v_0) = 1$, $(v_{2k}, v_0) \in E$. Противоречие с определением раскраски.

$\Leftarrow$: Пусть $G = (V, E)$: в G нет циклов нечетной длины. Рассмотрим два множества A и B таких, что: $A, B \subset V$, $A \cup B = V$, $A \cap B = \varnothing$.

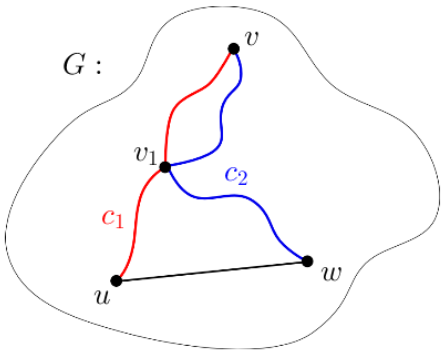
$$A = \{w \in V | \text{ длина минимальной цепи от } v \text{ к } w \text{ четна}\};$$
$$B = \{w \in V | \text{ длина минимальной цепи от } v \text{ к } w \text{ нечетна}\}.$$

Пример:



$v = 1$
$A = \{3, 1\}$
$B = \{2, 4\}$

Докажем, что не существует таких вершин $v, w \in A$: $(u, w) \in E$. (?) От противного: пусть существуют такие вершины $u, w \in A$: $(u, w) \in E$.



Пусть c_1 - цепь минимальной длины из v в u, c_2 - цепь минимальной длины из v в w. Пусть тогда v_1 - первая общая вершина c_1 и c_2, если их рассматривать от u к v и от w к v.

c_1' - часть цепи c_1 от v до v_1. c_2' - часть цепи c_2 от v до v_1. Цепи c_1' и c_2' имеют одинаковые длины, иначе или c_1, или c_2 выбрана неверно, и следовательно одну из них можно уменьшить.

c_1'' - часть цепи c_1 от v_1 до u. c_2'' - часть цепи c_2 от v_1 до w. Длины цепей c_1'' и c_2'' имеют одинаковую четность.

Рассмотрим цикл $c = c_1''(u, w)c_2''$. Он имеет нечетную длину, противоречие (?!).

Множество A - независимое множество вершин, т.е. для любых $u, w \in A$ $(u, w) \notin E$.
Пусть $\rho : V \to C : \rho(u) = 1, \forall u \in A$. Аналогично для B: $\rho(u) = 2, \forall v \in B$, ■.

Лемма 5: Если $G = (V, E)$ - связный планарный граф, и q_i, $i = \overline{1, n}$, число ребер в i-ой грани при какой-то планарной реализации, то

$$\sum_{i=1}^{n} q_i = 2|E| = 2q$$

Лемма 6: Если $G = (V, E)$ - связный планарный граф, не имеющий циклов с менее чем k ребрами, не являющийся деревом, и $|V| = p$, $|E| = q$, то

$$q \leq \frac{k}{k-2}(p-2)$$

Доказательство: По лемме 5 $\sum_{i=1}^{n} q_i = 2q$ и т.к. $q_i \geq 3$, то $r \leq \frac{2q}{k}$. С другой стороны по формуле Эйлера: $r = q - p + 1$.

$$q - p + 2 \leq \frac{2q}{k}$$
$$kq - kp + 2k \leq 2q$$
$$q(k-2) \leq k(p-2)$$
$$q \leq \frac{k}{k-2}(p-2), \blacksquare.$$

Следствие: Для любого связного планарного простого графа $G = (V, E)$, не являющегося деревом, верно $q \leq 3(p-2)$, где $|V| = p$, $|E| = q$.

Лемма 6: Если $G = (V, E)$ - связный планарный граф, то существует $v \in V : deg(v) \leq 5$.

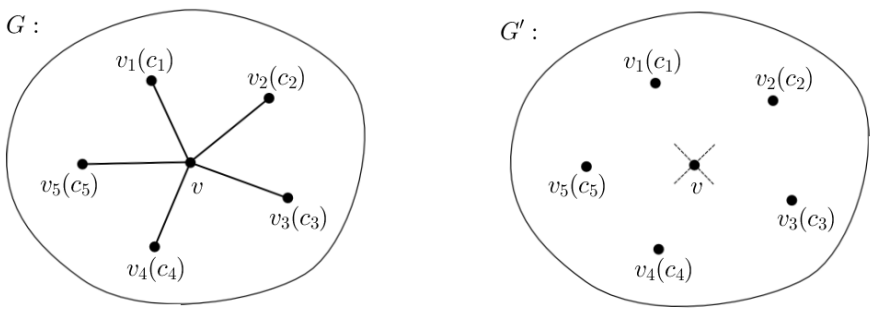
Доказательство: (от противного) Пусть для любого $v \in V : deg(v) \geq 6$. Тогда по формуле Эйлера для степеней вершин ($|E| = q$ и $|V| = p$):

$$6p \leq \sum_{v \in V} deg(v) = 2q$$
$$3p \leq q$$

По следствию из леммы 5: $q \leq 3(p-2) < 3p$, противоречие (?!), $\blacksquare$.

Теорема 13: Вершины любого планарного графа можно раскрасить в не более чем 5 цветов.

Доказательство: (индукция по $p = |V|$) Пусть $G = (V, E)$ - связный планарный граф.
Базис: Очевидно, что для $p \leq 5$ теорема верна.
Шаг: Пусть любой связный граф с не более чем p_0 вершинами можно окрасить в не более чем 5 цветов. Рассмотрим $G = (V, E)$ - связный, планарный и $|V| = p_0 + 1$. Тогда по лемме 6 существует $v \in V : deg(v) \leq 5$.



G' - связный планарный граф, в нем p_0 вершин, и следовательно по предположению индукции G' окрашен в не более, чем 5 цветов.

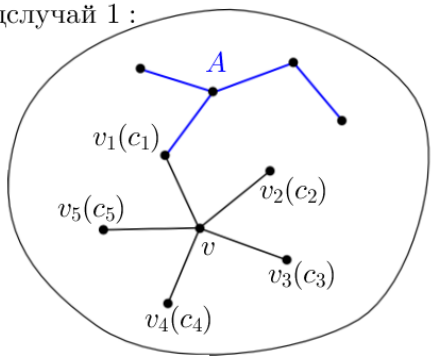
Случай 1: $c_1 - c_5$ содержат не все 5 цветов, тогда красим v в недостающий цвет.

Случай 2: $c_1 - c_5$ - все 5 разных цветов. Пусть A - множество вершин, в которое можно перейти из v_1 только по цветам c_1 и c_3.

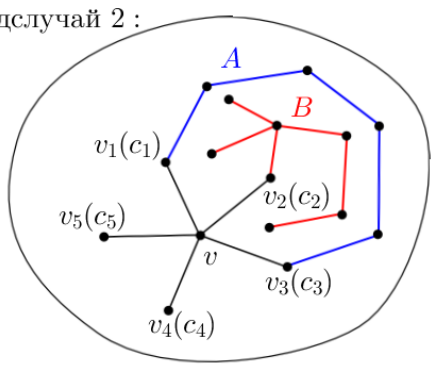
Подслучай 1: $v_3 \notin A$; внутри множества A перекрашиваем все вершины: $c_1 \to c_3$; $c_3 \to c_1$. Тогда красим v в c_1.

Подслучай 2: $v_3 \in A$; строим множество B - множество вершин, в которое можно перейти из v_2 только по цветам c_2 и c_4. Тогда $v_4 \notin A$, т.к. граф планарен и v_2 внутри цикла из цветов c_1 и c_3. Внутри множества B перекрашиваем все вершины: $c_2 \to c_4$; $c_4 \to c_2$. Тогда красим v в c_2.

Подслучай 1 :



Подслучай 2 :



, ■.

Глава 3

Алфавитное кодирование

$A = \{a_1, a_2, ..., a_n\}$ - исходный алфавит;
$B = \{b_1, b_2, ..., b_q\}$ - кодирующий алфавит;
A^* (соответственно B^*) - множество всех слов конечной длины в алфавите A (соответственно B);
$\Lambda \in A^* \cap B^*$ (Λ - пустое слово);
Пусть $\tilde{a} \in A^*$, тогда $l(\tilde{a})$ - длина слова $\tilde{a}$, $l(\Lambda) = 0$.
Кодированием называется отображение $\varphi : A^* \to B^*$.

Определение: Кодирование φ называется разделимым (или однозначно декодируемым, или инъективным, или взаимнооднозначным) тогда и только тогда, когда для любых $\tilde{a}', \tilde{a}'' \in A^*$ ($\tilde{a}' \neq \tilde{a}''$) справедливо $\varphi(\tilde{a}') \neq \varphi(\tilde{a}'')$. [сюръективность отображения не требуется]

Определение: Кодирование $\varphi : A^* \to B^*$ называется алфавитным тогда и только тогда, когда для любых $\tilde{a} = a_{i_1}a_{i_2}...a_{i_l} \in A^*$ имеет место равенство $\varphi(\tilde{a}) = \varphi(a_{i_1})\varphi(a_{i_2})...\varphi(a_{i_l})$ ($\varphi(\tilde{a})$ - конкатенация слов $\varphi(a_{i_1})$,$\varphi(a_{i_2})$,...,$\varphi(a_{i_l})$).

Определение: Пусть $\tilde{a} = \tilde{a}'\tilde{a}^0\tilde{a}''$, тогда $\tilde{a}'$ - префикс $\tilde{a}$, $\tilde{a}''$ - суффикс (постфикс) $\tilde{a}$.

Для алфавитного кодирования φ слова $B_i = \varphi(a_i)$ ($i = \overline{1,r}, a_i \in A$) - кодовые слова.
Далее будем считать, что все кодовые слова попарно различны.

Определение: Алфавитное кодирование называется равномерным тогда и только тогда, когда длины всех кодовых слов одинаковы.

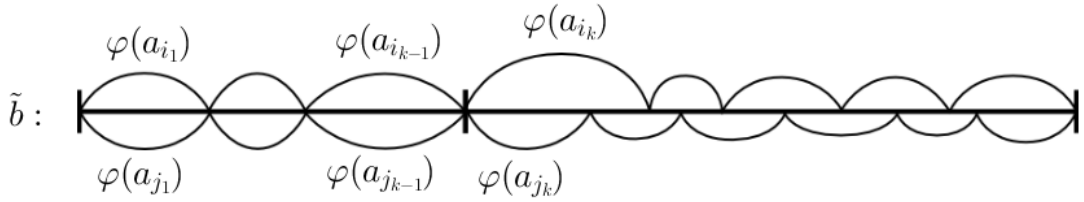
Теорема 1: Всякое равномерное алфавитное кодирование является разделимым.

Определение: Алфавитное кодирование называется префиксным (суффиксным) тогда и только тогда, когда никакое кодовое слово не является префиксом (суффиксом) другого кодового слова.

Теорема 2: Всякое префиксное (суффиксное) кодирование - разделимое.

Доказательство: (от противного) Пусть $\varphi : A^* \to B^*$ - префиксное кодирование, не являющееся разделимым, тогда существует $\tilde{b} \in B^*$: $\tilde{b} = \varphi(\tilde{a}') = \varphi(\tilde{a}'')$, где $\tilde{a}' \neq \tilde{a}''$.
Пусть $\left.\begin{array}{l}\tilde{a}' = a_{i_1}a_{i_2}...a_{i_{l_1}} \\ \tilde{a}'' = a_{j_1}a_{j_2}...a_{j_{l_2}}\end{array}\right| \Rightarrow \exists k \in \mathbb{N}$: $a_{i_1} = a_{j_1}$; $a_{i_2} = a_{j_2}$; $a_{i_{k-1}} = a_{j_{k-1}}$; $a_{i_k} \neq a_{j_k}$, тогда

$$\tilde{b} = \varphi(a_{i_1})\varphi(a_{i_2})...\varphi(a_{i_{k-1}})\varphi(a_{i_k})...\varphi(a_{i_{l_1}});$$
$$\tilde{b} = \varphi(a_{j_1})\varphi(a_{j_2})...\varphi(a_{j_{k-1}})\varphi(a_{j_k})...\varphi(a_{j_{l_2}}).$$



Тогда $\varphi(a_{i_k})$, $\varphi(a_{j_k})$ - префикс другого, противоречие (?!), ■.

Алгоритм распознавания разделимости кодирования

$A = \{a_1, a_2, ..., a_n\}$; $B = \{b_1, b_2, ..., b_q\}$; $\varphi : A^* \to B^*$ - алфавитное кодирование.
$\varphi(a_i) = B_i$ - кодовое слово ($i = \overline{1, r}$).

Построим для φ псевдограф $G_\varphi = (V, E)$ следующим образом:

S_0 - множество всех собственных (не совпадающих с самим кодовым словом) префиксов кодовых слов, являющихся собственными суффиксами кодовых слов; $\Lambda \in S_0$. $V = S_0$.

Рассмотрим все нетривиальные представления всех кодовых слов, имеющих следующий вид:

$$B_i = \beta' B_{j_1} B_{j_2} ... B_{j_w} \beta'', \qquad (*)$$

где β', $\beta'' \in S_0$; $B_i, B_{j_1}, ..., B_{j_w}$ - кодовые слова и при этом:

1. если $\beta' = \Lambda$ и $\beta'' = \Lambda$, то $w \geq 2$;
2. если $\beta' = \Lambda$ или $\beta'' = \Lambda$, то $w \geq 1$;
3. если $\beta' \neq \Lambda$ и $\beta'' \neq \Lambda$, то $w \geq 0$.

Для каждого разложения $(*)$ в G_φ имеется дуга, ведущая из вершины β' в вершину β'', и этой дуге приписано (соответствует) слово $B_{j_1}, B_{j_2}, ..., B_{j_w}$. Иных дуг нет.

Теорема 3: Алфавитное кодирование $\varphi : A^* \to B^*$ - разделимое тогда и только тогда, когда в псевдографе G_φ не ориентированных циклов (контуров), проходящих через вершину Λ.

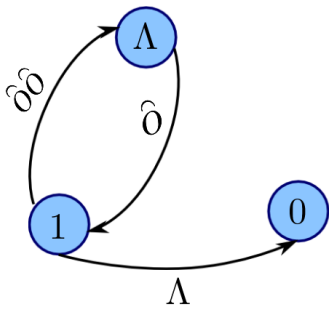
Доказательство: $\Rightarrow$: Пусть в G_φ имеется проходящий через вершину Λ ориентированный цикл: $Z = \Lambda e_{i_1} \beta^{(1)} e_{i_2} \beta^{(2)} ... \beta^{(t-1)} e_{i_t} \Lambda$. Тогда составим слово $\tilde{\beta}$ как конкатенацию слов, соответствующих вершинам и дугам: $Z : \tilde{\beta} = \Lambda B_1^{(1)} ... B_{w_1}^{(1)} \beta^{(1)} B_1^{(2)} ... B_{w_2}^{(2)} \beta^{(2)} ... \beta^{(t-1)} B_1^{(t)} ... B_{w_t}^{(t)} \Lambda$.

$t = 1$: в силу $(*)$ $\tilde{\beta}$ есть кодовое слово и $\tilde{\beta} = B_1^{(1)} ... B_{w_1}^{(1)}$, следовательно φ - неразделим.
$t \geq 2$: в силу $(*)$ возможны два разбиения $\tilde{\beta}$ на кодовые слова:

$$\tilde{b} = \overbrace{\Lambda \underbrace{B_1^{(1)}} ... \underbrace{B_{w_1}^{(1)} \beta^{(1)}} \overbrace{B_1^{(2)}} ... \overbrace{B_{w_2}^{(2)} \beta^{(2)}} ... \underbrace{\beta^{(t-1)}} \overbrace{B_1^{(t)}} ... \overbrace{B_{w_t}^{(t)} \Lambda}}^{},$$

следовательно φ не является разделимым.

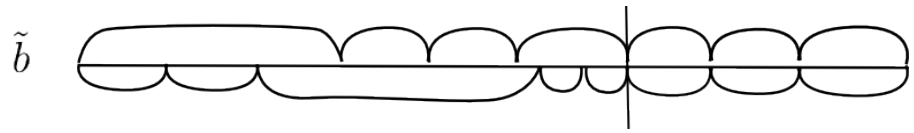
Пример: $\varphi(a_1) = B_1 = 001$; $\varphi(a_2) = 0$; $\varphi(a_3) = 10$. $S_0 = \{\Lambda, 0, 1\}$



$\tilde{b} = \Lambda\,0\,0\,1\,0\,\Lambda$

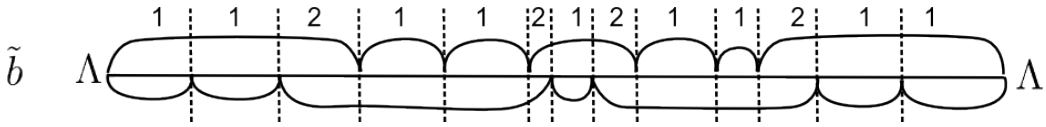
Определение: Слово $\tilde{b}$ в алфавите B называется неприводимым тогда и только тогда, когда $\tilde{b}$ допускает по крайней мере две расшифровки относительно φ, но при выбрасывании из $\tilde{b}$ любого связного куска получаем слово, допускающее не более одной расшифровки.

$\Leftarrow$: Пусть φ - неразделимое, тогда для φ существует неприводимое слово $\tilde{b}$. Заметим, т.к. $\tilde{b}$ - неприводимое, то две его расшифровки нигде не могут иметь общую границу между кодовыми словами.



Границами каждой из двух расшифровок разобьем $\tilde{b}$ на подслова. Возникнут подслова двух типов:

1. кодовые слова одной из расшифровок;
2. слова из S_0.



В соответствие с этим представлением $\tilde{b}$ можно записать в виде:

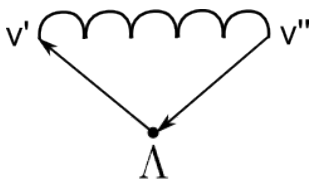
$$\tilde{b} = \Lambda\underbrace{B_1^{(1)}\ldots B_{w_1}^{(1)}}\beta^{(1)}\underbrace{B_1^{(2)}\ldots B_{w_2}^{(2)}}\beta^{(2)}\ldots\beta^{(t-1)}\underbrace{B_1^{(t)}\ldots B_{w_t}^{(t)}}\Lambda,$$

тогда в силу $(*)$ в G_φ имеется замкнутый ориентированный путь из вершины Λ в вершину Λ:
$\hat{Z} = \Lambda e_{i_1}\beta^{(1)}e_{i_2}\beta^{(2)}\ldots\beta^{(t-1)}e_{i_t}\Lambda$. Из $\hat{z}$ можно выделить простой ориентированный цикл, проходящий через вершину Λ.

Случай 1: Имеется петля на вершине Λ в $\hat{Z}$ - очевидно.

Случай 2: В $\hat{Z}$ имеются две противоположные дуги, одна из которых исходит из Λ, а другая - заходит в Λ - очевидно.

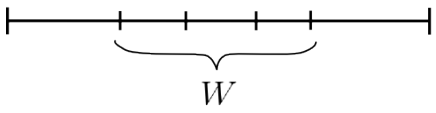
Случай 3: Иначе:



,

тогда по ориентированному аналогу леммы 1 главы 2 существует ориентированная простая цепь из v' в v'', а следовательно существует простой контур через Λ, ■.

Теорема 4: (Маркова) Пусть $\varphi = \{B_1, ..., B_r\}$ - алфавитный код, $|B_i| = l_i$, $i = \overline{1,r}$. Пусть W - максимальное число кодовых слов подряд умещающихся внутри кодового слова.



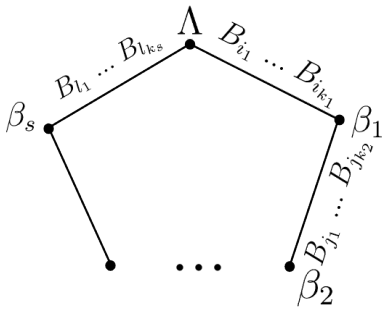
$$\varphi : A^* \to B^*$$

Тогда если φ - не взаимнооднозначное, то существуют слова $\alpha_1, \alpha_2 \in A^*$, $\alpha_1 \neq \alpha_2$.

1. $\varphi(\alpha_1) = \varphi(\alpha_2)$;
2. $|\alpha_1|, |\alpha_2| \leq \left\lfloor \frac{(L-r+2)(W+1)}{2} \right\rfloor$, где $L = l_1 + l_2 + ... + l_r$.

Доказательство: 1) φ - не взаимнооднозначно. В графе G_φ существует ориентированный цикл, проходящий через вершину Λ. Возьмем простой цикл:

$$\beta = \Lambda \overbrace{B_{i_1} ... B_{i_{k_1}}}\, \overbrace{\beta_1 B_{j_1} ... B_{j_{k_2}}}\, \overbrace{\beta_2 ... \beta_s B_{l_1} ... B_{l_{k_s}}}\, \Lambda \in B^*$$



$\exists\, \alpha_1, \alpha_2 \in A^*$ $\alpha_1 \neq \alpha_2$ $\varphi(\alpha_1) = \varphi(\alpha_2) = \beta$. $\beta_1, ...\beta_s \in B^*$ - различные слова, так как цикл простой.
2) $s \leq (l_1 - 1) + (l_2 - 1) + ...(l_r - 1) = L - r$ ($l_i - 1$ - количество различных префиксов)
Слова разбивают слово β не более чем на $L - r + 1$ кусков. Рассмотрим пары соседних кусков. Их не более

$$\left\lceil \frac{L-r+1}{2} \right\rceil \leq \frac{L-r+2}{2},$$

а в каждом из них укладывается слов не более чем $W + 1$. Тогда $|\alpha_1|, |\alpha_2| \leq \left\lfloor \frac{(L-r+2)(W+1)}{2} \right\rfloor$, ■.

Теорема 5: (Неравенство Макмиллана) Пусть $\varphi = \{B_1, ..., B_r\}$ - алфавитный код, $\varphi : A^* \to B^*$, где $|B| = q$, $|B_i| = l_i$, $i = \overline{1,r}$. Тогда если φ - взаимнооднозначное, то

$$\sum_{i=1}^{r} \frac{1}{q^{l_i}} \leq 1$$

Доказательство: $A = \{a_1...a_r\}$, $B = \{b_1...b_q\}$, $n \geq 1$.

$$(a_1 + ... + a_r)^n = \underbrace{(a_1 + ... + a_r)...(a_1 + ... + a_r)}_{n} = \sum_{i_1=1}^{r} \sum_{i_2=1}^{r} ... \sum_{i_n=1}^{r} a_{i_1} a_{i_2} ... a_{i_r}$$

$$(\frac{1}{q^{l_1}} + ... + \frac{1}{q^{l_r}})^n = \sum_{i_1=1}^{r} \sum_{i_2=1}^{r} ... \sum_{i_n=1}^{r} \frac{1}{q^{l_{i_1}}} \frac{1}{q^{l_{i_2}}} ... \frac{1}{q^{l_{i_r}}} = \sum_{i_1=1}^{r} \sum_{i_2=1}^{r} ... \sum_{i_n=1}^{r} \frac{1}{q^{l_{i_1} + l_{i_2} + ... + l_{i_r}}} = \sum_{k=1}^{n \cdot l_{max}} \frac{l_k}{q_k},$$

где $l_{max} = \max\limits_{1 \leq i \leq r} l_i$, а $\max(l_{i_1} + ... + l_{i_n}) = n \cdot l_{max}$; c_k - число наборов $(i_1, ..., i_n)$: $l_{i_1} + ... + l_{i_n} = k$.

Лемма 6: $c_k \le q^k$

Доказательство: c_k - число наборов $(i_1, ..., i_n)$: $l_{i_1} + ... + l_{i_n} = k$.

$$\alpha = a_{i_1}a_{i_2}...a_{i_n} \xrightarrow{\varphi} B_{i_1}B_{i_2}...B_{i_n} = \beta \in B^*; |\beta| = k$$

Всего слов длины k в алфавите B^* q^k и так как φ - взаимнооднозначное $q_k \ge c^k$, ■.

$$\sum_{k=1}^{n\cdot l_{max}} \frac{l_k}{q_k} \le \sum_{k=1}^{n\cdot l_{max}} 1 = n \cdot l_{max}$$

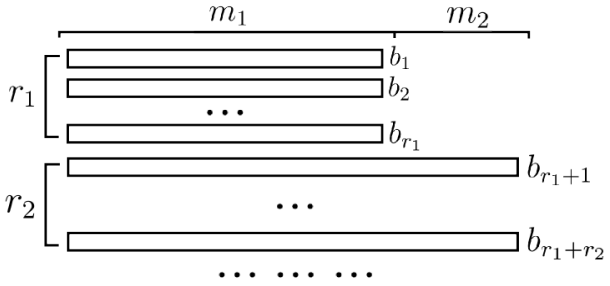
$$\Big(\sum_{i=1}^{r} \frac{1}{q^{l_i}}\Big)^n \le n \cdot l_{max} \Longleftrightarrow \sum_{i=1}^{r} \frac{1}{q^{l_i}} \le \sqrt[n]{n \cdot l_{max}} \underset{n\to\infty}{\longrightarrow} 1 \Rightarrow \sum_{i=1}^{r} \frac{1}{q^{l_i}} \le 1, ■.$$

Пример: $\varphi = \{B_1, B_2, B_3\}$; $B = \{0, 1\}$; $|B_1| = |B_2| = 1$, $|B_3| = 2 \Rightarrow \frac{1}{2^1} + \frac{1}{2^1} + \frac{1}{2^2} = \frac{5}{4} > 1$, противоречие.

Теорема 7: (о существовании префиксного кода с заданными длинами кодовых слов)
Если $q, l_1, ...l_r \in \mathbb{N}$ и $\sum\limits_{i=1}^{r} \frac{1}{q^{l_i}} \le 1$, то существует префиксный код $\varphi = \{B_1, ..., B_n\}$ в алфавите B, $|B| = q$ и $|B_i| = l_i$, $i = \overline{1, n}$.

Доказательство: Рассмотрим $l_1...l_n$: $l_1 \le l_2 \le ... \le l_r$. Пусть $m_1...m_s$ - разные числа из $l_1...l_r$: $m_1 < m_2 < ... < m_s$ и чисел m_j есть r_j, $j = \overline{1, s}$, $r_1 + r_2 + ... + r_s = r$, тогда $\sum\limits_{i=1}^{r} \frac{1}{q^{l_i}} = \sum\limits_{i=1}^{s} \frac{r_j}{q^{m_j}} \le 1$.

(1)	$\frac{r_1}{q^{m_1}} \le 1$	$\to$	$r_1 \le q^{m_1}$
(2)	$\frac{r_1}{q^{m_1}} + \frac{r_2}{q^{m_2}} \le 1$	$\to$	$r_2 \le q^{m_2} - r_1 \cdot q^{m_2-m_1}$
...	...	...	...
(s)	$\frac{r_1}{q^{m_1}} + \frac{r_2}{q^{m_2}} + ... + \frac{r_s}{q^{m_s}} \le 1$	$\to$	$r_s \le q^{m_s} - r_1 \cdot q^{m_s-m_1} - r_2 \cdot q^{m_s-m_2} - ... - r_{s-1} \cdot q^{m_s-m_{s-1}}$



r_1 - слов длины m_1, r_2 - слов длины m_2, ..., r_s - слов длины m_s. Запрещены слова вида: $r_i q^{m_{i+1}-m_i}$, ■.

Пример: $\varphi = \{B_1, B_2, B_3, B_4\}$; $B = \{0, 1\}$; $|B_1| = 1$, $|B_2| = 3$, $|B_3| = |B_4| = 4 \Rightarrow \frac{1}{2^1} + \frac{1}{2^2} + \frac{2}{2^4} \le 1$

(1)	B_1	=	0
(3)	B_2	=	100
(4)	B_3	=	1100
	B_4	=	1110

Теорема 8: Если $\varphi = \{B_1, B_2, ...B_r\}$ - взаимнооднозначный код, то существует префиксный код $\varphi' = \{B'_1, B'_2, ...B'_r\}$ в том же алфавите B: $|B'_i| = |B_1|$, $i = \overline{1, r}$.

Доказательство: Пусть $|B_i| = l_i$, $|B| = q$. Т.к. φ - взаимнооднозначный, то $\sum\limits_{i=1}^{r} \frac{1}{q^{l_i}} \le 1$ и по теореме 7 существует префиксный код с условием теоремы, ■.

Оптимальные коды

$A = \{a_1, ...a_r\}$ - исходный алфавит
$B = \{b_1, ...b_q\}$ - кодирующий алфавит. Здесь и далее $q = 2$, $B = \{0, 1\}$
$\varphi : A^* \to B*$ - разделимое алфавитное кодирование; $\varphi(a_i) = B_i$ - кодовое слово.
p_i - частота встречаемости (вероятность встречи) буквы a_i; $p_i > 0$, $i = \overline{1, r}$; $\sum\limits_{i=1}^{r} p_i = 1$.

Пример: Для текста конечной длины p_i можно определить как $\frac{\text{количество символов}}{\text{длина текста}}$.
$P = (p_1, p_2, ..., p_r)$ - набор частот (распределение вероятностей).

Определение: Цена (избыточность) кодирования φ: $c(P, \varphi) = \sum\limits_{i=1}^{r} p_i \cdot l(B_i)$.
Для рассмотренного примера хорошо видно, что $c(P, \varphi)$ для фиксированного P и различных φ тем меньше, чем меньше длина текста, полученного из исходного при кодировании φ.

Определение: Кодирование $\varphi : A^* \to B^*$ (алфавитное) называется оптимальным для распределения вероятностей $P = (p_1, p_2, ..., p_r)$ тогда и только тогда, когда

1. φ - разделимое;
2. $c(P, \varphi) = \inf\limits_{\substack{\hat{\varphi}: A^* \to B^* \\ \text{разделимое}}} c(P, \hat{\varphi})$.

Теорема 9: Для любых r, q, $P = (p_1, ..., p_r)$, где $p_i > 0$, $i = \overline{1, r}$ и $\sum\limits_{i=1}^{r} p_i = 1$, существует оптимальное кодирование $\varphi : A^* \to B^*$ ($|A| = r$, $|B| = q$).

Доказательство: Существует алфавитное кодирование $\check{\varphi} : A^* \to B^*$; $l(B_i) = l$ ($i = \overline{1, r}$), l можно определить как $l = \lceil \log_q r \rceil$. По теореме 1 $\check{\varphi}$ - разделимое.
Рассмотрим все разделимые алфавитные кодирования $\varphi : A^* \to B^*$ такие, что

$$C(P, \varphi) \leq c(P, \check{\varphi}) = \sum_{i=1}^{r} p_i \cdot l = \lceil \log_q r \rceil,$$

тогда для любого кодового слова B_i в φ выполняется $l(B_i) \leq \dfrac{\lceil \log_q r \rceil}{p_i} = const$. Следовательно таких кодовых слов (да и кодирований тоже) конечное число, ■.

Следствие. Если φ - оптимальное кодирование ($\varphi : A^* \to B^*$, $|A| = r$, $|B| = q$), то $c(P, \varphi) \leq \lceil \log_q r \rceil$.

Замечание. По теореме 8 всякое оптимальное кодирование можно заменить на префиксное, сохранив набор длин кодовых слов. Будем считать, что все оптимальные кодирования - префискные.

Свойства оптимальных кодов

(Код: $C = \{B_1, B_2, ...B_r\}$)

Лемма 1: Пусть $\varphi : A^* \to B^*$ - оптимальное кодирование для $P = (p_1, ..., p_r)$.
Если $p_i < p_j$, то $l(B_i) \geq l(B_j)$.

Доказательство: Пусть, это не так и $l(B_i) < l(B_j)$. Построим кодирование φ_1 по φ, поменяв в φ местами B_i и B_j. Рассмотрим разность:

$$c(P, \varphi) - c(P, \varphi_1) = (p_i \cdot l(B_i) + p_j \cdot l(B_j)) - (p_i \cdot l(B_j) + p_j \cdot l(B_i)) = (p_j - p_i)(l(B_j) - l(B_i)) > 0,$$

следовательно φ - не оптимальный, противоречие (?!), ■.

Лемма 2: Пусть $\varphi : A^* \to B^*$ - оптимальное префиксное кодирование для $P = (p_1, ..., p_r)$. Тогда в коде φ найдутся два кодовых слова максимальной длины, отличающиеся одно от другого лишь последним символом ($B = \{0; 1\}$; кодовые слова: $B_i = \tilde{B}0, B_j = \tilde{B}1$).

Доказательство: Если это не так, то построим по φ кодирование φ_1, удалив последний символ у произвольного кодового слова максимальной длины. Новое кодирование будет префиксным (и следовательно разделимым по теореме 2), $c(P, \varphi) > c(P, \varphi_1)$ - противоречие с оптимальностью φ, ■.

Лемма 3: Пусть φ - оптимальное префиксное кодирование. Тогда можно так переставить кодовые слова в φ_1, чтобы получилось кодирование, в котором двум наименьшим вероятностям соответствовали бы кодовые слова максимальной длины, отличающиеся лишь последним символом.

Доказательство: Такие слова существуют по лемме 2, но по лемме 1 двум наименьшим вероятностям соответствуют слова той же длины, откуда следует требуемое, ■.

Лемма 4: Пусть имеются два алфавитных кодирования:

$$\varphi\colon \begin{pmatrix} p_1 & p_2 & ... & p_{i-1} & p_i & p_{i+1} & ... & p_r \\ B_1 & B_2 & ... & B_{i-1} & B_i & B_{i+1} & ... & B_r \end{pmatrix},$$

$$\varphi'\colon \begin{pmatrix} p_1 & p_2 & ... & p_{i-1} & p_{i+1} & ... & p_r & p' & p'' \\ B_1 & B_2 & ... & B_{i-1} & B_{i+1} & ... & B_r & B_i0 & B_i1 \end{pmatrix},$$

где $p_i = p' + p''$, кодирующий алфавит $B = \{0, 1\}$,
$P = (p_1, ..., p_{i-1}, p_i, p_{i+1}, ..., p_r)$, $P' = (p_1, ..., p_{i-1}, p_{i+1}, ..., p_r, p', p'')$.
Тогда если одно из этих кодирований - префиксное, то и другое тоже префиксное, и при этом

$$c(P', \varphi') = c(P, \varphi) + p_i.$$

Доказательство: Взаимная префиксность очевидна.
$c(P', \varphi') - c(P, \varphi) = (p' \cdot l(B_i0) + p'' \cdot l(B_i1)) - p_i \cdot l(B_i) = (l(B_i) + 1) \cdot \underbrace{(p' + p'')}_{p_i} - p_i \cdot l(B_i) = p_i$, ■.

Теорема 10: (теорема редукции) Пусть φ и φ' - алфавитные префиксные кодирования (такие же, как в утверждении леммы 4). Тогда:

1. если φ' - оптимальное кодирование (отн. P'), то φ - оптимальное кодирование (отн. P);
2. если φ - оптимальное кодирование (отн. P) и при этом p', p'' - две наименьшие вероятности в P', то φ' - оптимальное кодирование (отн. P').

Доказательство: 1) Пусть φ' - оптимальное, но φ - не оптимальное. Тогда существует префиксное кодирование φ_1 такое, что $c(P,\varphi_1) < c(P,\varphi)$.

$$\varphi_1\colon \begin{pmatrix} p_1 & p_2 & \dots & p_{i-1} & p_i & p_{i+1} & \dots & p_r \\ D_1 & D_2 & \dots & D_{i-1} & D_i & D_{i+1} & \dots & D_r \end{pmatrix}$$

Тогда рассмотрим

$$\varphi_1'\colon \begin{pmatrix} p_1 & p_2 & \dots & p_{i-1} & p_{i+1} & \dots & p_r & p' & p'' \\ D_1 & D_2 & \dots & D_{i-1} & D_{i+1} & \dots & D_r & D_i0 & D_i1 \end{pmatrix}$$

По лемме 4 из того, что φ_1' - префиксное кодирование, следует, что оно является разделимым;

$$\left.\begin{array}{c} c(P',\varphi_1') = c(P,\varphi_1) + p_i \\ c(P',\varphi') = c(P,\varphi) + p_i \end{array}\right| \Rightarrow c(P',\varphi_1') < c(P',\varphi'),$$

что противоречит оптимальности кодирования φ'.

2) φ - оптимальное, p', p'' - наименьшие вероятности в P', но φ' - не оптимальное, тогда существует префиксное оптимальное кодирование φ_2' (для P'): $c(P',\varphi_2') < c(P',\varphi')$.
По лемме 3 по φ_2' построим кодирование φ_3, в котором два кодовых слова максимальной длины отличаются лишь последним символом, соответствуют вероятностям p' и p''.
Ясно, что $c(P',\varphi_2') = c(P',\varphi_3')$. Пусть

$$\varphi_3'\colon \begin{pmatrix} p_1 & p_2 & \dots & p_{i-1} & p_{i+1} & \dots & p_r & p' & p'' \\ E_1 & E_2 & \dots & E_{i-1} & E_{i+1} & \dots & E_r & E_i0 & E_i1 \end{pmatrix}$$

Тогда рассмотрим

$$\varphi_3\colon \begin{pmatrix} p_1 & p_2 & \dots & p_{i-1} & p_i & p_{i+1} & \dots & p_r \\ E_1 & E_2 & \dots & E_{i-1} & E_i & E_{i+1} & \dots & E_r \end{pmatrix}$$

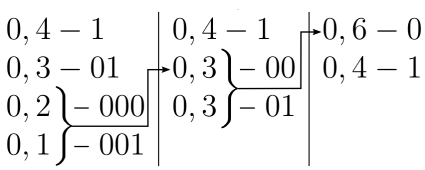
По лемме 4 φ_3 - префиксное, а значит, разделимое, и:

$$\left.\begin{array}{c} c(P',\varphi_3') = c(P,\varphi_3) + p_i \\ c(P',\varphi') = c(P,\varphi) + p_i \end{array}\right| \Rightarrow c(P',\varphi_3') < c(P',\varphi'),$$

противоречие, ■.

На основании теоремы редукции строится алгоритм Хаффмана построения оптимального двоичного кодирования.

Пример: $P = (0,4; 0,3; 0,3; 0,1)$; $B = 0,1$.



Коды, исправляющие ошибки

$A = \{a_1, ..., a_n\}$ - исходный алфавит; $B = \{0, 1\}$ - кодирующий алфавит; $\varphi : a^* \to B^*$ - равномерное алфавитное кодирование. $\varphi(a_i) = B_i = \alpha_i \in E_2^n$, $l(B_i) = n$, $i = \overline{1, n}$.
При передаче кодового слова могло произойти не более t ошибок типа замены переменной.

Определение: Код $C = \{B_1, ..., B_r\}$ называется обнаруживающим t ошибок тогда и только тогда, когда по всякому полученному слову можно распознать, имела ли место хотя бы одна ошибка (или получено переданное слово).

Определение: Код $C = \{B_1, ..., B_r\}$ называется обнаруживающим t ошибок тогда и только тогда, когда по всякому полученному слову можно восстановить передававшееся слово.

Определение: Расстояние Хэмминга между наборами $\alpha = (\alpha_1...\alpha_n)$ и $\beta = (\beta_1...\beta_n)$ есть число координат, в которых α и β отличаются:

$$\rho(\alpha, \beta) = \sum_{i=1}^{n} |\alpha_i - \beta_i|$$

Определение: Сфера радиуса R с центром в $\alpha \in E_2^n$: $S_{n,R}^{\alpha} = \{\beta \mid \beta \in E_2^n, \rho(\alpha, \beta) = R\}$.

Определение: Шар радиуса R с центром в $\alpha \in E_2^n$: $\hat{S}_{n,R}^{\alpha} = \{\beta \mid \beta \in E_2^n, \rho(\alpha, \beta) \leq R\}$.

Заметим, что при передаче набора α полученный набор лежит в $\hat{S}_{n,t}^{\alpha}$ (любой набор этого шара может быть получен при передаче α).

Определение: Кодовым расстоянием кода $C = \{\tilde{\alpha}_1, ..., \tilde{\alpha}_r\}$ ($C \subseteq E_2^n$) называется величина

$$d(C) = \min_{\substack{\tilde{\alpha}_i, \tilde{\alpha}_j \in C \\ \tilde{\alpha}_i \neq \alpha_j}} \rho(\tilde{\alpha}_i, \tilde{\alpha}_j)$$

Лемма 5: Число наборов в сфере $S_{n,R}^{\alpha}$ ($0 \leq R \leq n, R \in \mathbb{Z}, \alpha \in E_2^n$) равно

$$S_{n,R} = \binom{n}{R} = C_n^R = \frac{n!}{R!(n-R)!}$$

Доказательство: число R-элементных подмножеств n-множества есть $\binom{n}{R}$, ■.

Лемма 6: Число наборов в шаре $\hat{S}_{n,R}^{\alpha}$ ($0 \leq R \leq n, R \in \mathbb{Z}, \alpha \in E_2^n$) равно

$$\hat{S}_{n,R} = \sum_{i=0}^{R} \binom{n}{i}$$

Теорема 11: Код $C = \{\tilde{\alpha}_1, ..., \tilde{\alpha}_r\}$ ($C \subseteq E_2^n$) обнаруживает t ошибок тогда и только тогда, когда

$$d(C) \geq t + 1.$$

Доказательство: $\Rightarrow$: $d(C) \leq t$. Докажем, что код C не обнаруживает t ошибок. Существуют $\tilde{\alpha}_i, \tilde{\alpha}_j \in C$ $(\tilde{\alpha}_i \neq \tilde{\alpha}_j)$: $\rho(\tilde{\alpha}_i, \tilde{\alpha}_j) \leq t$. При получении $\tilde{\alpha}_j$ мог передаваться сам $\tilde{\alpha}_j$ (и тогда ошибок не было), а мог передаваться $\tilde{\alpha}_i$ (и тогда ошибки были), следовательно распознать наличие ошибок нельзя, C не обнаруживает t ошибок.

$\Leftarrow$: Пусть $d(C) \geq t + 1$, тогда никакое кодовое слово $\tilde{\alpha}_j$ не лежит в шаре $\hat{S}_{n,t}^{\tilde{\alpha}_i}$ ($\tilde{\alpha}_i$ - другое кодовое слово). Если получено кодовое слово, то оно и передавалось, и ошибок не было; а если было получено не кодовое слово, то ошибки были. Следовательно C - код, обнаруживающий t ошибок, ■.

Теорема 12: Код $C = \{\tilde{\alpha}_1, ..., \tilde{\alpha}_r\}$ ($C \subseteq E_2^n$) исправляет t ошибок тогда и только тогда, когда

$$d(C) \geq 2t + 1.$$

Доказательство: $\Rightarrow$: $d(C) \leq 2t$. Тогда существуют $\tilde{\alpha}_i, \tilde{\alpha}_j \in C$ $\tilde{\alpha}_i \neq \tilde{\alpha}_j$, и $\tilde{\gamma} \in E_2^n$: $\tilde{\gamma} \in \hat{S}_{n,t}^{\tilde{\alpha}_i} \cap \hat{S}_{n,t}^{\tilde{\alpha}_j}$. При получении $\tilde{\gamma}$ не ясно, передавалось ли $\tilde{\alpha}_i$ или $\tilde{\alpha}_j$, следовательно C не исправляет t ошибок.

$\Leftarrow$: Пусть $d(C) \geq 2t+1$, тогда для любых $\tilde{\alpha}_i$ и $\tilde{\alpha}_j$ из C $(\tilde{\alpha}_i \neq \tilde{\alpha}_j)$: $\hat{S}_{n,t}^{\tilde{\alpha}_i} \cap \hat{S}_{n,t}^{\tilde{\alpha}_j} = \varnothing$, тогда если получили некоторый $\tilde{\beta}$, то существуют единственный $\tilde{\alpha} \in C$: $\rho(\tilde{\alpha}, \tilde{\beta}) \leq t$, значит передавалось кодовое слово $\tilde{\alpha}$, и C исправляет t ошибок, ■.

Определение: $M_t(n)$ - максимальное число наборов в коде, исправляющем t ошибок.

Теорема 13:

$$\frac{2^n}{\hat{S}_{n,2t}} \leq M_t(n) \leq \frac{2^n}{\hat{S}_{n,t}}$$

Доказательство: Пусть $C \subseteq E_2^n$ - такой код, исправляющий t ошибок, что $|C| = M_t(n)$.

Оценка сверху: т.к. по теореме 12 $d(C) \geq 2t+1$, то шары радиуса t с центрами в кодовых словах не пересекаются, следовательно каждый набор из E_2^n лежит не более чем в 1 шаре: $|C| \cdot \hat{S}_{n,t} \leq |E_2^n|$, т.е. $M_t(n) \leq \frac{2^n}{\hat{S}_n n,t}$.

Оценка снизу: (от противного) Пусть $2^n > |C| \cdot \hat{S}_{n,2t}$, тогда существует набор $\tilde{\alpha}$ в E_2^n, не лежащий ни в одном шаре радиуса 2t с центром в кодовом слове, следовательно для любого $\tilde{\beta} \in C : \rho(\tilde{\beta}, \tilde{\alpha}) \geq 2t + 1$, тогда по теореме 12 код $C' = C \cup \{\tilde{\alpha}\}$ исправляет t ошибок, но $|C'| > M_t(n)$ - противоречие с максимальность кода C по числу наборов, ■.

Линейные (групповые) коды

Определение: Равномерный код $C \subseteq E_2^n$ называется линейным (групповым) тогда и только тогда, когда для любых $\tilde{\alpha}$ и $\tilde{\beta}$ из C набор $\tilde{\gamma} = \tilde{\alpha} \oplus \tilde{\beta}$ (покоординатное сложение) лежит в C.

Заметим:

1. $(0, ..., 0)$ лежит в линейном коде;
2. наборы кода C образуют группу относительно покоординатного сложения по модулю 2;
3. наборы кода C образуют линейной пространство с операциями покоординатного сложения по модулю 2 векторов (наборов) и умножения вектора на число из $E_2^n = \{0, 1\}$.

Как и в линейной алгебре можно определить $\dim C$, вводить базисы в C, рассматривать ортогональное пространство.

Пусть какой-то базис в C имеет вид:

$$B = \{\tilde{h}^{(1)}, \tilde{h}^{(2)}, ..., \tilde{h}^{(d)}\},$$

где $\tilde{h}^{(i)} = (h_{i_1}, h_{i_2}, ...h_{i_n}), i = \overline{1, d}$. Тогда всякий набор из C представим в виде:

$$\tilde{\alpha} = c_1\tilde{h}^{(1)} + c_2\tilde{h}^{(2)} + ... + c_d\tilde{h}^{(d)},$$

где $(c_1, c_2, ..., c_2) \in E_2^d$.

Пусть

$$H = H(C) = \begin{pmatrix} h_{11} & h_{12} & \cdots & h_{1n} \\ h_{21} & h_{22} & \cdots & h_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ h_{d1} & h_{d2} & \cdots & h_{dn} \end{pmatrix}$$

– порождающая матрица кода C.

Тогда остальные наборы C суть набора вида: $\tilde{\alpha} = \tilde{c} \cdot H(C)$, где $c = (c_1, c_2, ..., c_2) \in E_2^d$.
Замечание: $\tilde{\alpha}, \tilde{c}$ - вектор-строка.

Пусть $C^\perp$ - ортогональное пространство к линейному пространству C, и пусть $B^\perp = \{\tilde{g}^{(1)}, \tilde{g}^{(2)}, ..., \tilde{g}^{(d)}\}$ - базис $C^\perp$, тогда каждый вектор $\tilde{\alpha} = (\alpha_1, ..., \alpha_n)$ из C - решение системы уравнений:

$$(\tilde{\alpha}, \tilde{g}^{(j)}) = 0, j = \overline{1, k}.$$

Если $\tilde{g}^{(j)} = (g_{j_1}, ..., g_{j_n})$, то система имеет вид:

$$\alpha_1 g_{j_1} \oplus \alpha_2 g_{j_2} \oplus ... \oplus \alpha_n g_{j_n} = 0, j = \overline{1, k}.$$

В матричной форме:

$$G = G(C) = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{pmatrix}$$

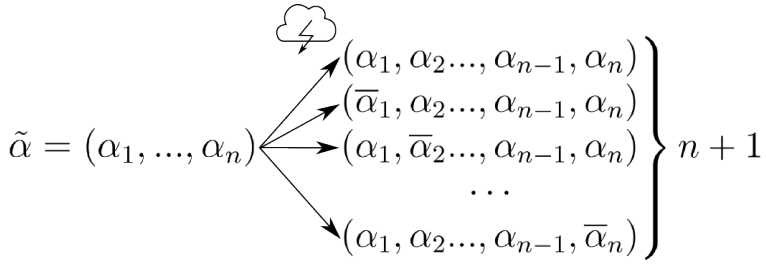
– проверочная матрица кода C. $G \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ (размер столбца $\tilde{0}$ равен k).

Теорема 14: Пусть $C \subseteq E_2^n$ - линейный код. Тогда $d(C) = \min\limits_{\substack{\tilde{\alpha}\in C \\ ||\tilde{\alpha}||\neq 0}} ||\tilde{\alpha}||$, где $||\tilde{\alpha}||$ - вес (число '1' в $\tilde{\alpha}$).

Доказательство: Ясно, что $\underbrace{(0,0,...0)}_{n} = \alpha_0 \in C$. Пусть $\tilde{\beta} \in C$ - ненулевой набор минимального веса в C; $||\tilde{\beta}|| = w$. Тогда $d(c) \leq \rho(\tilde{\alpha}_0, \tilde{\beta}) = w$.
Пусть $d(c) < w$, тогда существуют $\tilde{\alpha}_i$ и $\tilde{\alpha}_j$ из C $(\tilde{\alpha}_i \neq \tilde{\alpha}_j) : \rho(\tilde{\alpha}_i, \tilde{\alpha}_j) = d' < w$, тогда набор $\tilde{\gamma} = \tilde{\alpha} \oplus \tilde{\beta}$ лежит в C. $0 < ||\tilde{\gamma}|| = d' < w$, следовательно $\tilde{\beta}$ не является ненулевым набором минимального веса в C - противоречие (?!). Значит, $d(c) = w$, ■.

Коды Хэмминга

Коды Хэмминга - класс линейных кодов, исправляющих одну ошибку.



Выделим k контрольных разрядов и $n - k = m$ информативных разрядов. В информационных разрядах произвольное содержание, в контрольных - непроизвольное. При выборе k минимально возможным выполняются неравенства:

$$\begin{cases} 2^k \geq n+1 \\ 2^{k-1} < n+1 \end{cases} \Rightarrow n+1 \leq 2^k \leq 2n \Rightarrow k = \lfloor \log_2 n \rfloor + 1 = \lceil \log_2 (n+1) \rceil$$

С помощью k двоичных разрядов можно записать любое (целое) число от 1 до n.
Положим $D_i = \{j | j \in \{1, ..., n\}, j = (\gamma_{k-1}\gamma_{k-2}...\gamma_1\gamma_0)_2, \gamma_i = 1\}$; $i = \overline{0, k-1}$.

Пример: $n = 7; k = 3$

	0	1	2	3	4	5	6	7
γ_2	0	0	0	0	1	1	1	1
γ_1	0	0	1	1	0	0	1	1
γ_0	0	1	0	1	0	1	0	1

$D_0 = \{1, 3, 5, 7\}$
$D_1 = \{2, 3, 6, 7\}$
$D_2 = \{4, 5, 6, 7\}$

Заметим: $2^i \in D_i \backslash (\bigcup\limits_{\substack{i' \in \{0,...,k-1\} \\ i' \neq i}} D'_i)$; $2^i = (0, ..., 0, 1, \underbrace{0, ..., 0}_{i})_2$

Определение: Код Хэмминга C_n^H ($C_n^H \subseteq E_2^n$) - множество всех таких наборов $\tilde{\alpha} = (\alpha_1, ..., \alpha_n)$, что

$$\forall i \in \{0, ..., k-1\} : \bigoplus_{j \in D_i} \alpha_j = 0; \qquad (*)$$

В силу замечания:

$$\alpha_{2^i} = \bigoplus_{\substack{j \in D_i \\ j \neq 2^i}} \alpha_j \qquad (**)$$

В правых частях $(**)$ не встречаются $\alpha_1, \alpha_2, \alpha_4, ..., \alpha_{2^{k-1}}$. Эти разряды $(1, 2, 4, ..., 2^{k-1})$ - контрольные, остальные - информационные.

Теорема 15: Код Хэмминга C_n^H исправляет одну ошибку и $|C_n^H| = 2^{n-k}$, где $k = \lfloor \log_2 n \rfloor + 1$.

Доказательство: Количество информационных разрядов есть $n-k$, следовательно число наборов в C_n^H есть 2^{n-k} (в силу $(**)$).

Пусть посылается набор набор $\tilde{\alpha} = (\alpha_1...\alpha_n)$ из C_n^H, получен набор $\tilde{\beta} = (\beta_1...\beta_n)$ и $\rho(\tilde{\alpha}, \tilde{\beta}) \leq 1$.

Вычислим величины:

$$\delta_i = \bigoplus_{j \in D_i} \beta_j; i = \overline{1, k}$$

Пусть $\Delta = (\delta_{k-1}...\delta_0)_2$.

- Если ошибки не было, то в силу $(*)$ $\Delta = (\underbrace{0...0}_{k})_2 = 0$;
- Пусть ошибка произошла в разряде $\varepsilon = (\varepsilon_{k-1}\varepsilon_{k-2}...\varepsilon_0)_2$, $\varepsilon \in \{1, 2, ..., n\}$. Докажем, что $\Delta = \varepsilon$:

  Случай 1: $\varepsilon \in D_i \Rightarrow \varepsilon_i = 1$;

$$\delta_i = \bigoplus_{j \in D} \beta_j = \beta_\varepsilon \oplus \bigoplus_{\substack{j \in D_i \\ j \neq \varepsilon}} \beta_j = (\alpha_\varepsilon \oplus 1) \oplus \bigoplus_{\substack{j \in D_i \\ j \neq \varepsilon}} \alpha_j = \bigoplus_{j \in D} \alpha_j \oplus 1 = 0 \oplus 1 = 1 = \varepsilon_i$$

  Случай 2: $\varepsilon \notin D_i \Rightarrow \varepsilon_i = 0$;

$$\delta_i = \bigoplus_{j \in D_i} \beta_j = \bigoplus_{j \in D_i} \alpha_j = 0 = \varepsilon_i$$

В обоих случаях $\forall i \in \{0, ..., k-1\} : \delta_i = \varepsilon_i \Rightarrow \Delta = \varepsilon > 0$, по $\Delta = (\delta_{k-1}, ..., \delta_0)_2$ можно определить была ли ошибка и в каком разряде, следовательно C_n^H исправляет одну ошибку, ■.

Теорема 16:

$$\frac{2^n}{2n} \leq M_1(n) \leq \frac{2^n}{n+1}$$

Доказательство: При $t = 1 : \hat{S}_{n,1} = n + 1 \Rightarrow$ **верхняя оценка** по теореме 13.

Нижняя оценка:

$$M_1(n) \geq |C_n^H| \overset{\text{т.15}}{=} 2^{n-k} = \frac{2^n}{2^{\lfloor \log_2 n \rfloor + 1}} \geq \frac{2^n}{2^{\log_2 n + 1}} = \frac{2^n}{2n}, \blacksquare.$$

Глава 4

Схемы из функциональных элементов

Рассмотрим псевдоконечные графы.

Определение: Исток - вершина, в которую не заходят дуги.

Определение: Сток - вершина, из которой не исходят дуги.

Теорема 1: Во всяком конечном псевдографе $G = (V, E)$ без ориентированных циклов имеется по крайней мере один и сток и по крайней мере один сток.

Доказательство: Докажем для стока (для истока аналогично). Рассмотрим произвольную вершину v. Если v - исток, то утверждение доказано. Иначе из v исходит хотя бы одна дуга, ведущая в вершину w. Повторим рассуждения для $v = w$. Так как нет ориентированных циклов, то попасть в пройденную ранее вершину невозможно, следовательно за конечное число шагов найдется вершина из которой не ведут дуги - сток, ■.

Определение: Глубиной вершины v конечного псевдографа G без ориентированных циклов называется максимальная длина ориентированного пути в G до данной вершины.

Алгоритм топологической сортировки вершины псевдографа G без ориентированных циклов

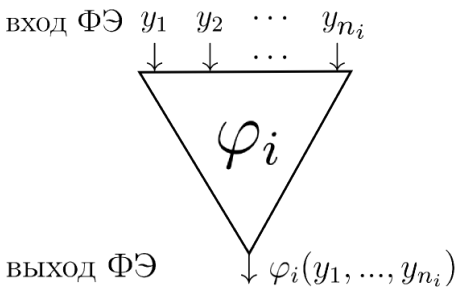
1. $i = 0$;
2. Помечаем все истоки числом i;
3. Если после удаления всех истоков получается псевдограф без вершин, то конец работы алгоритма, иначе - удалим все истоки, $i = i + 1$; перейдем к пункту 2.

Замечание: Пусть $d(u)$ - глубина вершины u в псевдографе G без ориентированных циклов. Если $e = (u, w)$ - дуга в G, то $d(u) < d(w)$.

Определение: Псевдограф называется упорядоченным тогда и только тогда, когда для каждой вершины задан порядок заходящих в нее дуг.

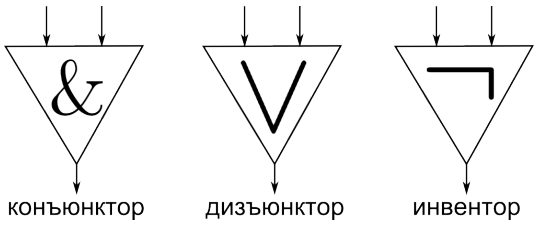
[Схемный] базис: Б $= \{\varphi_i(y1, ..., y_n) | i = \overline{1, s}\}$

Функциональный элемент



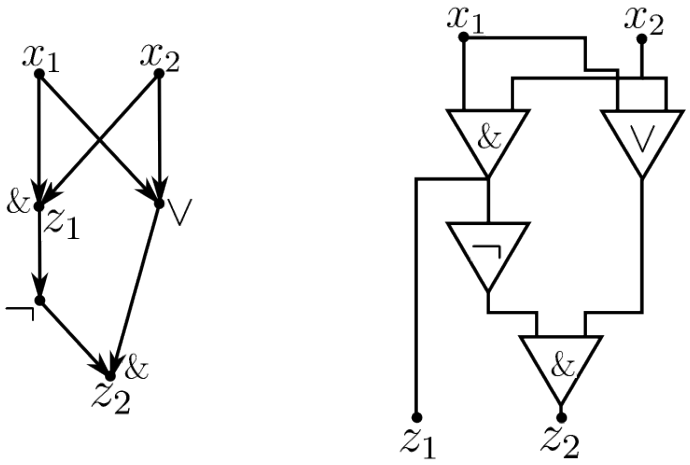
На вход подаются (одновременно) двоичные символы $\alpha_i, ..., \alpha_{n_i}$, на выходе мгновенно оказывается $\varphi_i(\alpha_i, ..., \alpha_{n_i})$.

$Б_0 = \{x_1 \cdot x_2, x_1 \vee x_2, \overline{x}\}$ - стандартный базис.



Определение: Схемой из функциональных элементов (СФЭ) в базисе Б называется конечный упорядоченный псевдограф Σ без ориентированных циклов, у которого:

1. Каждый исток помечен символом входной переменной (из множества $X = \{x_1, x_2...\}$), разные истоки помечены разными переменными. Истоки являются входами СФЭ.
2. Каждой вершине, отличной от истока, приписан символ ФЭ из Б, при этом число заходов в вершину дуг равно числу входов этого ФЭ, и порядок входов определяется порядком заходящих в вершину дуг.
3. Некоторые вершины помечены различными символами выходных переменных (из множества $Z = \{z_1, z_2, ...\}$) - это выходы СФЭ.



Индукцией по глубине вершины вершины v в Σ определим реализуемую в v булеву функцию f_v от всех переменных $x_1...x_n$ СФЭ Σ.

Базис: Пусть $d(v) = 0$, v - исток, которому приписана входная переменная $x_i \Rightarrow f_v(x_1...x_n) = x_i$.

Шаг: Пусть для всех вершин v глубины $d(v) \leq d' - 1$ функции f_v определены. Рассмотрим вершину v: $d(v) = d'$. Пусть в v заходят дуги из вершин $w_{i_1}, w_{i_2}, ..., w_{i_t}$ (в этом порядке) и в этих вершинах реализуется булевы функции $f_{w_{i_1}}, ..., f_{w_{i_t}}$ и самой вершине приписан символ ФЭ φ из Б. Тогда

$$f_v(x_1, ..., x_n) = \varphi(f_{w_{i_1}}, ..., f_{w_{i_t}});$$

Пусть $v_1, ..., v_m$ - все выходные вершины СФЭ Σ.

Тогда говорят, что СФЭ Σ реализует систему функций $\bar{f} = \{f_{v_1}, ..., f_{v_m}\}$.

- Число ФЭ в Σ - сложность $L(\Sigma)$ СФЭ Σ.
- Сложность реализации системы булевых функций $\bar{f}$ схемами в базисе Б:

$$L_{\text{Б}}(\bar{f}) = \min_{\substack{\Sigma \text{ - СФЭ в Б,} \\ \text{реализ. } \bar{f}}} L(\Sigma)$$

- Функция Шеннона сложности СФЭ в базисе

$$L_{\text{Б}}(n) = \max_{f(x_1,...,x_n) \in P_2(n)} L_{\text{Б}}(\{f\}); n \in \mathbb{N}_0$$

Теорема 2: Для любой системы булевых функций $\bar{f}(x_1, ..., x_n) = \{g_1, ..., g_m\}$ существует реализующая ее СФЭ $\Sigma_{\bar{f}}$ в базисе $\text{Б}_0 = \{xy, x \vee y, \bar{x}\}$, такая что:

$$L(\Sigma_{\bar{f}}) \leq m \cdot n \cdot 2^{n+1}; m, n \in \mathbb{N}$$

Доказательство: Реализуем каждую булеву функцию $g_i(x_1, ..., x_n)$ "своей" СФЭ Σ_{g_i} следующим образом:

- если $g_i \equiv 0$, то Σ_{g_i} моделирует формулу $x_i \cdot \bar{x}_i$ (2 ФЭ);
- если $g_i \not\equiv 0$, то Σ_{g_i} моделирует совершенную ДНФ функции g_i:

$$L(\Sigma_{g_i}) = \underset{\substack{\text{число слаг.} \\ \text{в сов. ДНФ}}}{2^n} (\overset{'\neg'}{n} + \overset{'\&'}{(n-1)} + \overset{'\vee'}{1}) = n \cdot 2^{n+1}$$

Отождествляя все входы x_1, все входы x_2, ..., все входы x_n получим исходную $\Sigma_{\bar{f}}$ из $\Sigma_{g_1}, ..., \Sigma_{g_m}$ ($n \in \mathbb{N}_0$), ■.

Следствие: $L_{\text{Б}_0} \leq n \cdot 2^{n+1}$ ($n \in \mathbb{N}$)

Некоторые "арифметические" СФЭ

Определение: Сумматором порядка n называется СФЭ с $2n$ входами: $x_1, ..., x_n, y_1, ..., y_n$ - и $n+1$ выходами: $z_0, ..., z_n$ - таких что для любых значения на входах имеет место равенство:

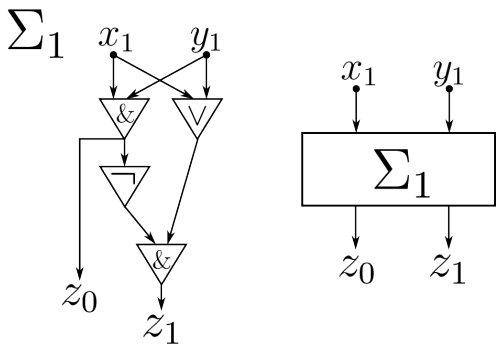
$$\nu(x_1, ..., x_n) + \nu(y_1, ..., y_n) = \nu(z_0, ..., z_n)$$

$$\nu(x_1, ..., x_n) = \sum_{i=1}^{n} 2^{n-i} x_i = |(x_1, ..., x_n)|$$

$$\begin{array}{r} (x_1 x_2 ... x_n)_2 \\ + (y_1 y_2 ... y_n)_2 \\ \hline (z_0 z_1 z_2 ... z_n)_2 \end{array}$$

Теорема 3: Существует сумматор Σ_n порядка n в базисе $\text{Б}_0 = \{xy, x \vee y, \bar{x}\}$ сложности $9n - 5$.

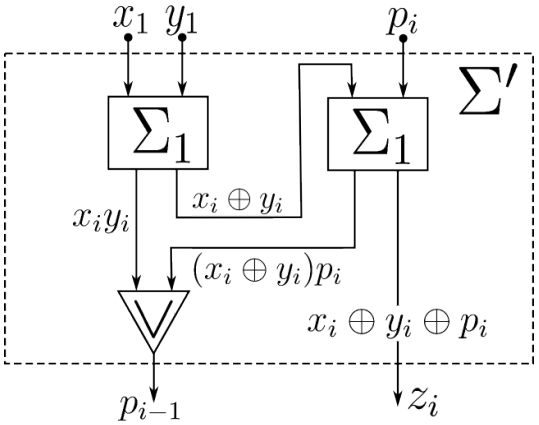
Доказательство: Сумматор порядка 1:



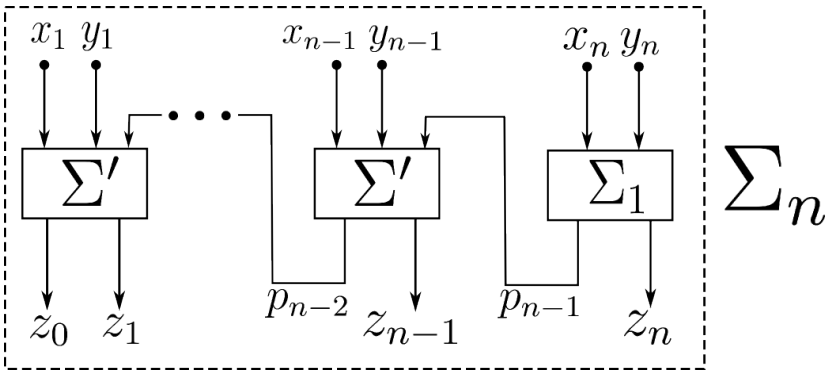
$$z_0 = x_1 y_1; z_1 = (\overline{x_1 y_1})(x_1 \vee y_1) = (\bar{x}_1 \vee \bar{y}_1)(x_1 \vee y_1) = x_1 \oplus y_1;$$

Ячейка сумматора p_i - перенос из разряда $i+1$ в разряд i $(i < n)$:

$$\begin{array}{rr} & p_i \\ + & x_i \\ - & y_i \\ \hline & p_{i-1} z_i \end{array}$$



$$p_{i-1} = m(x_i, y_i, p_i); L(\Sigma_1) = 4; L(\Sigma') = 9$$



$$L(\Sigma_n) = L(\Sigma_1) + (n-1)L(\Sigma') = 4 + 9(n-1) = 9n - 5, \blacksquare.$$

Определение: Вычитателем порядка n называется СФЭ с $2n$ входами $x_1, ..., x_n, y_1, ..., y_n$ и n выходами $z'_1, z'_2, ..., z'_n$ такая что:

если $\nu(x_1, ..., x_n) \geq \nu(y_1, ..., y_n)$, то $\nu(x_1, ..., x_n) - \nu(y_1, ..., y_n) = \nu(z'_1, ..., z'_n)$;
если $\nu(x_1, ..., x_n) < \nu(y_1, ..., y_n)$, то результат нам не важен.

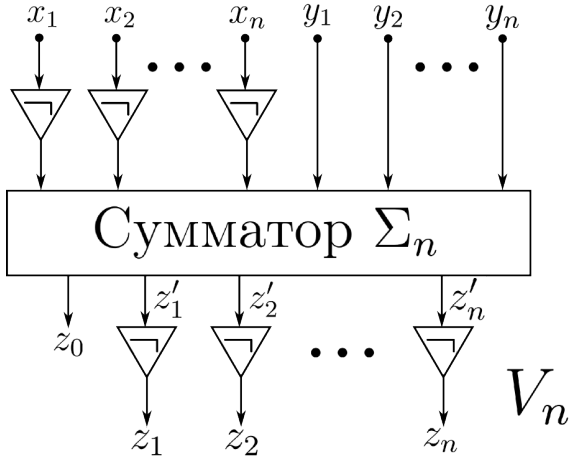
Теорема 4: Существует вычитатель V_n порядка n в базисе $\text{Б}_0 = \{xy, x \vee y, \bar{x}\}$ сложности $11n - 5$.

Доказательство:

$$\begin{array}{r} (x_1x_2...x_n)_2 \\ +\,(\bar{x}_1\bar{x}_2...\bar{x}_n)_2 \\ \hline (1\ 1\ \ ...\ \ 1)_2 \end{array}$$

$$|(x_1, ..., x_n)| + |(\bar{x}_1, ..., \bar{x}_n)| = 2^n - 1;$$

Если $|(x_1, ..., x_n)| \geq |(y_1, ..., y_n)|$, то $|(z'_1, ..., z'_n)| = (2^n - 1) - [((2^n - 1) - |(x_1, ..., x_n)|) + |(y_1, ..., y_n)|]$;



$$L(V_n) = 2n + L(\Sigma_n) = 11n - 5, \blacksquare.$$

Определение: Умножителем порядка n называется СФЭ с $2n$ входами $x_1, ..., x_n, y_1, ..., y_n$ и $2n$ выходами $z_1, z_2, ..., z_{2n}$ такая что:

$$\nu(x_1, ..., x_n) \cdot \nu(y_1, ..., y_n) = \nu(z_0, ..., z_{2n})$$

Замечание 1: При умножении n-разрядного двоично числа на одноразрядное двоичное число достаточно n конъюнкторов.

$$\begin{array}{r} (x_1x_2...x_n)_2 \\ \times\qquad (y_n)_2 \\ \hline (z'_1\ z'_2\ ...\ z'_n)_2 \end{array}$$

Замечание 2: Сложность умножителя порядка n в базисе $Б_0 = \{xy, x \vee y, \bar{x}\}$, моделирующее умножение в столбик есть $O(n^2)$.

$$
\begin{array}{cccccccc}
 & & & & & & \times & (x_1x_2...x_n)_2 \\
 & & & & & & & (y_1y_2...\ y_n)_2 \\
\hline
 & & & & z_{n1} & z_{n2} & \cdots & z_{nn} \\
+ & & & z_{(n-1)1} & z_{(n-1)2} & \cdots & z_{(n-1)n} & \\
 & & \cdots & \cdots & \cdots & \cdots & & \\
 & z_{11} & z_{12} & \cdots & z_{1n} & & & \\
\hline
 & z_1 & \cdots & \cdots & \cdots & \cdots & \cdots & z_{2n}
\end{array}
$$

Теорема 5: (А.А.Карацуба) Существует умножитель порядка n в базисе $Б_0 = \{xy, x \vee y, \bar{x}\}$ сложности $O(n^{\log_2 3})$.

Определение: Число $M(n)$ - минимальная сложность умножителя порядка n в базисе $Б_0$. [1]

Лемма 1: Существует константа c_1 ($c_1 > 0$) такая что:

$$\forall n \in \mathbb{N} : M(n+1) \leq M(n) + c_1 \cdot n$$

Доказательство: Рассмотрим

$$X = |(x_0, ..., x_n)|;\ Y = |(y_0, ..., y_n)|;$$
$$X_1 = |(x_1, ..., x_n)|;\ Y_1 = |(y_1, ..., y_n)|.$$

$X \cdot Y = (x_0 2^n + X_1)(y_0 2^n + Y_1) = x_0 y_0 2^{2n} + 2^n \cdot (x_0 Y_1 + y_0 X_1) + X_1 Y_1.$

Значит, $M(n+1) \leq M(n) + c_1 \cdot n, \blacksquare$.

Лемма 2: (основная) Существует константа c_2 ($c_2 > 0$) такая, что:

$$\forall n \in \mathbb{N} : M(2n) \leq 3M(n) + c_2 \cdot n$$

Доказательство: Рассмотрим

$$X = |(x_0, ..., x_n, x_{n+1}, ..., x_{2n})|;\ Y = |(y_0, ..., y_n, y_{n+1}, ..., y_{2n})|;$$
$$X_1 = |(x_1, ..., x_n)|;\ X_2 = |(x_{n+1}, ..., x_{2n})|;$$
$$Y_1 = |(y_1, ..., y_n)|;\ Y_2 = |(y_{n+1}, ..., y_{2n})|.$$

$X \cdot Y = (X_1 \cdot 2^n + X_2)(Y_1 \cdot 2^n + Y_2) = X_1 Y_2^{2n} + 2^n (X_1 Y_2 + X_2 Y_1) + X_2 Y_2 =$
$X_1 Y_1 2^{2n} + 2^n ((X_1 + X_2)(Y_1 + Y_2) - X_1 Y_1 - X_2 Y_2) + X_2 Y_2.$

Значит, $M(2n) \leq 3M(n) + c_2 \cdot n, \blacksquare$.

[1] Я и сам не понимаю доказательства этих трех лемм :C агр!

Лемма 3: Существует константа c_2 ($c_2 > 0$) такая, что:

$$\forall l \in \mathbb{N} : M(2^l) \leq c_3 \cdot 3^l$$

Доказательство: Обозначим $f(l) = \frac{M(2^l)}{3^l}$. По лемме 2:

$$f(l) \leq \frac{3M(2^{l-1}) + c_2 \cdot 2^{l-1}}{3^l} = f(l-1) + \frac{c_2}{3} \cdot \left(\frac{2}{3}\right)^{l-1}$$

$$f(l) \leq f(l-1) + \frac{c_2}{3} \cdot \left(\frac{2}{3}\right)^{l-1} \leq f(l-2) + \frac{c_2}{3} \cdot \left(\left(\frac{2}{3}\right)^{l-1} + \frac{2}{3}\right)^{l-2}\Big) \leq ...$$

$$... \leq \underbrace{f(1)}_{\leq const} + \frac{c_2}{3} \cdot \left(\left(\frac{2}{3}\right)^{l-1} + \left(\frac{2}{3}\right)^{l-2} + ... + \left(\frac{2}{3}\right)^{1}\right) \leq c_3, \blacksquare.$$

Доказательство: (теоремы 5) Рассмотрим произвольное $n \in \mathbb{N}(n \geq 2)$, тогда существует такое $l \in \mathbb{N}$, что $2^{l-1} < n \leq 2^l$.

Построим умножитель порядка 2^l и промоделируем в нем умножитель порядка n, подав нули на старшие $2^l - n$ разрядов каждого из переменных чисел.

$$M(n) \leq M(2^l) + \underset{x_1 \cdot \bar{x}_1 = 0}{2} \leq c_3 \cdot 3^l + 2 = 3c_3 \cdot 3^{l-1} + 2 \leq 3c_3(2^{l-1})^{\log_2 3} + 2 \leq 3c_3 n^{\log_2 3} + 2 = O(n^{\log_2 3}), \blacksquare.$$

Глава 4

Автоматы

Определение: Конечным инициальным автоматом называют шестерку объектов вида:

$$M = (A, B, C, F, G; c_1), \text{где}$$

- $A = \{a_1 ... a_\nu\}$ - входной алфавит;
- $B = \{b_1 ... b_\mu\}$ - выходной алфавит;
- $C = \{c_1 ... c_\lambda\}$ - внутренний алфавит (алфавит состояний);
- $F : A \times C \to B$ - функция выходов;
- $F : A \times C \to C$ - функция переходов;
- $c_1 \in C$ - начальное состояние.

Дискретное время: $t = 0, 1, 2, 3, ...$. $t = 0$ - автомат находится в состоянии c_1 и не запущен.
$t \in \mathbb{N}$ - в каждый натуральный момент времени (такт) t.
На вход автомата подается символ входного алфавита, по нему и состоянию в предыдущий такт вычисленный символ на выходе и текущее состояние.

$x(t)$ - символ на входе в момент t;
$z(t)$ - символ на выходе в момент t;
$q(t)$ - символ состояния в момент t.

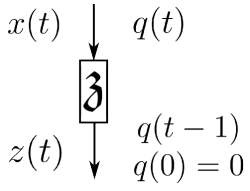
Работа автомата M может быть описана каноническими уравнениями:

$$\begin{cases} z(t) = F(x(t), q(t-1)) \\ q(t) = G(x(t), q(t-1)) \\ q(0) = c_1 \end{cases}$$

один из способов задания автомата.

Диаграмма Мура конечного инициального автомата $M = (A, B, C, F, G; c_1)$ - псевдограф $G_M = (V, E)$ с пометками на дугах, где $V = C$, и для каждой пары $(a, c) \in A \times C$ в G_M имеется дуга, исходящая из вершины c, заходящая в вершину $c' = G(a, c)$, и этой дуге приписано выражение $a(b)$, где $b = F(a, c)$. Начальное состояние помечается $*$.

Пример: Автомат единичной задержки $M_з = (A, B, C, F, G; c_1)$, где $A = B = C = \{0, 1\}$ и для любого слова бесконечной длины в алфавите A $\tilde{x}^\omega = x(1)x(2)x(3)...x(t)...$ слово, возникающее на выходе имеет вид: $\tilde{y}^\omega = 0x(1)x(2)...x(t-1)...$.

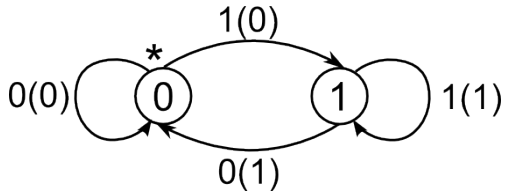


$$\begin{cases} z(t) = q(t-1) \\ q(t) = x(t) \\ q(0) = 0 \end{cases}$$

Каноническая таблица:

$q(t-1)$	$x(t)$	$q(t)$	$z(t)$
0	0	0	0
0	1	1	0
1	0	0	1
1	1	1	1

Диаграмма Мура $M_{\text{з}}$:



$A^\infty(B^\infty)$ - множество всех слов бесконечной длины в алфавите A (B).

Определение: Словарная функция - всякая функция вида: $\varphi : A^\infty \to B^\infty$.

Определение: Словарная функция $\varphi : A^\infty \to B^\infty$ называется автоматной тогда и только тогда, когда существует конечный инициальный автомат $M = (A, B, C, F, G; c_1)$, реализующий функцию φ (т.е. для любого слова $\tilde{a}^\omega = a(1)a(2)...a(t)... \in A^\infty$ при посимвольной подаче слова $\tilde{a}^\omega$ на вход M на выходе M посимвольно возникает слово $\tilde{b}^\omega = b(1)b(2)...b(t)... = \varphi(\tilde{a}^\omega)$).

Определение: Словарная функция $\varphi : A^\infty \to B^\infty$ называется детерминированной тогда и только тогда, когда для любого $l \in \mathbb{N}_0$, любого слова $\tilde{a} = a_{i_1}a_{i_2}...a_{i_l} \in A^l$ и любых двух слов $\tilde{a}'$ и $\tilde{a}''$ из A^∞, начинающихся со слова $\tilde{a}$, их образы $\tilde{b}' = \varphi(\tilde{a}')$ и $\tilde{b}'' = \varphi(\tilde{a}'')$ относительно функции φ имеют одинаковые начала длины l.

Примеры:

1. $\varphi(\tilde{x}^\omega) = \tilde{0}^\omega$ - детерминированная функция;
2. $\varphi(\tilde{x}^\omega) = 1\overset{1}{0}1\overset{2}{00}1\overset{3}{000}1\overset{4}{0000}1...$ - детерминированная функция;
3. $\varphi(\tilde{x}^\omega) = \begin{cases} \widetilde{0}^\omega, \text{если } \tilde{x}^\omega = \tilde{0}^\omega \\ \widetilde{1}^\omega, \text{если } \tilde{x}^\omega \neq \tilde{0}^\omega \end{cases}$ - не детерминированная функция.

Пусть $\varphi : A^\infty \to B^\infty$ - детерминированная функция, $\tilde{a} = a_{i_1}a_{i_2}...a_{i_l} \in A^l$. Определим по φ и $\tilde{a}$ остаточную функцию $\varphi_{\tilde{a}}$ следующим образом: если $\tilde{a}' = a_{i_1}a_{i_2}...a_{i_l}a(1)a(2)...a(t)...$ и при этом $\varphi(\tilde{a}') = b_{j_1}b_{j_2}...b_{j_l}b(1)b(2)...b(t)...$, то $\varphi_{\tilde{a}}(a(1)a(2)...a(t)...) = b(1)b(2)...b(t)...$.

Всякая остаточная функция для детерминированной функция - детерминированная функция.

Отношение равенства остаточных функций есть отношение эквивалентности, и оно разбивает множество всех остаточных функций данной детерминированной функции на классы эквивалентности.

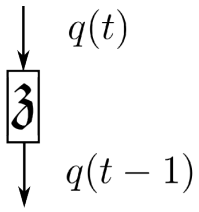
Определение: Ограниченно-детерминированной функцией (о.-д.ф.) называется всякая такая детерминированная функция $\varphi : A^\infty \to B^\infty$, у которой число классов эквивалентности остаточных функций - конечное.

Примеры:

1. $\varphi(\tilde{x}^\omega) = \tilde{0}^\omega$ - о.-д.ф.;
2. $\varphi(\tilde{x}^\omega) = 1\overset{1}{0}1\overset{2}{00}1\overset{3}{000}1\overset{4}{0000}1...$ - не о.-д.ф.

Утверждение: Класс автоматных функций вида: $\varphi : A^\infty \to B^\infty$ - совпадает с классом о.-д.ф. вида: $\varphi' : A^\infty \to B^\infty$.

Схемы из функциональных элементов [единичной] задержки



- элемент единичной задержки.

Базис ФЭ и элемента задержки $\mathfrak{z}$: $Б^{\mathfrak{z}} = Б \cup \{\mathfrak{z}\}$, где Б - базис ФЭ.
В частности, если $Б_0 = \{xy, x \vee y, \bar{x}\}$, то $Б_0^{\mathfrak{z}} = \{xy, x \vee y, \bar{x}, \mathfrak{z}\}$.

Определение: СФЭЗ в базисе $Б^{\mathfrak{z}}$ похоже на определение СФЭ в базисе Б, отличия таковы:

1. в СФЭЗ каждый ориентированный цикл (контур) обязан проходить через один элемент задержки;
2. входы СФЭЗ (истоки) помечаются различными переменными $x_1(t), ..., x_n(t)$;
3. выходы СФЭЗ (стоки) помечаются различными переменными $z_1(t), ..., z_m(t)$.

Теорема 1: Всякая СФЭЗ Σ (в базисе $Б^{\mathfrak{z}}$) есть конечный инициальный автомат.

Доказательство: Пусть у СФЭЗ Σ имеется n входов, помеченных $x_1(t), ..., x_n(t)$, и m выходов $z_1(t), ..., z_m(t)$, и r элементов единичной задержки, которым можно приписать переменные $q_1, ..., q_r$.

Положим $A = E_2^n$, $B = E_2^m$, $C = E_2^r$.

В СФЭЗ Σ "забудем" о наличии задержек, добавив к СФЭЗ вместо элементов задержки q_j новый вход $q_j(t-1)$ (на месте выхода q_j) и новый выход $q_j(t)$ (на месте входа q_j), $j = \overline{1,r}$ - получим СФЭ Σ' с входами $x_1(t), ..., x_n(t), q_1(t-1), ..., q_r(t-1)$ и выходами $z_1(t), ..., z_m(t), q_1(t), ..., q_r(t)$, реализующую некоторую систему булевых функций:

$$\begin{cases} z_i(t) = f_i(x_1(t), ..., x_n(t), q_1(t-1), ..., q_r(t-1)), i = \overline{1,m} \\ q_j(t) = g_j(x_1(t), ..., x_n(t), q_1(t-1), ..., q_r(t-1)), j = \overline{1,r} \end{cases}$$

СФЭ Σ' срабатывает в каждый такт t.

Положим:

$$X(t) = (x_1(t), ..., x_n(t));$$
$$Z(t) = (z_1(t), ..., z_m(t));$$
$$Q(t) = (q_1(t), ..., q_r(t));$$
$$F = (f_1(t), ..., f_m(t));$$
$$G = (g_1(t), ..., g_r(t)).$$

Тогда с учетом наличия задержки функционирование СФЭЗ Σ описывается каноническими уравнениями:

$$\begin{cases} Z(t) = F(X(t), Q(t-1)) \\ Q(t) = G(X(t), Q(t-1)) \\ Q(0) = (\underbrace{0, 0, ..., 0}_{r}) \end{cases}$$

Следовательно СФЭЗ Σ - есть конечный инициальный автомат, ■.

Определение: Пусть $\varphi : A^\infty \to B^\infty$ - автоматная функция, а Σ - СФЭЗ с n входами $x_1(t), ..., x_n(t)$ и m выходами $z_1(t), ..., z_m(t)$. Говорят, что СФЭЗ Σ моделирует автоматную функцию φ тогда и только тогда, когда существует инъективные (кодирования) отображения $K_1 : A \to E_2^n$ и $K_2 : B \to E_2^n$ такие, что если для любого слова $\tilde{a} = a(1)a(2)...a(t)... \in A^\infty$ $\varphi(\tilde{a}) = b(1)b(2)...b(t)... \in B^\infty$, то при последовательной подаче на входы Σ наборов $K_1(a(1)), K_1(a(2)), ..., K_1(a(t)), ...$ на входах Σ будут последовательно появляться наборы $K_2(b(1)), K_2(b(2)), ..., K_2(b(t)), ...$ соответственно.

Теорема 2: Для любой автоматной функции $\varphi : A^\infty \to B^\infty$ существует моделирующая ее СФЭЗ Σ в базисе $Б_0^з = \{xy, x \vee y, \bar{x}, з\}$.

Доказательство: Т.к. φ - автоматная функция, то существует реализующий φ конечный автомат $M = (A, B, C, F, G; c_1)$.

Пусть $|A| = \nu$, $|B| = \mu$, $|C| = r$. Положим $n = \lceil log_2 \nu \rceil$, $m = \lceil log_2 \mu \rceil$, $\rho = \lceil log_2 r \rceil$. Тогда существуют инъективные отображения: $K_1 : A \to E_2^n$, $K_2 : B \to E_2^m$, $K_3 : C \to E_2^\rho$, причем $K_3(c_1) = (\underbrace{0, 0, ...0}_{\rho})$.

Автомат M описывается системой:

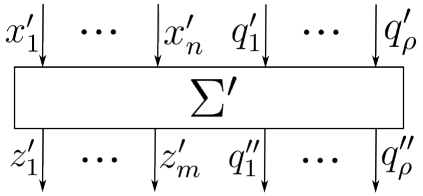
$$\begin{cases} Z(t) = F(X(t), Q(t-1)) \\ Q(t) = G(X(t), Q(t-1)) \\ Q(0) = c_1 \end{cases} \quad (*)$$

Закодируем эту систему с помощью кодирований K_1, K_2, K_3:

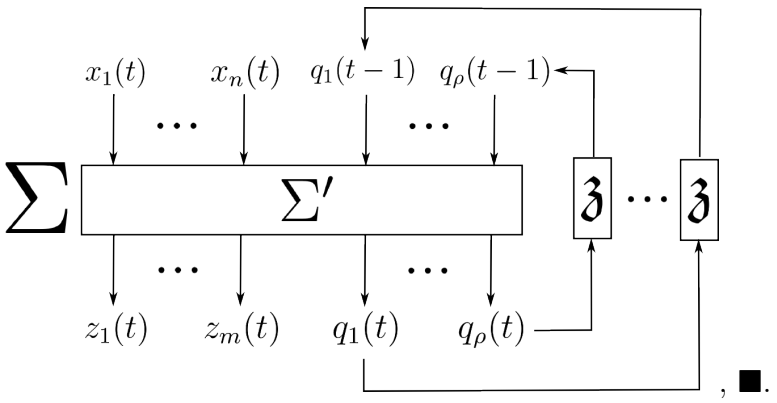
$$\begin{cases} z_i(t) = f_i(x_1(t), ..., x_n(t), q_1(t-1), ..., q_\rho(t-1)), i = \overline{1, m} \\ q_j(t) = g_j(x_1(t), ..., x_n(t), q_1(t-1), ..., q_\rho(t-1)), j = \overline{1, \rho} \\ q_j(0) = 0 \end{cases} \quad (**)$$

Здесь функции f_i, g_j - вообще говоря, не всюду определенные булевы функции. Доопределим их произвольным образом. Тогда существует СФЭ Σ' в базисе $Б_0 = \{xy, x \vee y, \bar{x}\}$ с входами $x'_1, ..., x'_n, q'_1, ..., q'_\rho$ и выходами $z'_1, ..., z'_m, q''_1, ..., q''_\rho$, реализующие систему функций:

$$\begin{cases} z'_i = f_i(x'_1, ..., x'_n, q'_1, ..., q'_\rho), i = \overline{1, m} \\ q''_j = g_j(x'_1, ..., x'_n, q'_1, ..., q'_\rho), j = \overline{1, \rho} \end{cases}$$



Но тогда, легко видеть, что следующая СФЭЗ Σ моделирует функцию φ:



, ■.

Эксперименты с автоматами

Определение: Конечный неинициальный автомат - $M = (A, B, C, F, G)$ (в отличие от ициниального автомата не указано начальное состояние).

Задача: Инициальный автомат M мог находиться в одном из двух начальных состояний c', c''. Определить, если это возможно, в каком именно.

Пусть автомат M находился в состоянии c и на его вход последовательно было подано слово $\hat{a} = a_{i_1}a_{i_2}...a_{i_l} \in A^*$ при этом автомат перешел в состояние $\hat{c}$ и на его входе посимвольно появилось слово $\hat{b} = b_{j_1}b_{j_2}...b_{j_l} \in B^*$. Тогда положим $\tilde{F}(\hat{a}, c) = \hat{b}$, $\tilde{G}(\hat{a}, c) = \hat{c}$. Функции:

$$\tilde{F} : A^* \times C \to B^*$$
$$\tilde{G} : A^* \times C \to C$$

- обобщения функций F, G.

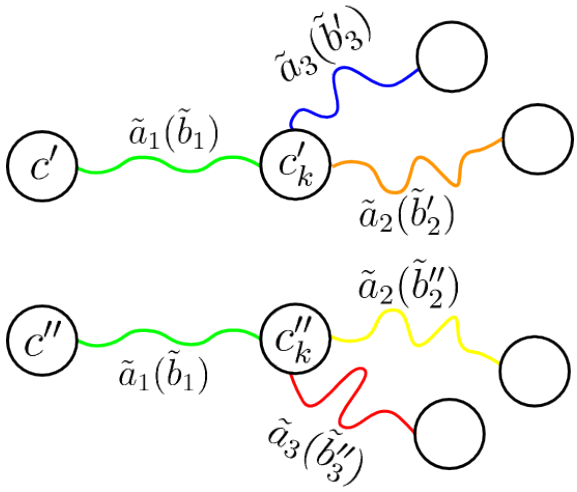
Определение: Два состояния c', c'' автомата M называются отличными тогда и только тогда, когда существует слово $\hat{a} \in A^*$ такое, что $\tilde{F}(\hat{a}, c') = \tilde{F}(\hat{a}, c'')$. В этом случае $\hat{a}$ называется экспериментально отличающим состояния c' c'' автомата M.

Лемма 1: Пусть состояния c' и c'' автомата M отличимы экспериментом длины p и не отличимы никаким более коротким экспериментом. Тогда для любого $k = \overline{1, p}$ найдутся два состояния c'_k, c''_k автомата M, отличимые экспериментом длины k и не отличимы никаким более коротким экспериментом.

Доказательство: Пусть $\tilde{a}$ - эксперименты длины p, отличающий c' и c''. Представим a в виде $\tilde{a} = \tilde{a}_1\tilde{a}_2$, где длина $\tilde{a}_2$ есть $k = l(\tilde{a}_2)$.

Пусть $G(\tilde{a}_1, c') = c'_k$, $G(\tilde{a}_1, c'') = c''_k$. $\tilde{F}(\tilde{a}_1\tilde{a}_2, c') = \tilde{b}_1\tilde{b}'_2$, $\tilde{F}(\tilde{a}_1\tilde{a}_2, c'') = \tilde{b}_1\tilde{b}''_2$, где $l(\tilde{b}'_2) = l(\tilde{b}''_2) = k$.

Т.к. $\tilde{a}_1\tilde{a}_2$ - самый короткий эксперимент, отличающий c' и c'', то слова $\tilde{b}_1\tilde{b}'_2$ и $\tilde{b}_1\tilde{b}''_2$ отличаются лишь последними символами. А т.к. $\tilde{F}(\tilde{a}_2, c'_k) = \tilde{b}'_2$, $\tilde{F}(\tilde{a}_2, c''_k) = \tilde{b}''_2$, то состояния c'_k и c''_k отличаются экспериментом длины k. Если существует эксперимент $\tilde{a}_3$ длины $k' < k$, отличающий c'_k и c''_k, то эксперименты $\tilde{a}_1\tilde{a}_3$ длины $(p-k)+k' \leq p$ отличает c' и c'', что невозможно. Значит, состояния c'_k и c''_k - искомые, ■.



Теорема 3: (Э. Ф. Мура об одном автомате) Пусть c' и c'' - отличные состояния конечного неинициального автомата $M = (A, B, C, F, G)$ причем $|C| = r$. Тогда существует эксперимент $\tilde{a}$, отличающий c' и c'', и такой, что $l(\tilde{a}) \leq r - 1$.

Доказательство: Пусть $\tilde{a}$ - кратчайший эксперимент, отличающий c' и c'', и $l(\tilde{a}) = p$.

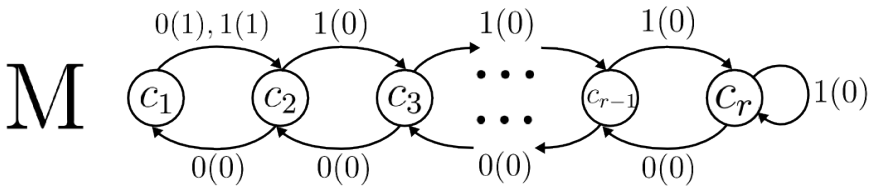
Введем на множестве C бинарное отношение $\mathcal{R}_k$ следующим образом: $(c_i, c_j) \in \mathcal{R}_k \Leftrightarrow c_i$ и c_j не отличимы никаким экспериментом длины $k \in \mathbb{N}_0$. $\mathcal{R}_k$ - рефлексивно, симметрично и транзитивно, следовательно $\mathcal{R}_k$ - отношение эквивалентности. Тогда по отношению $\mathcal{R}_k$ множество C разбивают на классы эквивалентности $C_1^{(k)}, C_2^{(k)}, ..., C_{s(k)}^{(k)}$ ($s(k)$ - число классов эквивалентности относ. $\mathcal{R}_k$).

Если c_i, c_j лежат в одном классе эквивалентности относительно $\mathcal{R}_k$, то они не отличимы экспериментами длины k, а если в разных - то отличимы экспериментами длины k, а значит и экспериментами длины, большей чем k. Значит, $1 = s(0) \leq s(1) \leq s(2) \leq ... \leq S(p)$. Но по лемме 1: $\forall k = \overline{1,p} : s(k-1) < s(k)$ - следовательно

$$1 = s(0) < s(1) < s(2) < \ldots < s(p–1) < s(p) \leq r \Rightarrow p + 1 \leq r \Rightarrow p \leq r - 1, \blacksquare.$$

Теорема 4: Существует автомат M с r состояниями и два его отличимых состояния c_{r-1}, c_r для которых длина кратчайшего отличающего их эксперимента равна $r-1$ (т.е. оценка в т. Мура неулучшаема).

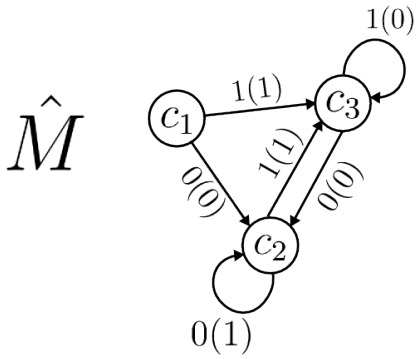
Доказательство:



Чтобы отличить c_{r-1} и c_r необходимо достичь из c_{r-1} состояния c_1 и подать на вход еще один символ. Тогда $a = \underbrace{00...0}_{r-1}$ - кратчайший эксперимент, отличающий c_{r-1} и c_r, $\blacksquare$.

Теорема 5: Существует автомат $\hat{M}$ с тремя попарно отличающимися состояниями, в котором невозможно одним экспериментом определить начальное состояние.

Доказательство:



Пара состояний (c', c'')	Эксперимент, отл. (c', c'')
(c_1, c_2)	1
(c_1, c_3)	0
(c_2, c_3)	0

Пусть существует эксперимент $\tilde{a}$, определяющий начальное состояние. Если $\tilde{a}$ начинается с 0, то он не может отличить c_1 от c_2, а если с 1, то не может отличить c_1 от c_3, $\blacksquare$.