**МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ М. В. ЛОМОНОСОВА**

**Факультет вычислительной математики и кибернетики**

В. Б. Алексеев

# Лекции по дискретной математике

**Москва 2004**

УДК 510.5, 519.71
ББК 22.12:22.18
А47

**Алексеев В. Б. Лекции по дискретной математике** (учебное пособие для студентов) — М.: Издательский отдел факультета ВМиК МГУ (лицензия ИД № 05899 от 24.09.2001), 2004 г. — ?? с.

Рецензенты: проф. Ложкин С. А., д. ф.-м. н.
??

Печатается по решению Редакционно-издательского совета факультета вычислительной математики и кибернетики МГУ им. М. В. Ломоносова

??

ISBN 5-89407-147-X

# Оглавление

**Введение** 5

**Глава I. Функции алгебры логики** 6

§1. Функции алгебры логики. Равенство функций. Тождества для элементарных функций 6
§2. Теорема о разложении функции алгебры логики по переменным. Теорема о совершенной дизъюнктивной нормальной форме 9
§3. Полные системы. Примеры полных систем 11
§4. Теорема Жегалкина о представимости функции алгебры логики полиномом 12
§5. Понятие замкнутого класса. Замкнутость классов $T_0$, $T_1$ и $L$ 14
§6. Двойственность. Класс самодвойственных функций, его замкнутость 16
§7. Класс монотонных функций, его замкнутость 18
§8. Лемма о несамодвойственной функции 19
§9. Лемма о немонотонной функции 19
§10. Лемма о нелинейной функции 20
§11. Теорема Поста о полноте системы функций алгебры логики 21
§12. Теорема о максимальном числе функций в базисе алгебры логики 22
§13. Теорема о предполных классах 23
§14. *k*-значные функции. Теорема о существовании конечной полной системы в множестве *k*-значных функций 24

**Глава II. Основы теории графов** 26

§15. Основные понятия теории графов. Изоморфизм графов. Связность 26
§16. Деревья. Свойства деревьев 29
§17. Корневые деревья. Верхняя оценка их числа 31
§18. Геометрическая реализация графов. Теорема о реализации графов в трёхмерном пространстве 33
§19. Планарные (плоские) графы. Формула Эйлера 33
§20. Доказательство непланарности графов $K_5$ и $K_{3,3}$. Теорема Понтрягина-Куратовского 35
§21. Теорема о раскраске планарных графов в пять цветов 37

**Глава III. Основы теории управляющих систем** **40**

§22. Схемы из функциональных элементов. Реализация функций алгебры логики схемами 40
§23. Сумматор. Верхняя оценка сложности сумматора. Вычитатель 43
§24. Метод Карацубы построения схемы для умножения, верхняя оценка её сложности 45
§25. Дешифратор. Асимптотика сложности дешифратора. Верхняя оценка сложности реализации произвольной функции алгебры логики 48
§26. Мультиплексор. Верхняя оценка сложности мультиплексора. Метод Шеннона 50
§27. Шифратор. Верхняя оценка сложности шифратора 53

**Глава IV. Основы теории кодирования** **54**

§28. Алфавитное кодирование. Теорема Маркова о взаимной однозначности алфавитного кодирования 54
§29. Неравенство Макмиллана 56
§30. Существование префиксного кода с заданными длинами кодовых слов 57
§31. Оптимальные коды, их свойства 58
§32. Теорема редукции 60
§33. Коды с исправлением $r$ ошибок. Оценка функции $M_r(n)$ 61
§34. Коды Хэмминга. Оценка функции $M_1(n)$ 63

**Глава V. Основы теории конечных автоматов** **66**

§35. Понятие ограниченно детерминированных (автоматных) функций, их представление диаграммой Мура. Единичная задержка 66
§36. Схемы из функциональных элементов и элементов задержки. Автоматность осуществляемых ими отображений 68
§37. Моделирование автоматной функции схемой из функциональных элементов и элементов задержки 69
§38. Теорема Мура. Теорема об отличимости состояний двух автоматов 71

# Введение

# Глава I. Функции алгебры логики

## §1. Функции алгебры логики. Равенство функций. Тождества для элементарных функций

### 1°. Функции алгебры логики.

**Определение 1.** Пусть $E_2 = \{0, 1\}$ — основное множество (исходный алфавит значений переменных), тогда $E_2^n = \{(\alpha_1, \ldots, \alpha_n) \mid \forall i\ \alpha_i \in E_2\}$. *Всюду определённой булевой функцией* назовём отображение $f(x_1, \ldots, x_n)$: $E_2^n \to E_2$. Такую функцию можно задать таблично. Например, для $n = 1$:

| $x$ | 0 | 1 | $x$ | $\overline{x}$ |
|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 1 |
| 1 | 0 | 1 | 1 | 0 |

При этом функция 0 называется *константой нулём*, функция 1 — *константой единицей*, функция $x$ — *тождественной*, а функция $\overline{x}$ — *отрицанием* $x$. При этом для последней функции используется также иное обозначение: $\overline{x} \equiv \neg x$.

Для $n = 2$:

| $x$ | $y$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ | $f_7$ |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 |

При заполнении таблицы столбцы переменных заполняются в лексикографическом порядке (по возрастанию двоичных чисел).

$f_1$ — *дизъюнкция, функция «или», логическое сложение*: $f_1 = x \vee y$.

$f_2$ — *конъюнкция*: $f_2 = x \cdot y = x \,\&\, y = xy$.

$f_3$ — *сложение по модулю 2 (исключающее «или»)*: $f_3 = x \oplus y = x + y$.

$f_4$ — *импликация*: $f_4 = x \to y$.

$f_5$ — *эквивалентность*: $f_5 = x \sim y = \overline{x \oplus y}$.

$f_6$ — *штрих Шеффера*: $f_6 = x \mid y = \overline{xy}$.

$f_7$ — *стрелка Пирса*: $f_7 = x \downarrow y = \overline{x \vee y}$.

**Лемма (о числе слов).** В алфавите $A = \{a_1, \ldots, a_r\}$ из $r$ букв можно построить ровно $r^m$ различных слов длины $m$.

**Доказательство.** Проведём индукцию по $m$. Для $m = 1$ утверждение очевидно. Пусть утверждение леммы верно для $m - 1$, то есть существует ровно $r^{m-1}$ различных слов длины $m - 1$. Для каждого такого слова длины $m - 1$ существует ровно $r$ возможностей добавить одну букву в конец. Так как всего слов длины $m - 1$ — $r^{m-1}$, то различных слов длины $m$ получится $r \cdot r^{m-1} = r^m$. Лемма доказана.

Рассмотрим таблицу некоторой функции алгебры логики от $n$ переменных.

$$
\begin{array}{c|cccc|c}
 & x_1 & x_2 & \text{K} & x_n & f \\
2^n & 0 & 0 & \text{K} & 0 & \alpha_0 \\
 & 0 & 0 & \text{K} & 1 & \alpha_1 \\
 & \text{K} & \text{K} & \text{K} & \text{K} & \text{K} \\
 & 1 & 1 & \text{K} & 1 & \alpha_{2^n-1}
\end{array}
$$

Для её задания необходимо и достаточно определить её значения на $2^n$ наборах. Таким образом, получаем, что всего различных функций от $n$ переменных столько, сколько существует различных наборов из нулей и единиц длины $2^n$, т.е. $2^{2^n}$.

Используя последний факт можно, например, получить оценку числа функций от 10 переменных. Всего таких функций будет $2^{2^{10}} = 2^{1024} > 2^{1000} = \left(2^{10}\right)^{100} > \left(1000\right)^{100} = 10^{300}$. Таким образом, при росте числа переменных число функций возрастает очень быстро, и их табличное задание становится неудобным.

**2°. Равенство функций.** В обычной алгебре справедливо равенство $x + y - y = x$, несмотря на то, что в левой части записана функция от двух переменных, а в правой — от одной. Таким образом, функции от разного числа переменных могут быть одинаковыми, что даёт повод ввести понятие *существенных и фиктивных переменных*.

**Определение 2.** Переменная $x_i$ называется *существенной переменной функции алгебры логики* $f(x_1, \ldots, x_n)$, если существуют такие $\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n \in E_2$, что

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

Такие наборы, отличающиеся лишь одной переменной $x_i$, называются *соседними по* $x_i$. В противном случае переменная $x_i$ называется *фиктивной*.

Если $x_i$ — фиктивная переменная функции $f$, то функция $f$ однозначно определяется некоторой функцией $g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$. Таблицу любой функции можно расширить введением любого числа фиктивных переменных.

**Определение 3.** Две функции алгебры логики называются *равными*, если одну из них можно получить из другой путём добавления и изъятия любого числа фиктивных переменных.

**3°. Формулы.**

**Определение 4.** Пусть имеется некоторое множество функций

$$A = \{f_1(\ldots), f_2(\ldots), \ldots, f_n(\ldots), \ldots\}.$$

Введем понятие формулы над $A$:

1) Любая функция из $A$ называется формулой над $A$.
2) Если $f(x_1, \ldots, x_n) \in A$ и для любого $i$ $H_i$ — либо переменная, либо формула над $A$, то выражение вида $f(H_1, H_2, \ldots, H_n)$ является также формулой над $A$.
3) Только те объекты называются формулами над $A$, которые можно построить с помощью пунктов 1 и 2 данного определения.

**Замечание.** Среди $H_1, H_2, \ldots, H_n$ вполне могут быть одинаковые.

**4°. Основные эквивалентности.**

1. *Коммутативность*:
   $x \vee y = y \vee x$ ;
   $xy = yx$ ;
   $x \oplus y = y \oplus x$ ;
   $x \sim y = y \sim x$ .
2. *Ассоциативность*:
   $(x \vee y) \vee z = x \vee (y \vee z) = x \vee y \vee z$ ;
   $(xy)\, z = x\, (yz) = xyz$ ;
   $(x \oplus y) \oplus z = x \oplus (y \oplus z) = x \oplus y \oplus z$.
3. *Дистрибутивность*:
   $(x \oplus y)\, z = (xz) \oplus (yz)$ ;
   $(x \vee y)\, z = (xz) \vee (yz)$ ;
   $(xy) \vee z = (x \vee z) \cdot (y \vee z)$.
4. $\overline{\overline{x}} = x$ ,
   *правила де Моргана*:
   $\overline{x \vee y} = \overline{x} \cdot \overline{y}$ ,
   $\overline{x \cdot y} = \overline{x} \vee \overline{y}$ .

5. *Законы поглощения.*

$x \vee x = x$
$x \cdot x = x$
$x \vee \overline{x} = 1$
$x \cdot \overline{x} = 0$
$x \vee 1 = 1$
$x \cdot 1 = x$
$x \vee 0 = x$
$x \cdot 0 = 0.$

6. $x \mid y = \overline{x \cdot y}$
$x \downarrow y = \overline{x \vee y}$
$x \to y = \overline{x} \vee y$
$x \oplus y = (x \cdot \overline{y}) \vee (\overline{x} \cdot y)$
$x \sim y = \overline{x \oplus y} = (xy) \vee (\overline{x} \quad \overline{y})$

Приоритет конъюнкции выше, чем приоритеты дизъюнкции и суммы по модулю 2. Благодаря этому, часто удаётся опустить ряд ненужных скобок. Имеют место следующие очевидные утверждения:

$x_1 \cdot x_2 \cdot \ldots \cdot x_n = 1 \Leftrightarrow \forall i\ x_i = 1,$
$x_1 \vee x_2 \vee \ldots \vee x_n = 1 \Leftrightarrow \exists i\colon x_i = 1.$

**Определение 5.** *x в степени сигма* называется функция

$$x^{\sigma} = \begin{cases} x, & \sigma = 1 \\ \overline{x}, & \sigma = 0 \end{cases};$$

$x^{\sigma} = 1 \Leftrightarrow x = \sigma.$

## §2. Теорема о разложении функции алгебры логики по переменным. Теорема о совершенной дизъюнктивной нормальной форме

**Теорема 1 (о разложении функции алгебры логики по переменным)**. Для любой функции алгебры логики $f(x_1, \ldots, x_n)$ и для любого $k$ $(1 \le k \le n)$ справедливо следующее равенство:

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

**Доказательство.** Для любого набора $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ вычислим значение правой части на этом наборе. Как только хотя бы один из сомножителей будет равен нулю, вся конъюнкция обратится в нуль. Таким образом, из ненулевых конъюнкций останется лишь одна — та, в которой $\alpha_i = \sigma_i$ для $i = 1, \ldots, k$, и

$$\bigvee_{(\sigma_1,\sigma_2,\text{K},\sigma_k)\in E_2^k} \alpha_1^{\sigma_1}\cdot\alpha_2^{\sigma_2}\cdot\text{K}\cdot\alpha_k^{\sigma_k} f\left(\sigma_1,\sigma_2,\text{K},\sigma_k,\alpha_{k+1},\text{K},\alpha_n\right) =$$

$$= 0\vee\text{K}\vee 0\vee\alpha_1^{\alpha_1}\cdot\alpha_2^{\alpha_2}\,\text{L}\;\alpha_k^{\alpha_k} f\left(\alpha_1,\text{K},\alpha_n\right),$$

а в силу того, что $x^x = 1$, указанное выражение равно $f(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Теорема доказана.

**Следствие 1.** Разложение произвольной функции алгебры логики по одной переменной имеет вид

$$f\left(x_1,x_2,\text{K},x_n\right) = \overline{x_1} f\left(0,x_2,\text{K},x_n\right)\vee x_1 f\left(1,x_2,\text{K},x_n\right).$$

**Следствие 2 (теорема о совершенной дизъюнктивной нормальной форме).** Для любой функции алгебры логики $f(x_1, x_2, \ldots, x_n)$, отличной от тождественного нуля, справедливо следующее представление:

$$f\left(x_1,\text{K},x_n\right) = \bigvee_{(\sigma_1,\text{K},\sigma_n):f(\sigma_1,\text{K},\sigma_n)=1} x_1^{\sigma_1}x_2^{\sigma_2}\Lambda\; x_n^{\sigma_n}.$$

**Доказательство.** Пусть функция $f(x_1, x_2,\ldots, x_n)$ отлична от тождественного нуля. Напишем разложение этой функции по $k = n$ переменным:

$$f\left(x_1,\text{K},x_n\right) = \bigvee_{(\sigma_1,\sigma_2,\text{K},\sigma_n)\in E_2^n} x_1^{\sigma_1}x_2^{\sigma_2}\,\text{K}\;x_n^{\sigma_n} f\left(\sigma_1,\sigma_2,\text{K},\sigma_n\right),$$

что можно переписать в эквивалентном виде

$$\bigvee_{(\sigma_1,\text{K},\sigma_n):f(\sigma_1,\text{K},\sigma_n)=1} x_1^{\sigma_1}x_2^{\sigma_2}\,\text{K}\;x_n^{\sigma_n} f\left(\sigma_1,\text{K},\sigma_n\right)\vee$$

$$\vee\bigvee_{(\sigma_1,\text{K},\sigma_n):f(\sigma_1,\text{K},\sigma_n)=0} x_1^{\sigma_1}x_2^{\sigma_2}\,\text{K}\;x_n^{\sigma_n} f\left(\sigma_1,\text{K},\sigma_n\right).$$

Учитывая, что в первой дизъюнкции все значения функции равны единице, а вторая обнуляется из-за того, что все значения функции в ней равны нулю, получаем утверждение следствия. Следствие доказано.

**Теорема 2 (о совершенной конъюнктивной нормальной форме).** Для любой функции алгебры логики $f(x_1, x_2, \ldots, x_n)$, отличной от тождественной единицы, справедливо представление

$$f\left(x_1,\text{K},x_n\right) = \mathop{\&}_{\substack{(\sigma_1,\sigma_2,\text{K},\sigma_n)\\ f(\sigma_1,\sigma_2\text{K},\sigma_n)=0}} \left(x_1^{\bar{\sigma}_1}\vee x_2^{\bar{\sigma}_2}\vee\text{K}\vee x_n^{\bar{\sigma}_n}\right).$$

## §3. Полные системы. Примеры полных систем (с доказательством полноты)

**Определение.** Множество функций алгебры логики $A$ называется *полной системой* (в $P_2$), если любую функцию алгебры логики можно выразить формулой над $A$.

**Теорема 3.** Система $A = \{\vee, \&, \neg\}$ является полной.

**Доказательство.** Если функция алгебры логики $f$ отлична от тождественного нуля, то $f$ выражается в виде совершенной дизъюнктивной нормальной формы, в которую входят лишь дизъюнкция, конъюнкция и отрицание. Если же $f \equiv 0$, то $f = x \cdot \bar{x}$. Теорема доказана.

**Лемма 2.** Если система $A$ — полная, и любая функция системы $A$ может быть выражена формулой над некоторой другой системой $B$, то $B$ — также полная система.

**Доказательство.** Рассмотрим произвольную функцию алгебры логики $f(x_1,\ldots,x_n)$ и две системы функций: $A=\{g_1, g_2, \ldots\}$ и $B=\{h_1, h_2, \ldots\}$. В силу того, что система $A$ полна, функция $f$ может быть выражена в виде формулы над ней: $f(x_1,\text{K},x_n) = \mathfrak{I}[g_1, g_2,\text{K}]$, где $g_i = \mathfrak{R}_i[h_1, h_2,\text{K}]$, то есть функция $f$ представляется в виде $f(x_1,\text{K},x_n) = \mathfrak{I}[\mathfrak{R}_1, \mathfrak{R}_2,\text{K}]$, иначе говоря, может быть представлена формулой над $B$. Перебирая таким образом все функции алгебры логики, получим, что система $B$ также полна. Лемма доказана.

**Теорема 4.** Следующие системы являются полными в $P_2$:

1) $\{x \vee y, \bar{x}\}$;
3) $\{x \mid y\}$;
2) $\{x \cdot y, \bar{x}\}$;
4) $\{x \cdot y,\ x \oplus y,\ 1\}$.

**Доказательство.** 1) Известно (теорема 3), что система $A=\{x \vee y, x \cdot y, \bar{x}\}$ полна. Покажем, что полна система $B=\{x \vee y, \bar{x}\}$. Действительно, из закона де Моргана $\overline{x \cdot y} = \bar{x} \vee \bar{y}$ получаем, что $x \cdot y = \overline{\bar{x} \vee \bar{y}}$, то есть конъюнкция выражается через дизъюнкцию и отрицание, и все функции системы $A$ выражаются формулами над системой $B$. Согласно лемме 2 система $B$ полна.

2) Аналогично пункту 1: $\overline{x \vee y} = \bar{x} \cdot \bar{y} \Leftrightarrow x \vee y = \overline{\bar{x} \cdot \bar{y}}$ и из леммы 2 следует истинность утверждения пункта 2.

3) $x|x=\bar{x}$, $x\cdot y=\overline{x|y}=(x|y)|(x|y)$ и, согласно лемме 2, система полна.

4) $\bar{x}=x\oplus 1$ и, согласно лемме 2, система полна.

Теорема доказана.

## §4. Теорема Жегалкина о представимости функции алгебры логики полиномом

**Определение 1.** *Монотонной конъюнкцией* от переменных $x_1,\ldots,x_n$ называется любое выражение вида $x_{i_1}\cdot x_{i_2}\cdot x_{i_3}\Lambda\ x_{i_s}$, где $s\geq 1$, $1\leq i_j\leq n$ $\forall j=1,2,\ldots,s$, все переменные различны ($i_j\neq i_k$, если $j\neq k$); либо просто 1.

**Определение 2.** *Полиномом Жегалкина* над $x_1, \ldots, x_n$ называется выражение вида

$$K_1\oplus K_2\oplus K_3\oplus\ldots\oplus K_l,$$

где $l\geq 1$ и все $K_j$ суть различные монотонные конъюнкции над $x_1, \ldots, x_n$; либо константа 0.

**Теорема 5 (теорема Жегалкина).** Любую функцию алгебры логики $f(x_1, \ldots, x_n)$ можно единственным образом выразить полиномом Жегалкина над $x_1, \ldots, x_n$.

**Доказательство.** 1) Докажем существование полинома. Система $\{x\cdot y, x\oplus y, 1\}$ полна, следовательно, любую функцию алгебры логики $f(x_1, \ldots, x_n)$ можно реализовать формулой над $\{x\cdot y, x\oplus y, 1\}$.

*a)* Пользуясь дистрибутивностью, раскрываем все скобки в этой реализации и получаем, что $f(x_1, \ldots, x_n) = K_1'\oplus K_2'\oplus\ldots\oplus K_l'$, где любая $K_i'$ — конъюнкция переменных и единиц.

*b)* Преобразуем все полученные конъюнкции в монотонные, пользуясь при этом коммутативностью и соотношениями $x\cdot x=x$, $1\cdot 1=1$ и $A\cdot 1=A$. Очевидно, все конъюнкции станут монотонными.

*c)* Преобразуем полученную сумму в полином Жегалкина, пользуясь при этом соотношениями $A\oplus A=A$ и $A\oplus 0=A$. В результате получим либо

$$K_{i_1}\oplus K_{i_2}\oplus K_{i_3}\oplus\mathrm{L}\ \oplus K_{i_m}$$

либо константу 0.

Существование доказано.

2) Докажем единственность представления. Подсчитаем число различных всевозможных монотонных конъюнкций от $n$ переменных. Для этого составим таблицу вида

| | $x_1$ | $x_2$ | $x_3$ | $x_4$ |
|---|---|---|---|---|
| $x_1x_2x_4$ | 1 | 1 | 0 | 1 |
| $x_2x_3$ | 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 0 | 0 |

,

где каждой переменной соответствует единица, если она присутствует в монотонной конъюнкции и ноль в противном случае. При этом константе единице поставим в соответствие нулевой набор. Очевидно, что построенное отображение взаимно однозначно. Следовательно, всего различных монотонных конъюнкций от $n$ переменных — $2^n$. Построим аналогичное взаимно однозначное отображение между всевозможными суммами монотонных конъюнкций и векторами длины $2^n$ — числа конъюнкций. Для этого составим таблицу вида

| | $xy$ | $x$ | $y$ | 1 |
|---|---|---|---|---|
| $xy+1$ | 1 | 0 | 0 | 1 |
| 0 | 0 | 0 | 0 | 0 |

,

где под соответствующей монотонной конъюнкцией стоит единица, если она входит в данную сумму, и ноль, если не входит. При этом константе ноль ставится в соответствие нулевой набор. Очевидно, такое отображение взаимно однозначно. Всего таких различных сумм будет столько, сколько существует различных булевых векторов длины $2^n$, то есть — $2^{2^n}$. Мы получили, что число различных полиномов Жегалкина совпадает с числом функций алгебры логики. Поскольку каждой функции соответствует хотя бы один полином, а каждому полиному соответствует ровно одна функция, то соответствие между ними взаимно однозначно, так как множества полиномов Жегалкина над $n$ переменными и функций алгебры логики от $n$ переменных равномощны. Единственность доказана.

## §5. Понятие замкнутого класса. Замкнутость классов $T_0$, $T_1$ и $L$.

### 1°. Понятие замкнутого класса.

**Определение 1.** Пусть $A \subseteq P_2$. Тогда *замыканием* $A$ называется множество всех функций алгебры логики, которые можно выразить формулами над $A$.

***Обозначение***: $[A]$.

Имеют место следующие свойства:

1) $[A] \supseteq A$;
2) $A \supseteq B \Rightarrow [A] \supseteq [B]$, причём, если в левой части импликации строгое вложение, то из него вовсе не следует строгое вложение в правой части — верно лишь

$$A \supset B \Rightarrow [A] \supseteq [B];$$

3) $[[A]] = [A]$.

**Определение 2.** Система функций алгебры логики $A$ называется полной, если $[A] = P_2$.

**Определение 3.** Пусть $A \subseteq P_2$. Тогда система $A$ называется замкнутым классом, если замыкание $A$ совпадает с самим $A$: $[A] = A$.

**Утверждение.** Пусть $A$ — замкнутый класс, $A \neq P_2$ и $B \subseteq A$. Тогда $B$ — неполная система (подмножество неполной системы будет также неполной системой).

**Доказательство.** $B \subseteq A \Rightarrow [B] \subseteq [A] = A \neq P_2 \Rightarrow [B] \neq P_2$. Следовательно, $B$ — неполная система. Утверждение доказано.

### 2°. Примеры замкнутых классов.

**Класс $T_0$** $= \{f(x_1, \ldots, x_n) \mid f(0, \ldots, 0) = 0\}$.

Классу $T_0$ принадлежат, например, функции $0$, $x$, $xy$, $x \vee y$, $x \oplus y$.

Классу $T_0$ не принадлежат функции $1$, $\overline{x}$, $x \to y$, $x \mid y$, $x \downarrow y$, $x \sim y$.

Подсчитаем число функций в классе $T_0$. Для этого построим следующую таблицу:

| $x_1$ | K | $x_n$ | |
|---|---|---|---|
| 0 | K | 0 | 0 |
| K | K | K | $\}\, 2^n - 1$ |

.

Все функции, принадлежащие указанному классу, принимают на нулевом наборе нулевое значение. Таким образом, всего функций в классе $T_0$ столько, сколько существует булевых векторов длины $2^n - 1$ (первый разряд вектора длины $2^n$ необходимо равен нулю), то есть $|T_0| = 2^{2^n-1} = \frac{1}{2}2^{2^n}$.

**Теорема 6.** Класс $T_0$ —замкнутый.

**Доказательство.** Рассмотрим произвольную систему функций алгебры логики $\left\{ f(x_1,\text{K},x_n), g_1(y_{11},\text{K},y_{1m_1}),\text{K}, g_n(y_{n1},\text{K},y_{nm_n}) \right\}$ из $T_0$. Рассмотрим функцию

$$h(y_1,\text{K},y_r) = f\left(g_1(y_{11},\text{K},y_{1m_1}),\text{K}, g_n(y_{n1},\text{K},y_{nm_n})\right).$$

Среди переменных функций $g_i$ могут встречаться и одинаковые, поэтому в качестве переменных функции $h$ возьмём все различные из них. Тогда $h(0, \ldots, 0) = f(g_1(0, \ldots, 0), \ldots, g_n(0, \ldots, 0)) = f(0, \ldots, 0) = 0$, следовательно, функция $h$ также сохраняет ноль. Рассмотрен только частный случай (без переменных в качестве аргументов). Однако, поскольку тождественная функция сохраняет ноль, подстановка простых переменных эквивалентна подстановке тождественной функции, теорема доказана.

**Класс $T_1$** $= \{f(x_1, \ldots, x_n) \mid f(1, 1, \ldots, 1) = 1\}$.

Классу $T_1$ принадлежат функции $1$, $x$, $xy$, $x \vee y$, $x \to y$, $x \sim y$.

Классу $T_1$ не принадлежат функции $0$, $\bar{x}$, $x \oplus y$, $x \mid y$, $x \downarrow y$.

**Теорема 7.** Класс $T_1$ замкнут.

**Доказательство** повторяет доказательство аналогичной теоремы для класса $T_0$.

**Класс $L$** линейных функций.

**Определение 4**. Функция алгебры логики $f(x_1, \ldots, x_n)$ называется линейной, если

$$f(x_1, \ldots, x_n) = a_0 \oplus a_1 x_1 \oplus \ldots \oplus a_n x_n, \text{ где } a_i \in \{0, 1\}.$$

Иными словами, в полиноме линейной функции нет слагаемых, содержащих конъюнкцию.

Классу $L$ принадлежат функции $0$, $1$, $\bar{x} = x \oplus 1$, $x \sim y$, $x \oplus y$.

Классу $L$ не принадлежат функции $xy$, $x \vee y$, $x \to y$, $x \mid y$, $x \downarrow y$.

**Теорема 8.** Класс $L$ замкнут.

**Доказательство.** Поскольку тождественная функция — линейная, достаточно (как и в теоремах 6 и 7) рассмотреть только случай подстановки в формулы функций: пусть $f(x_1, \ldots, x_n) \in L$ и $g_i \in L$. Достаточно доказать, что $f(g_1, \ldots, g_n) \in L$. Действительно, если не учитывать слагаемых с коэффициентами $a_i = 0$, то всякую линейную функцию можно представить в виде $x_{i_1} \oplus x_{i_2} \oplus \mathrm{K} \oplus x_{i_k} \oplus a_0$. Если теперь вместо каждого $x_{i_j}$ подставить линейное выражение, то получится снова линейное выражение (или константа единица или нуль).

## §6. Двойственность. Класс самодвойственных функций, его замкнутость.

### 1°. Двойственность.

**Определение 1.** Функцией, *двойственной* к функции алгебры логики $f(x_1, \ldots, x_n)$, называется функция $f^*(x_1, \mathrm{K}, x_n) = \overline{f}\left(\overline{x_1}, \mathrm{K}, \overline{x_n}\right)$.

**Теорема 9 (принцип двойственности).** Пусть

$$\Phi(y_1, \mathrm{K}, y_m) = f\left(g_1\left(y_{11}, \mathrm{K}, y_{1k_1}\right), \mathrm{K}, g_n\left(y_{n1}, \mathrm{K}, y_{nk_n}\right)\right).$$

Тогда $\Phi^*(y_1, \mathrm{K}, y_m) = f^*\left(g_1^*\left(y_{11}, \mathrm{K}, y_{1k_1}\right), \mathrm{K}, g_n^*\left(y_{n1}, \mathrm{K}, y_{nk_n}\right)\right)$.

**Доказательство.** Рассмотрим

$$\begin{aligned}
\Phi^*(y_1, \mathrm{K}\, y_m) &= \overline{f}\left(g_1\left(\overline{y}_{11}, \mathrm{K}, \overline{y}_{1k_1}\right), \mathrm{K}, g_n\left(\overline{y}_{n1}, \mathrm{K}, \overline{y}_{nk_n}\right)\right) = \\
&= \overline{f}\left(\overline{\overline{g}}_1\left(\overline{y}_{11}, \mathrm{K}, \overline{y}_{1k_1}\right), \mathrm{K}, \overline{\overline{g}}_n\left(\overline{y}_{n1}, \mathrm{K}, \overline{y}_{nk_n}\right)\right) = \\
&= \overline{f}\left(\overline{g_1^*}\left(\overline{y}_{11}, \mathrm{K}, \overline{y}_{1k_1}\right), \mathrm{K}, \overline{g_n^*}\left(\overline{y}_{n1}, \mathrm{K}, \overline{y}_{nk_n}\right)\right) = \\
&= f^*\left(g_1^*\left(y_{11}, \mathrm{K}, y_{1k_1}\right), \mathrm{K}, g_n^*\left(y_{n1}, \mathrm{K}, y_{nk_n}\right)\right).
\end{aligned}$$

Теорема доказана.

**Следствие.** Пусть функция $\Phi(y_1, \ldots, y_m)$ реализуется формулой над $A = \{f_1, f_2, \ldots\}$. Тогда если в этой формуле всюду заменить вхождения $f_i$ на $f_i^*$, то получится формула, реализующая $\Phi^*(y_1, \ldots, y_m)$.

**Утверждение.** Для любой функции алгебры логики $f(x_1, \ldots, x_n)$ справедливо равенство

$$f(x_1, \ldots, x_n) = f^{**}(x_1, \ldots, x_n).$$

**Доказательство.** $f^{**} = \left[\overline{f}\left(\overline{x_1}, \ldots, \overline{x_n}\right)\right]^* = \overline{\overline{f}}\left(\overline{\overline{x_1}}, \ldots, \overline{\overline{x_n}}\right) = f\left(x_1, \ldots, x_n\right)$,

и утверждение доказано.

**2°. Класс *S* самодвойственных функций.**

**Определение 2.** Функция алгебры логики $f(x_1, \ldots, x_n)$ называется самодвойственной, если

$$f(x_1, \ldots, x_n) = f^*(x_1, \ldots, x_n).$$

Иначе говоря, $S = \{f \mid f = f^*\}$.

Классу *S* принадлежат функции

$$x,\ \overline{x},\ x \oplus y \oplus z \oplus a,\ m(x, y, z) = xy \vee yz \vee zx = \begin{cases} 1, & x + y + z \geq 2 \\ 0, & x + y + z \leq 1 \end{cases}.$$

Классу *S* не принадлежат функции

$$0\ (f(x) \equiv 0 \Rightarrow f^*(x) = \overline{f}(\overline{x}) \equiv 1),\ 1,$$

$$x \vee y\ (\text{поскольку } (x \vee y)^* = \overline{\overline{x} \vee \overline{y}} = x \cdot y \neq x \vee y),\ xy.$$

**Теорема 10.** Класс *S* замкнут.

**Доказательство.** Пусть $f(x_1, \ldots, x_n) \in S$, $\forall i\ \ g_i\left(y_{i1}, \ldots, y_{ik_i}\right) \in S$, $i = 1, 2, \ldots, n$ и

$$\Phi = f\left(g_1\left(y_{11}, \ldots, y_{1k_1}\right), \ldots, g_n\left(y_{n1}, \ldots, y_{nk_n}\right)\right).$$

Тогда из принципа двойственности следует, что

$$\Phi^* = f^*\left(g_1^*\left(y_{11}, \ldots, y_{1k_1}\right), \ldots, g_n^*\left(y_{n1}, \ldots, y_{nk_n}\right)\right) = f(g_1(\ldots), \ldots, g_n(\ldots)).$$

Таким образом, мы получили, что $\Phi = \Phi^*$ и $\Phi \in S$. Теорема доказана.

## §7. Класс монотонных функций, его замкнутость.

**Определение 1.** Пусть $\tilde{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ и $\tilde{\beta} = (\beta_1, \beta_2, \ldots, \beta_n)$. Тогда

$$\tilde{\alpha} \le \tilde{\beta} \Leftrightarrow \forall i\,(\alpha_i \le \beta_i).$$

**Замечание**. Существуют наборы, для которых неприменимо отношение упорядоченности, определённое выше. Так, например, наборы (0, 0, 1) и (0, 1, 0) несравнимы.

**Определение 2.** Функция алгебры логики $f(x_1, \ldots, x_n)$ называется *монотонной*, если для любых двух сравнимых наборов $\tilde{\alpha}$ и $\tilde{\beta}$ выполняется импликация

$$\tilde{\alpha} \le \tilde{\beta} \Rightarrow f(\tilde{\alpha}) \le f(\tilde{\beta}).$$

Класс всех монотонных функций обозначим $M$.

Классу $M$ принадлежат функции

$$0,\ 1,\ x,\ xy,\ x \vee y,\ m(x, y, z) = xy \vee yz \vee zx.$$

Классу $M$ не принадлежат функции

$$\overline{x},\ x \mid y,\ x \downarrow y,\ x \oplus y,\ x \sim y,\ x \to y.$$

**Теорема 11.** Класс $M$ замкнут.

**Доказательство.** Поскольку тождественная функция монотонна, достаточно проверить лишь случай суперпозиции функций. Пусть $f(x_1, \ldots, x_n) \in M$, для любого $j$ $g_j(y_1, \ldots, y_m) \in M$ и

$$\Phi(y_1, \ldots, y_m) = f(g_1(y_1, \ldots, y_m), \ldots, g_n(y_1, \ldots, y_m)).$$

Рассмотрим произвольные наборы $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_m)$, $\tilde{\beta} = (\beta_1, \ldots, \beta_m)$ такие, что $\tilde{\alpha} \le \tilde{\beta}$. Обозначим

$$g_i(\tilde{\alpha}) = \gamma_i,\ \ g_i(\tilde{\beta}) = \delta_i.$$

Тогда для любого $i$ имеем $g_i \in M$ и $g_i(\tilde{\alpha}) \le g_i(\tilde{\beta})$, то есть $\forall i\ \ (\gamma_i \le \delta_i)$. Обозначим

$$\tilde{\gamma} = (\gamma_1, \gamma_2, \ldots, \gamma_n),\ \ \tilde{\delta} = (\delta_1, \delta_2, \ldots, \delta_n).$$

Тогда по определению $\gamma \leq \delta$ и, в силу монотонности функции $f$, $f(\gamma) \leq f(\delta)$. Но

$$\Phi(\alpha) = f(\gamma_1, \ldots, \gamma_n) = f(\gamma), \ \Phi(\beta) = f(\delta_1, \ldots, \delta_n) = f(\delta),$$

откуда $\Phi(\alpha) \leq \Phi(\beta)$, следовательно, $\Phi \in M$. Теорема доказана.

## §8. Лемма о несамодвойственной функции

**Лемма (о несамодвойственной функции).** Из любой несамодвойственной функции алгебры логики $f(x_1, \ldots, x_n)$, подставляя вместо всех переменных функции $\bar{x}$ и $x$, можно получить $\varphi(x) \equiv \text{const}$.

**Доказательство.** Пусть $f \notin S$. Тогда

$$\bar{f}(\bar{x}_1, \ldots, \bar{x}_n) \neq f(x_1, \ldots, x_n) \Rightarrow \exists \sigma = (\sigma_1, \ldots, \sigma_n):$$
$$\bar{f}(\bar{\sigma}_1, \ldots, \bar{\sigma}_n) \neq f(\sigma_1, \ldots, \sigma_n) \Leftrightarrow f(\bar{\sigma}_1, \ldots, \bar{\sigma}_n) = f(\sigma_1, \ldots, \sigma_n).$$

Построим функцию $\varphi(x)$ так: $\varphi(x) = f(x \oplus \sigma_1, \ldots, x \oplus \sigma_n)$. Тогда

$$\varphi(0) = f(\sigma_1, \ldots, \sigma_n), \ \varphi(1) = f(\bar{\sigma}_1, \ldots \bar{\sigma}_n)$$

и $\varphi(0) = \varphi(1) \Rightarrow \varphi(x) = \text{const}$. Заметим, что подстановка удовлетворяет условию теоремы, так как $x \oplus \sigma = \begin{cases} x, & \sigma = 0 \\ \bar{x}, & \sigma = 1 \end{cases}$. Лемма доказана.

## §9. Лемма о немонотонной функции

**Лемма (о немонотонной функции).** Из любой немонотонной функции алгебры логики $f(x_1, \ldots, x_n)$, подставляя вместо всех переменных функции $x$, 0, 1, можно получить функцию $\varphi(x) = \bar{x}$.

**Доказательство**. Пусть $f \notin M$. Тогда существуют такие наборы $\alpha = (\alpha_1, \ldots, \alpha_n)$ и $\beta = (\beta_1, \ldots, \beta_n)$, что $\alpha < \beta$ (то есть $\forall j \ (\alpha_j \leq \beta_j)$ и $\alpha \neq \beta$) и $f(\alpha) > f(\beta)$. Выделим те разряды $i_1, \ldots, i_k$ наборов $\alpha$ и $\beta$, в которых они различаются. Очевидно, в наборе $\alpha$ эти разряды равны 0, а в

наборе $\beta$ — 1. Рассмотрим последовательность наборов $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_k$ таких, что $\alpha = \alpha_0 < \alpha_1 < \alpha_2 < \ldots < \alpha_k = \beta$, где $\alpha_{i+1}$ получается из $\alpha_i$ заменой одного из нулей, расположенного в одной из позиций $i_1, \ldots, i_k$, на единицу (при этом наборы $\alpha_i$ и $\alpha_{i+1}$ — соседние). Поскольку $f(\alpha) = 1$, а $f(\beta) = 0$, среди наборов $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_k$ найдутся два соседних $\alpha_i$ и $\alpha_{i+1}$, такие что $f(\alpha_i) = 1$ и $f(\alpha_{i+1}) = 0$. Пусть они различаются в $r$-ом разряде: $\alpha_i = (\alpha_1, \ldots, \alpha_{r-1}, 0, \alpha_{r+1}, \ldots, \alpha_n)$, $\alpha_{i+1} = (\alpha_1, \ldots, \alpha_{r-1}, 1, \alpha_{r+1}, \ldots, \alpha_n)$. Тогда определим функцию $\varphi(x)$ так: $\varphi(x) = f(\alpha_1, \alpha_2, \ldots, \alpha_{r-1}, x, \alpha_{r+1}, \ldots, \alpha_n)$. Действительно, тогда $\varphi(0) = f(\alpha_i) = 1$, $\varphi(1) = f(\alpha_{i+1}) = 0$ и $\varphi(x) = \overline{x}$. Лемма доказана.

## §10. Лемма о нелинейной функции

**Лемма (о нелинейной функции).** Из любой нелинейной функции алгебры логики $f(x_1, \ldots, x_n)$, подставляя вместо всех переменных $x$, $\overline{x}$, $y$, $\overline{y}$, 0, 1, можно получить $\varphi(x, y) = x \cdot y$ или $\varphi(x, y) = \overline{x \cdot y}$.

**Доказательство.** Пусть $f(x_1, \ldots, x_n) \notin L$. Рассмотрим полином Жегалкина этой функции. Из её нелинейности следует, что в нём присутствуют слагаемые вида $x_{i_1} \cdot x_{i_2} \cdot \ldots$. Не ограничивая общности рассуждений, будем считать, что присутствует произведение $x_1 \cdot x_2 \cdot \ldots$. Таким образом, полином Жегалкина этой функции выглядит так:

$$f(x_1, \ldots, x_n) = x_1 \cdot x_2 \cdot P_1(x_3, \ldots, x_n) \oplus x_1 \cdot P_2(x_3, \ldots, x_n) \oplus \oplus x_2 \cdot P_3(x_3, \ldots, x_n) \oplus P_4(x_3, \ldots, x_n),$$

причем $P_1(x_3, \ldots, x_n) \neq 0$. Иначе говоря, $\exists\, a_3, a_4, \ldots, a_n \in E_2 = \{0, 1\}$ такие, что $P_1(a_3, a_4, \ldots, a_n) = 1$. Рассмотрим вспомогательную функцию $f(x_1, x_2, a_3, a_4, \ldots, a_n) = x_1 x_2 \cdot 1 \oplus x_1 \cdot b \oplus x_2 \cdot c \oplus d$. Тогда функция

$$f(x \oplus c, y \oplus b, a_3, a_4, \ldots, a_n) = (x \oplus c)(y \oplus b) \oplus (x \oplus c)b \oplus (y \oplus b)c \oplus d =$$
$$= xy \oplus x \cdot b \oplus y \cdot c \oplus b \cdot c \oplus x \cdot b \oplus b \cdot c \oplus y \cdot c \oplus b \cdot c \oplus d =$$
$$= xy \oplus (bc \oplus d) = \begin{cases} xy, & bc \oplus d = 0 \\ \overline{xy}, & bc \oplus d = 1 \end{cases}.$$

Лемма доказана.

## §11. Теорема Поста о полноте системы функций алгебры логики

**Теорема 12 (теорема Поста).** Система функций алгебры логики $A = \{f_1, f_2, \ldots\}$ является полной в $P_2$ тогда и только тогда, когда она не содержится целиком ни в одном из следующих классов: $T_0$, $T_1$, $S$, $L$, $M$.

**Доказательство.** Необходимость. Пусть $A$ — полная система, $N$ — любой из классов $T_0$, $T_1$, $S$, $L$, $M$ и пусть $A \subseteq N$. Тогда

$$[A] \subseteq [N] = N \neq P_2 \text{ и } [A] \neq P_2.$$

Полученное противоречие завершает обоснование необходимости.

Достаточность. Пусть $A \not\subset T_0$, $A \not\subset T_1$, $A \not\subset M$, $A \not\subset L$, $A \not\subset S$. Тогда в $A$ существуют функции $f_0 \notin T_0$, $f_1 \notin T_1$, $f_M \notin M$, $f_L \notin L$, $f_S \notin S$. Достаточно показать, что $[A] \supseteq [f_0, f_1, f_M, f_L, f_S] = P_2$. Разобьём доказательство на три части: получение отрицания, констант и конъюнкции.

*a)* Получение $\overline{x}$. Рассмотрим функцию $f_0(x_1, \ldots, x_n) \notin T_0$ и получим из нее функцию $\varphi_0(x) = f_0(x, x, \ldots, x)$. Так как функция $f_0$ не сохраняет нуль, $\varphi_0(0) = f(0, 0, \ldots, 0) = 1$. Возможны два случая: либо $\varphi_0(x) = \overline{x}$, либо $\varphi_0(x) \equiv 1$. Рассмотрим функцию $f_1(x_1, \ldots, x_n) \notin T_1$ и аналогичным образом получим функцию $\varphi_1(x) = f_1(x, x, \ldots, x)$. Так как функция $f_1$ не сохраняет единицу, $\varphi_1(1) = f(1, 1, \ldots, 1) = 0$. Возможны также два случая: либо $\varphi_1(x) = \overline{x}$, либо $\varphi_1(x) \equiv 0$. Если хотя бы в одном случае получилось искомое отрицание, пункт завершён. Если же в обоих случаях получились константы, то согласно лемме о немонотонной функции, подставляя в функцию $f_M \notin M$ вместо всех переменных константы и тождественную функцию, можно получить отрицание. Отрицание получено.

*b)* Получение констант 0 и 1. Имеем $f_S \notin S$. Согласно лемме о несамодвойственной функции, подставляя вместо всех переменных функции $f_S$ отрицание (которое получено в пункте *a*) и тождественную функцию, можно получить константы: $[f_S, \overline{x}\,] \ni [0, 1]$. Константы получены.

*c)* Получение конъюнкции $x \cdot y$. Имеем функцию $f_L \notin L$. Согласно лемме о нелинейной функции, подставляя в функцию $f_L$ вместо всех переменных константы, переменные и отрицания

переменных (которые были получены на предыдущих шагах доказательства), можно получить либо конъюнкцию, либо отрицание конъюнкции. Однако на первом этапе отрицание уже получено, следовательно, всегда можно получить конъюнкцию: $[f_L, 0, 1, \overline{x}\,] \ni [xy, \overline{xy}\,]$. Конъюнкция получена.

В результате получено, что $\left[ f_0, f_1, f_M, f_L, f_S \right] \supseteq \left[ \overline{x}, xy \right] = P_2$. Последнее равенство следует из пункта 2 теоремы 4. В силу леммы 2 достаточность доказана.

## §12. Теорема о максимальном числе функций в базисе алгебры логики

**Определение.** Система функций алгебры логики $A \subseteq P_2$ называется *базисом* (в $P_2$), если

1) $[A] = P_2$;
2) $\forall f \in A\ ([A \setminus \{f\}] \neq P_2)$.

**Теорема 13.** Максимальное число функций в базисе алгебры логики равно 4.

**Доказательство.** 1) Докажем, что из любой полной системы можно выделить полную подсистему, содержащую не более четырёх функций. Действительно, если $A$ — полная система ($[A] = P_2$), то согласно теореме Поста в ней существуют пять функций $f_0 \notin T_0$, $f_1 \notin T_1$, $f_S \notin S$, $f_M \notin M$, $f_L \notin L$. По теореме Поста система функций $\{f_0, f_1, f_S, f_M, f_L\}$ полна. Рассмотрим функцию $f_0(x_1, \ldots, x_n) \notin T_0$ ($f_0(0, 0, \ldots, 0) = 1$). Возможны два случая:

*a)* $f_0(1, 1, \ldots, 1) = 1 \Rightarrow f_0 \notin S \Rightarrow [f_0, f_1, f_L, f_M] = P_2$ и система $\{f_0, f_1, f_L, f_M\}$ полна.

*b)* $f_0(1, 1, \ldots, 1) = 0 \Rightarrow f_0 \notin M, T_1 \Rightarrow [f_0, f_L, f_S] = P_2$ и система $\{f_0, f_L, f_S\}$ полна.

2) Покажем, что существует базис алгебры логики из четырёх функций. Действительно, рассмотрим систему функций

$$\{0, 1, x \cdot y, x \oplus y \oplus z\}.$$

Эта система функций полная, так как $0 \notin T_1$, $S$, $1 \notin T_0$, $x \cdot y \notin L$, $x \oplus y \oplus z \notin M$ ($0 \oplus 0 \oplus 1 = 1$, $0 \oplus 1 \oplus 1 = 0$). Однако, любая её подсистема не полна:

$\{0, 1, x \cdot y\} \subseteq M$

$\{0, 1, x \oplus y \oplus z\} \subseteq L$

$\{0, xy, x \oplus y \oplus z\} \subseteq T_0$

$\{1, xy, x \oplus y \oplus z\} \subseteq T_1$.

Теорема доказана.

## §13. Теорема о предполных классах

### 1 . Предполные классы.

**Определение.** Пусть $A \subseteq P_2$. $A$ называется *предполным классом*, если

1) $[A] \neq P_2$;

2) $\forall f \in P_2 \, ( f \notin A \Rightarrow [A \cup \{f\}] = P_2)$.

**Теорема 14.** В $P_2$ предполными являются лишь следующие 5 классов: $T_0$, $T_1$, $S$, $L$, $M$.

**Доказательство.** 1) Покажем сначала, что ни один из этих пяти классов не содержится в другом. Для этого достаточно для каждого из пяти вышеперечисленных классов указать четыре функции, принадлежащие данному классу, но не принадлежащие остальным четырем:

| $\in$ \ $\notin$ | $T_0$ | $T_1$ | $L$ | $M$ | $S$ |
|---|---|---|---|---|---|
| $T_0$ | | 0 | $xy$ | $x \oplus y$ | 0 |
| $T_1$ | 1 | | $xy$ | $x \oplus y \oplus 1$ | 1 |
| $L$ | 1 | 0 | | $x \oplus y$ | 0 |
| $M$ | 1 | 0 | $xy$ | | 0 |
| $S$ | $\overline{x}$ | $\overline{x}$ | $xy \oplus yz \oplus zx$ | $\overline{x}$ | |

2) Докажем, что все классы — $T_0$, $T_1$, $S$, $L$, $M$ являются предполными. Действительно, пусть $N \in \{T_0, T_1, L, M, S\}$ и $f \notin N$. Тогда система $N \cup \{f\}$ не содержится ни в одном из пяти классов Поста (так как $N$ не содержится в четырёх из них, а $f$ не содержится в $N$). Следовательно, система $N \cup \{f\}$ — полная и $N$ — предполный класс.

3) Пусть $A$ — предполный класс. Тогда $[A] \neq P_2 \Rightarrow \exists \, N \in \{T_0, T_1, L, M, S\}$: $A \subseteq N$. Если $A \neq N$, то $\exists \, f \, ( f \in N, f \notin A)$:

$$A \cup \{f\} \subseteq N \Rightarrow [A \cup \{f\}] \neq P_2.$$

Полученное противоречие завершает доказательство.

**2 . Результаты Поста.**

1) В $P_2$ существует ровно счётное число замкнутых классов.
2) В любом замкнутом классе существует конечный базис.

## §14. *k*-значные функции. Теорема о существовании конечной полной системы в множестве *k*-значных функций

**1°. *k*-значные функции.** Будем рассматривать конечный алфавит $E_k = \{0, 1, 2, \ldots, k-1\}$. Функцией $k$-значной логики назовём отображение вида $f(x_1, x_2, \ldots, x_n)$: $E_k^n \to E_k$.

Некоторые функции $k$-значной логики.

1) *Константы* $0, 1, 2, \ldots, k-1$ (всего — $k$);
2) *Тождественная* функция $f(x) = x$;
3) *Отрицания*: $f(x) = \overline{x} = x + 1 \pmod k$ — *отрицание Поста*,
   $f(x) = {\sim} x = (k-1) - x$ — *отрицание Лукасевича*;
4) *Сложение по модулю k*: $f(x, y) = x + y \pmod k$;
5) *Умножение по модулю k*: $f(x, y) = xy \pmod k$;
6) *Максимум*: $\max(x, y)$;
7) *Минимум*: $\min(x, y)$;
8) $J_\sigma(x) = \begin{cases} k-1, & x = \sigma \\ 0, & x \neq \sigma \end{cases}$.

**Теорема 15.** Система

$$\{0, 1, \ldots, k-1, \max(x, y), \min(x, y), J_0(x), J_1(x), \ldots, J_{k-1}(x)\}$$

полна в $P_k$.

**Доказательство.** Утверждается, что для любой функции $f(x_1, \ldots, x_n) \in P_k$ справедливо представление

$$f(x_1, \ldots, x_n) = \max_{(\sigma_1, \ldots, \sigma_n) \in E_k^n} \left\{ \min\left( J_{\sigma_1}(x_1), \ldots, J_{\sigma_n}(x_n), f(\sigma_1, \sigma_2, \ldots, \sigma_n) \right) \right\} .$$

Действительно, для любого набора $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in E_k^n$ рассмотрим значение правой части: если существует такое $i$, что $\sigma_i \neq \alpha_i$, то $J_{\sigma_i}(\alpha_i) = 0$ и весь минимум станет равным нулю. Таким образом, правая часть станет равна

$$\max\{0, 0, \ldots, 0, \min(J_{\alpha_1}(\alpha_1), J_{\alpha_2}(\alpha_2), \ldots, J_{\alpha_n}(\alpha_n), f(\alpha_1, \alpha_2, \ldots, \alpha_n)), 0, \ldots, 0\},$$

а учитывая то, что в $P_k$

$$J_a(a) = k - 1,$$

получим, что правая часть равна просто $f(\alpha_1, \alpha_2, \text{К}, \alpha_n)$ . Теорема доказана.

**Замечание.**

$$\min(x_1, x_2, x_3) = \min(x_1, \min(x_2, x_3));$$
$$\min(x_1, x_2, \ldots, x_n) = \min(x_1, \min(x_2, \ldots, x_n)).$$

Аналогично определяется функция максимума от $n$ переменных.

**2°. Особенности *k*-значной логики.**

1) В $P_k$ существует континуум замкнутых классов (при $k \geq 3$).
2) В $P_k$ существуют замкнутые классы с бесконечным базисом (при $k \geq 3$).
3) В $P_k$ существуют замкнутые классы, не имеющие базиса (при $k \geq 3$).

# Глава II. Основы теории графов

## §15. Основные понятия теории графов. Изоморфизм графов. Связность

**Определение 1.** *Графом* называется произвольное множество элементов $V$ и произвольное семейство $E$ пар из $V$. Обозначение: $G = (V, E)$.

В дальнейшем будем рассматривать конечные графы, то есть графы с конечным множеством элементов и конечным семейством пар.

**Определение 2.** Если элементы из $E$ рассматривать как неупорядоченные пары, то граф называется *неориентированным*, а пары называются *рёбрами*. Если же элементы из $E$ рассматривать как упорядоченные, то граф *ориентированный*, а пары — *дуги*.

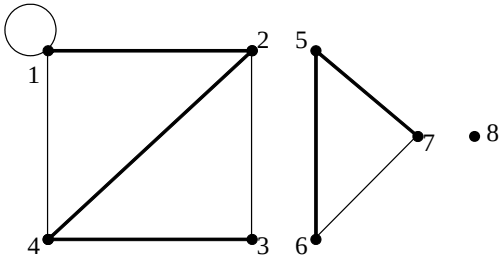
**Определение 3.** Пара вида $(a, a)$ называется *петлёй*, если пара $(a, b)$ встречается в семействе $E$ несколько раз, то она называется *кратным ребром* (*кратной дугой*).

**Определение 4.** В дальнейшем условимся граф без петель и кратных рёбер называть *неориентированным графом* (или просто *графом*), граф без петель — *мультиграфом*, а мультиграф, в котором разрешены петли — *псевдографом*.

**Определение 5.** Две вершины графа называются *смежными*, если они соединены ребром.

**Определение 6.** Говорят, что вершина и ребро *инцидентны*, если ребро содержит вершину.

**Определение 7.** *Степенью вершины* ($\deg v$) называется количество рёбер, инцидентных данной вершине. Для псевдографа полагают учитывать петлю дважды.



**Утверждение 1.** В любом графе (псевдографе) справедливо следующее соотношение: $\sum_{i=1}^{p} \deg v_i = 2q$, где $p$ — число вершин, а $q$ — число рёбер.

**Доказательство.** Когда мы считаем степень одной вершины, мы считаем все рёбра, выходящие из неё. Вычисляя сумму всех степеней, мы получаем, что каждое ребро считается дважды, так как оно инцидентно двум вершинам (петли по определению степени также посчитаются дважды). Поэтому общая сумма будет равна удвоенному числу рёбер. Утверждение доказано.

**Определение 8.** Пусть множество вершин графа $V = \{v_1, v_2, \ldots, v_p\}$. Тогда *матрицей смежности* этого графа назовём матрицу $A = \|a_{ij}\|$, где $a_{ij} = 1$, если вершины $v_i$ и $v_j$ смежны (2, 3, … для мультиграфа или псевдографа) и 0 в противном случае, $a_{ii}$ при этом равно числу петель в вершине $v_i$.

**Определение 9.** Два графа (или псевдографа) $G_1 = (V_1, E_1)$ и $G_2 = (V_2, E_2)$ называются *изоморфными*, если существуют два взаимно однозначных отображения $\varphi_1: V_1 \to V_2$ и $\varphi_2: E_1 \to E_2$ такие, что для любых двух вершин $u$ и $v$ графа $G_1$ справедливо $\varphi_2(u, v) = (\varphi_1(u), \varphi_1(v))$.

**Определение 10 (изоморфизм графов без петель и кратных рёбер).** Два графа $G_1 = (V_1, E_1)$ и $G_2 = (V_2, E_2)$ называются *изоморфными*, если существует взаимно однозначное отображение $\varphi_1: V_1 \to V_2$ такое, что $(u, v) \in E_1 \Leftrightarrow (\varphi(u), \varphi(v)) \in E_2$.

**Определение 11.** Граф $G_1 = (V_1, E_1)$ называется *подграфом* графа $G = (V, E)$, если

$$V_1 \subseteq V,\ E_1 \subseteq E.$$

**Определение 12.** *Путём* в графе $G = (V, E)$ называется любая последовательность вида

$$v_0, (v_0, v_1), v_1, (v_1, v_2), \ldots, v_{n-1}, (v_{n-1}, v_n), v_n.$$

Число $n$ в данных обозначениях называется *длиной пути*.

**Определение 13.** *Цепью* называется путь, в котором нет повторяющихся рёбер.

**Определение 14.** *Простой цепью* называется путь без повторения вершин.

**Утверждение 2.** Пусть в $G = (V, E)$ $v_1 \neq v_2$ и пусть $P$ — путь из $v_1$ в $v_2$. Тогда в $P$ можно выделить подпуть из $v_1$ в $v_2$, являющийся простой цепью.

**Доказательство.** Пусть данный путь — не простая цепь. Тогда в нём повторяется некоторая вершина $v$, то есть он имеет вид: $P_1 = v_0C_1vC_2vC_3v_2$. Тогда он содержит подпуть $P_2 = v_0C_1vC_3v_2$. Если в $P_2$ повторяется некоторая вершина, то аналогично удалим ещё кусок и так далее. Процесс должен закончиться, так как $P_1$ — конечный путь. Утверждение доказано.

**Определение 15.** Путь называется *замкнутым*, если $v_0 = v_n$.

**Определение 16.** Путь называется *циклом*, если он замкнут, и рёбра в нём не повторяются.

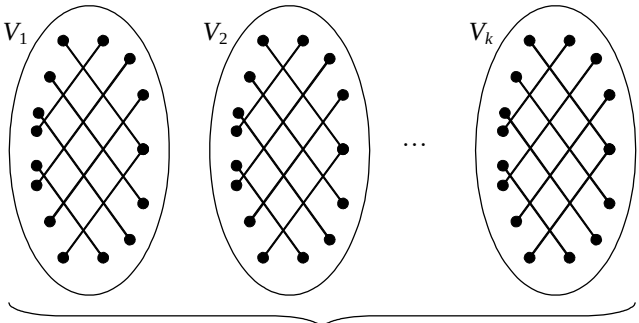
**Определение 17.** Путь называется *простым циклом*, если $v_0 = v_n$ и вершины не повторяются.

**Определение 18.** Граф $G = (V, E)$ называется *связным*, если для любых вершин $v_i, v_j \in V$ $(v_i \neq v_j)$ существует путь из $v_i$ в $v_j$.

Рассмотрим отношение $v_i \to v_j$ существования пути из $v_i$ в $v_j$. Оно

1) симметрично, так как $(v_i \to v_j) \Rightarrow (v_j \to v_i)$,
2) транзитивно, так как $(v_i \to v_j)\ \&\ (v_j \to v_k) \Rightarrow (v_i \to v_k)$,
3) рефлексивно, так как $\forall i\ (v_i \to v_i)$.

Таким образом, получено, что $v_i \to v_j$ — отношение эквивалентности и множество вершин разбивается на конечное число классов эквивалентности: $V \to V_1 \cup V_2 \cup \ldots \cup V_k$, $V_i \cap V_j = \varnothing \Leftarrow i \neq j$. При этом граф $G$ разбивается на связные подграфы, которые называются *компонентами связности*.



Связные компоненты графа $G$

## §16. Деревья. Свойства деревьев.

**Определение 1.** *Деревом* называется связный граф без циклов.

**Определение 2.** Подграф $G_1 = (V_1, E_1)$ графа $G = (V, E)$, называется *остовным деревом* в графе $G=(V,E)$, если $G_1=(V_1,E_1)$ — дерево и $V_1=V$.

**Лемма 1.** Если граф $G = (V, E)$ связный и ребро $(a, b)$ содержится в некотором цикле в графе $G$, то при выбрасывании из графа $G$ ребра $(a, b)$ снова получится связный граф.

**Доказательство.** Это утверждение следует из того, что при выбрасывании из графа $G$ ребра $(a, b)$ вершины $a$ и $b$ всё равно остаются в одной связной компоненте, поскольку из $a$ в $b$ можно пройти по оставшейся части цикла. Лемма доказана.

**Теорема 1.** Любой связный граф содержит хотя бы одно остовное дерево.

**Доказательство.** Если в $G$ нет циклов, то $G$ является искомым остовным деревом. Если в $G$ есть циклы, то удалим из $G$ какое-нибудь ребро, входящее в цикл. Получится некоторый подграф $G_1$. По лемме 1 $G_1$ — связный граф. Если в $G_1$ нет циклов, то $G_1$ и есть искомое остовное дерево, иначе продолжим этот процесс. Процесс должен завершиться, так как $E$ — конечное множество. Теорема доказана.

**Лемма 2.** Если к связному графу добавить новое ребро на тех же вершинах, то появится цикл.

**Доказательство.** Рассмотрим произвольный связный граф $G=(V,E)$. Пусть $u \in V$, $v \in V$, $(u, v) \notin E$. Так как $G$ — связный граф, то в нём есть путь из $v$ в $u$. Тогда в $G$ есть и простая цепь $C$ из $v$ в $u$. Поэтому в полученном графе есть цикл $C$, $(u, v)$, $v$. Лемма доказана.

**Лемма 3.** Пусть в графе $G = (V, E)$ $p$ вершин и $q$ рёбер. Тогда в $G$ не менее $p - q$ связных компонент. Если при этом в $G$ нет циклов, то $G$ состоит ровно из $p - q$ связных компонент.

**Доказательство.** Пусть к некоторому графу $H$, содержащему вершины $u$ и $v$, добавляется ребро $(u, v)$. Тогда если $u$ и $v$ лежат в разных связных компонентах графа $H$, то число связных компонент уменьшится на 1. Если $u$, $v$ лежат в одной связной компоненте графа $H$, то число связных компонент не изменится. В любом случае, число связных компонент уменьшается не более чем на 1. Значит, при добавлении $q$ рёбер число связных компонент уменьшается не более чем на $q$. Так как граф $G$ получается из графа $G_1 = (V, \varnothing)$ добавлением $q$ рёбер,

то в $G$ не менее $p - q$ связных компонент. Пусть теперь в $G$ нет циклов, и пусть в процессе получения $G$ из $G_1$ добавляется ребро $(u, v)$. Если бы $u, v$ лежали уже в одной связной компоненте, то в $G$, согласно лемме 2, возникал бы цикл. Следовательно, $u, v$ лежат в разных связных компонентах и при добавлении ребра $(u, v)$ число связных компонент уменьшается ровно на 1. Тогда $G$ состоит ровно из $p - q$ связных компонент. Лемма доказана.

**Теорема 2 (о различных определениях дерева).** Следующие пять определений эквивалентны ($p$ — число вершин, $q$ — число рёбер):

1) $G$ — дерево;
2) $G$ — без циклов и $q = p - 1$;
3) $G$ — связный граф и $q = p - 1$;
4) $G$ — связный граф, но при удалении любого ребра становится несвязным;
5) $G$ — без циклов, но при добавлении любого ребра на тех же вершинах появляется цикл.

**Доказательство.** Докажем следующие переходы: 1) $\Rightarrow$ 2) $\Rightarrow$ 3) $\Rightarrow$ $\Rightarrow$ 4) $\Rightarrow$ 5) $\Rightarrow$ 1), откуда будет следовать, что из любого условия вытекает любое другое.

1) $\Rightarrow$ 2): так как $G$ — связный граф и $G$ не содержит циклов, то $p - q = 1$ по лемме 3. Отсюда $q = p - 1$.

2) $\Rightarrow$ 3): по лемме 3 в $G$ число связных компонент равно $p - q = 1$, то есть $G$ — связный граф.

3) $\Rightarrow$ 4): при удалении одного ребра $p - q = 2$. Тогда по лемме 3 число связных компонент не менее чем $p - q = 2$.

4) $\Rightarrow$ 5): если $G$ имеет цикл, то согласно лемме 1 можно выбросить одно ребро так, что граф останется связным. Согласно лемме 2, если добавить любое новое ребро к связному графу $G$ на тех же вершинах, то появится цикл.

5) $\Rightarrow$ 1): если $G$ не связный граф и вершины $u, v$ лежат в разных связных компонентах графа $G$, то добавление к $G$ ребра $(u, v)$, очевидно, не порождает циклов, что противоречит 5). Отсюда следует, что $G$ — связный граф. Теорема доказана.

## §17. Корневые деревья. Верхняя оценка их числа

**Определение 1.** Любое дерево, в котором выделена одна вершина, называемая *корнем*, называется *корневым деревом*.

**Определение 2.** 1) Граф, состоящий из одной вершины, которая выделена, называется *корневым деревом*.

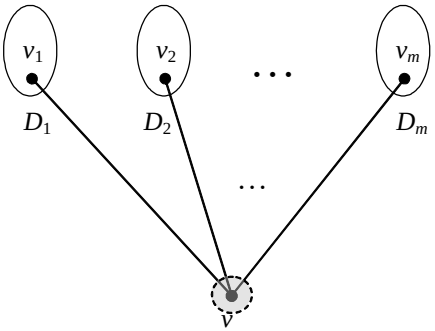
2) Пусть имеются корневые деревья $D_1,D_2,\ldots,D_m$ с корнями $v_1,v_2,\ldots,v_m$, $D_i = (V_i, E_i)$, $V_i \cap V_j = \varnothing$ $(i \neq j)$. Тогда граф $D = (V, E)$, полученный следующим образом:

$$V = V_1 \cup V_2 \cup \ldots \cup V_m \cup \{v\} \ (v \notin V_i, \forall i\ ),$$
$$E = E_1 \cup E_2 \cup \ldots \cup E_m \cup \{(v, v_1), (v, v_2), \ldots,(v, v_m)\}$$

и в котором выделена вершина $v$, называется *корневым деревом*.

3) Только те объекты являются *корневыми деревьями*, которые можно построить согласно пунктам 1) и 2).

При таком определении $D_1,D_2,\ldots,D_m$ называются *поддеревьями* дерева $D$.




**Утверждение.** Определения 1 и 2 эквивалентны.

**Определение 3.** *Упорядоченным корневым деревом* называется корневое дерево, в котором

1) задан порядок поддеревьев и
2) каждое поддерево $D_i$ является упорядоченным поддеревом.

Дерево с одной вершиной также является упорядоченным поддеревом.

**Теорема 3.** Число упорядоченных корневых деревьев с $q$ рёбрами не превосходит $4^q$.

**Доказательство.** Рассмотрим алгоритм обхода упорядоченного дерева, называемого «поиском в глубину». Этот обход описывается рекурсивно следующим образом:

1) Начать с корня. Пока есть поддеревья выполнять:
2) перейти в корень очередного поддерева, обойти это поддерево «в глубину».
3) Вернуться в корень исходного поддерева.

В результате обход «в глубину» проходит по каждому ребру дерева ровно 2 раза: один раз при переходе в очередное поддерево, второй раз при возвращении из этого поддерева. В соответствии с обходом «в глубину» будем строить последовательность из нулей и единиц, записывая на каждом шаге нуль или единицу, причём нуль будем записывать, если происходит переход в очередное поддерево, а единицу, если мы возвращаемся из поддерева. Получим последовательность из 0 и 1 длины $2q$, которую назовём кодом дерева. По этому коду однозначно восстанавливается дерево, поскольку каждый очередной разряд однозначно указывает, начинать ли строить новое очередное поддерево или возвращаться на ярус ближе к корню. Таким образом, упорядоченных корневых деревьев с $q$ рёбрами не больше, чем последовательностей из 0 и 1 длины $2q$, а их число равно $2^{2q} = 4^q$. Теорема доказана.

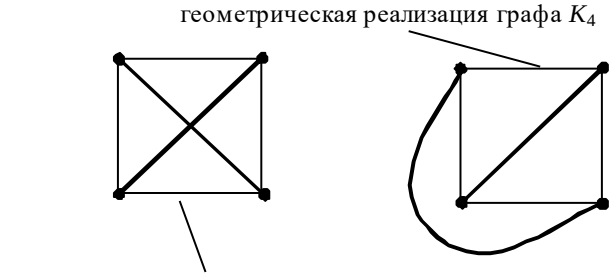
Изоморфизм корневых деревьев определяется так же, как и изоморфизм графов, но с дополнительным требованием: корень должен отображаться в корень. Для упорядоченных корневых деревьев также требуется сохранение порядка поддеревьев.

**Следствие.** Число неизоморфных корневых деревьев с $q$ рёбрами и число неизоморфных деревьев с $q$ рёбрами не превосходит $4^q$.

**Доказательство.** Выделяя в неизоморфных деревьях по одной вершине, мы получим неизоморфные корневые деревья. Упорядочивая поддеревья в неизоморфных корневых деревьях, мы получим различные упорядоченные корневые деревья. Поэтому число неизоморфных деревьев с $q$ рёбрами не превосходит числа неизоморфных корневых деревьев с $q$ рёбрами, которое, в свою очередь, не превосходит числа различных упорядоченных корневых деревьев с $q$ рёбрами. Отсюда и из теоремы следует утверждение следствия. Следствие доказано.

## §18. Геометрическая реализация графов. Теорема о реализации графов в трёхмерном пространстве

**Определение.** Пусть задан некоторый неориентированный граф $G = (V, E)$. Пусть любой вершине $v_i$ графа $G$ сопоставлена некоторая точка $a_i$: $v_i \to a_i$, $a_i \neq a_j$ $(i \neq j)$, а любому ребру $e = (a, b)$ сопоставлена некоторая непрерывная кривая $L$, соединяющая точки $a_i$ и $a_j$ и не проходящая через другие точки $a_k$ $(k \neq i, j)$. Тогда если все кривые, сопоставленные рёбрам, не имеют общих точек, кроме концевых, то говорят, что задана *геометрическая реализация графа G*.




**Теорема 4.** Для любого графа существует его реализация в трёхмерном пространстве.

**Доказательство.** Возьмём в пространстве любую прямую $l$ и разместим на ней все вершины графа $G$. Пусть в $G$ имеется $q$ рёбер. Проведём связку из $q$ различных полуплоскостей через $l$. После этого каждое ребро графа $G$ можно изобразить линией в своей полуплоскости и они, очевидно, не будут пересекаться. Теорема доказана.

## §19. Планарные (плоские) графы. Формула Эйлера

**Определение 1.** Граф называется *планарным*, если существует его геометрическая реализация на плоскости.

**Определение 2.** Если имеется планарная реализация графа и мы «разрежем» плоскость по всем линиям этой планарной реализации, то плоскость распадётся на части, которые называются *гранями* этой планарной реализации (одна из граней бесконечна, она называется *внешней гранью*).

**Теорема 5 (формула Эйлера).** Для любой планарной реализации связного планарного графа $G = (V, E)$ с $p$ вершинами, $q$ рёбрами и $r$ гранями выполняется равенство: $p - q + r = 2$.

**Доказательство.** Докажем теорему при фиксированном $p$ индукцией по $q$. Так как $G$ — связный граф, то $q \geq p - 1$.

*a)* Базис индукции: $q = p - 1$. Так как $G$ — связный и $q = p - 1$, то согласно пункту 3 теоремы 2 $G$ — дерево, то есть, в $G$ нет циклов. Тогда $r = 1$. Отсюда $p - q + r = p - (p - 1) + 1 = 2$.

*b)* Пусть для $q$: $p - 1 \leq q < q_0$ теорема справедлива. Докажем, что для $q = q_0$ она также справедлива. Пусть $G$ — связный граф с $p$ вершинами и $q_0$ рёбрами и пусть в его планарной реализации $r$ граней. Так как $q_0 > p - 1$, то $G$ — не дерево. Следовательно, в $G$ есть цикл. Пусть ребро $e$ входит в цикл. Тогда к нему с двух сторон примыкают разные грани. Удалим ребро $e$ из $G$. Тогда две грани сольются в одну, а полученный граф $G_1$ останется связным. При этом получится планарная реализация графа $G_1$ с $p$ вершинами и $q_0 - 1$ рёбрами и $r - 1$ гранями. Так как $q_0 - 1 < q_0$, то, по предположению индукции, для $G_1$ справедлива формула Эйлера, то есть $p - (q_0 - 1) + (r - 1) = 2$, откуда $p - q_0 + r = 2$. Что и требовалось доказать.

**Следствие 1.** Формула Эйлера справедлива и для геометрической реализации связных графов на сфере.

**Доказательство.** Пусть связный граф $G$ с $p$ вершинами и $q$ рёбрами реализован на сфере $S$ так, что число граней равно $r$. Пусть точка $A$ на сфере не лежит на линиях этой геометрической реализации. Пусть $P$ — некоторая плоскость. Поставим сферу $S$ на плоскость $P$ так, чтобы точка $A$ была самой удалённой от плоскости. Спроектируем $S$ на $P$ центральным проектированием с центром в точке $A$. Тогда на плоскости $P$ мы получим геометрическую реализацию связного графа с $p$ вершинами и $q$ рёбрами, причём число граней будет равно $r$ (грань на сфере, содержащая $A$, отображается на внешнюю грань на плоскости). По теореме получаем $p - q + r = 2$. Следствие доказано.

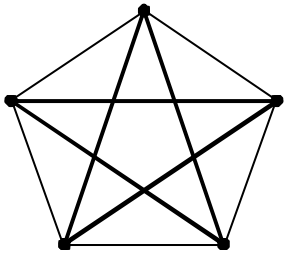
**Следствие 2.** Для любого выпуклого многогранника справедливо равенство $p - q + r = 2$, где $p$ — число вершин, $q$ — число рёбер, $r$ — число граней.

**Доказательство.** Пусть выпуклый многогранник $M$ имеет $p$ вершин, $q$ рёбер и $r$ граней. Пусть $O$ — внутренняя точка многогранника.

Разместим сферу $S$ с центром в точке $O$ настолько большого радиуса, чтобы $M$ целиком содержался в $S$. Рассмотрим центральное проектирование с центром в точке $O$, и спроектируем вершины и рёбра $M$ на $S$. Тогда на $S$ мы получим геометрическую реализацию некоторого связного графа с $p$ вершинами, $q$ рёбрами и $r$ гранями. Отсюда согласно следствию 1 $p - q + r = 2$. Следствие 2 доказано.

## §20. Доказательство непланарности графов $K_5$ и $K_{3,3}$. Теорема Понтрягина-Куратовского (доказательство в одну сторону)

**Определение 1.** Графом $K_5$ называется граф с пятью вершинами, в котором каждая пара вершин соединена ребром.

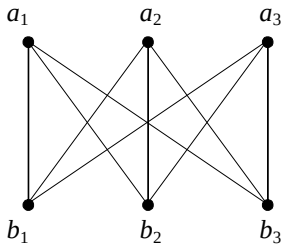


$K_5$

**Теорема 6.** Граф $K_5$ не планарен.

**Доказательство.** Допустим, что для графа $K_5$ существует планарная реализация. Так как граф $K_5$ связен, то для этой планарной реализации справедлива формула Эйлера $p - q + r = 2$. Поскольку в графе $K_5$ имеем $p = 5$ и $q = 10$, то число всех граней должно равняться $r = 2 - p + q = 7$. Пусть грани занумерованы 1, 2, …, $r$ и пусть при обходе $i$-ой грани по периметру (по её краю) проходится $q_i$ рёбер. Так как при этом каждое ребро обходится дважды (оно является стороной для двух граней), то $\sum_{i=1}^{r} q_i = 2q = 20$. Но в каждой грани не менее трёх сторон. Поэтому $q_i \geq 3$ для всех $i$. Отсюда $\sum_{i=1}^{r} q_i \geq 3r = 21$. Получаем $20 \geq 21$ — противоречие. Значит, для графа $K_5$ не существует планарной реализации.

**Определение 2.** Графом $K_{3,3}$ называется граф с шестью вершинами $a_1$, $a_2$, $a_3$, $b_1$, $b_2$, $b_3$, в котором каждая вершина $a_i$ соединена ребром с каждой вершиной $b_j$ и других рёбер нет.




$K_{3,3}$

**Теорема 7.** Граф $K_{3,3}$ не планарен.

**Доказательство.** Допустим, что для графа $K_{3,3}$ существует планарная реализация. Так как граф $K_{3,3}$ связен, то для этой планарной реализации справедлива формула Эйлера $p - q + r = 2$. Поскольку в графе $K_{3,3}$ имеем $p = 6$ и $q = 9$, то число всех граней должно равняться $r = 2 - p + q = 5$. Так же, как в доказательстве предыдущей теоремы, получаем, что $\sum_{i=1}^{r} q_i = 2q = 18$, где $q_i$ — число сторон в $i$-ой грани. Но в графе $K_{3,3}$ нет циклов длины 3. Поэтому в каждой грани не менее 4 сторон. Следовательно, $q_i \geq 4$ для всех $i$. Отсюда $\sum_{i=1}^{r} q_i \geq 4r = 20$. Получаем $18 \geq 20$ — противоречие. Значит, для графа $K_{3,3}$ не существует планарной реализации.

**Определение 3.** *Подразделением ребра* $(a, b)$ называется операция, состоящая в следующих действиях:

1) удаление $(a, b)$,
2) добавление новой вершины $c$,
3) добавление рёбер $(a, c)$ и $(c, b)$.

**Определение 4.** Граф $H$ называется *подразделением графа* $G$, если $H$ можно получить из $G$ путём конечного числа подразделений своих рёбер.

**Определение 5.** Два графа называются *гомеоморфными*, если существуют их подразделения, которые изоморфны.

**Теорема 8 (Понтрягина-Куратовского).** Граф является планарным тогда и только тогда, когда он не содержит ни одного подграфа, гомеоморфного графам $K_5$ или $K_{3,3}$.

**Доказательство.** Необходимость. Пусть $G$ — планарный. Допустим, что он содержит подграф $G_1$, гомеоморфный графу $K_5$ или $K_{3,3}$. Рассмотрим планарную реализацию графа $G$. Удалив лишние вершины и рёбра, мы получим планарную реализацию подграфа $G_1$. Но $G_1$ геометрически — это граф $K_5$ или $K_{3,3}$ с точками на рёбрах. Если проигнорировать эти точки, то мы получим планарную реализацию графа $K_5$ или $K_{3,3}$. Но это невозможно в силу теорем 1 и 2. Необходимость доказана.

Достаточность без доказательства.

## §21. Теорема о раскраске планарных графов в пять цветов

**Лемма 1.** Для любой геометрической реализации на плоскости связного планарного графа с $q$ рёбрами выполняется равенство:

$$\sum_{i=1}^{r} q_i = 2q,$$

где суммирование ведётся по всем граням (включая внешнюю).

**Доказательство.** Равенство следует из того, что у каждого ребра две стороны и при суммировании $q_i$ каждое ребро учитывается дважды: либо оно входит в границы двух соседних граней, либо оно дважды учитывается в одной грани. Лемма доказана.

**Теорема 9.** Если в связном планарном графе $G = (V, E)$ с $p$ вершинами и $q$ рёбрами, отличном от дерева, нет циклов длины меньше $k$ ($k \geq 3$), то $q \leq \frac{k}{k-2}(p-2)$.

**Доказательство.** Так как по условию $q_i \geq k$, то из леммы получаем $2q \geq kr$ и $r \leq \frac{2q}{k}$. Из формулы Эйлера $r = 2 - p + q$. Отсюда $2 - p + q \leq \frac{2q}{k}$. Далее $(k-2)q \leq k(p-2)$ и $q \leq \frac{k}{k-2}(p-2)$. Теорема доказана.

**Следствие.** В любом связном планарном графе $G = (V, E)$ без петель и кратных рёбер с $p \geq 3$ вершинами и $q$ рёбрами справедливо неравенство: $q \leq 3(p-2)$.

**Определение 1.** Подмножество $V_1 \subseteq V$ вершин графа $G = (V, E)$ называется *независимым*, если никакие две вершины из $V_1$ не соединяются ребром.

**Определение 2.** Пусть есть некоторое множество $C=\{C_1,C_2,\ldots,C_m\}$ — множество *цветов*. Тогда *раскраской графа* $G = (V, E)$ (*вершинной*) называется любое отображение $\varphi$: $V \to C$. Раскраска называется *правильной*, если для любого цвета вершины этого цвета образуют независимое множество.

**Лемма 2.** В планарном графе без петель и кратных рёбер существует вершина $v$:

$$\deg v \le 5.$$

**Доказательство.** Пусть $G$ — планарный граф с $p$ вершинами и $q$ рёбрами. Пусть в $G$ нет вершин степени 0 и 1. Тогда $q \le 3(p-2) < 3p$. Пусть $d_{\min}$ — минимальная степень вершин в $G$. Тогда получаем

$$6p > 2q = \sum_{i=1}^{p} \deg v_i \ge p d_{\min}.$$

Отсюда $d_{\min} < 6$, то есть $d_{\min} \le 5$. Лемма доказана.

**Теорема 10.** Вершины любого планарного графа можно правильно раскрасить в не более чем 5 цветов.

**Доказательство.** Проведём индукцию по числу вершин $p$.

1) Базис индукции: $p = 1$ — очевидно.

2) Пусть для $p < p_0$ утверждение справедливо и пусть $G=(V,E)$ — планарный граф с $|V| = p_0$. Согласно лемме 2 в $G$ есть вершина $v$ степени не более 5. Рассмотрим укладку на плоскости графа $G$ без пересечения рёбер. Удалим из $G$ вершину $v$ и все инцидентные ей рёбра. Получим планарный граф $G_1$ с числом вершин $p_0 - 1$. По предположению индукции его вершины можно правильно раскрасить в 5 цветов $C_1$, $C_2$, $C_3$, $C_4$, $C_5$. Пусть в $G$ вершина $v$ смежна с $v_1$, $v_2$, …, $v_k$, где $k \le 5$. Возможны два случая:

*a)* Среди цветов вершин $v_1, v_2, \ldots, v_k$ в $G$ нет цвета $C_i$ $(1 \le i \le 5)$. Тогда вершине $v$ припишем цвет $C_i$ и получим правильную раскраску графа $G$ в 5 цветов.

*b)* Степень вершины $v$ равна 5 и среди вершин $v_1$, $v_2$, …, $v_5$ в $G_1$ есть все 5 цветов. Без ограничения общности будем считать, что в укладке графа $G$ рёбра $(v, v_1)$, $(v, v_2)$, $(v, v_3)$, $(v, v_4)$, $(v, v_5)$ выходят из $v$ в порядке по часовой стрелке и что $C(v_i) = C_i$, $i = 1, \ldots, 5$. Пусть $A$ — множество всех вершин в $G_1$, до которых можно дойти из $v_1$ по рёбрам графа

$G_1$, используя только вершины цветов $C_1$ и $C_3$. Возможны два варианта:

*i)* $v_3 \notin A$. Тогда в $A$ поменяем цвета $C_1 \to C_3$, $C_3 \to C_1$. Так как вершины из $A$ не смежны с другими вершинами цветов $C_1$ и $C_3$, то останется правильная раскраска и среди $v_1$, $v_2$, $v_3$, $v_4$, $v_5$ не будет цвета $C_1$. Тогда вершине $v$ припишем цвет $C_1$.

*ii)* $v_3 \in A$. Это значит, что в $A$ есть цепь из $v_1$ в $v_3$, все вершины которой имеют цвета $C_1$ и $C_3$. Эта цепь вместе с рёбрами $(v_3, v)$ и $(v, v_1)$ образует цикл в $G$, причём вершины $v_2$ и $v_4$ лежат по разные стороны от этого цикла. Это значит, что из $v_2$ нельзя пройти в $v_4$ в графе $A$ только по вершинам цветов $C_2$ и $C_4$. Пусть $B$ — множество всех вершин в $G$, до которых можно дойти из $v_2$ по рёбрам графа $G$, используя только вершины цветов $C_2$ и $C_4$. Тогда $v_4 \notin B$ и далее поступаем как в *i)*.

В любом случае вершины графа $G$ можно правильно раскрасить в не более чем 5 цветов, и теорема доказана.

# Глава III. Основы теории управляющих систем

## §22. Схемы из функциональных элементов. Реализация функций алгебры логики схемами

**Определение 1.** Вершины орграфа, в которые не входит ни одной дуги, называются *истоками*.

**Определение 2.** Орграф называется *ациклическим*, если в нем нет ориентированных циклов.

**Определение 3.** В ациклическом орграфе *глубиной вершины* $v$ называется максимальное число дуг в ориентированном пути из какого-нибудь истока в вершину $v$.

Если в ациклическом орграфе есть дуга $(v_1, v_2)$, то глубина $v_2$ больше глубины $v_1$.

**Определение 4.** Орграф называется *упорядоченным*, если для каждой вершины $v_i$, в которую входит $k_i$ дуг, задан порядок $e_1, e_2, \text{K}, e_{k_i}$ этих дуг.

**Определение 5.** Систему Б = $\{g_1, g_2, \ldots, g_m\}$, где все $g_i$ — функции алгебры логики, будем называть *базисом функциональных элементов*.

**Определение 6.** *Схемой из функциональных элементов в базисе* Б называется ациклический упорядоченный орграф, в котором:

1) каждому истоку приписана некоторая переменная, причем разным истокам приписаны разные переменные (истоки при этом называются *входами схемы*, а приписанные им переменные — *входными переменными*);

2) каждой вершине, в которую входят $k \geq 1$ дуг, приписана функция из базиса Б, зависящая от $k$ переменных (вершина с приписанной функцией при этом называется *функциональным элементом*);

3) некоторые вершины выделены как *выходы* (истоки одновременно могут являться выходами).

Индукцией по глубине $q$ вершины $v$ определяется функция $f_v$, реализуемая в данной вершине. Если $q = 0$, то есть $v$ — исток, и $v$ приписана переменная $x_i$, то $f_v \equiv x_i$. Пусть реализуемые функции уже определены для всех вершин глубины меньшей, чем $q_0$, и глубина $v$ равна $q_0$. Пусть в $v$ входят дуги $e_1, e_2, \ldots, e_k$ из вершин $v_1, v_2, \ldots, v_k$ и в них реали-

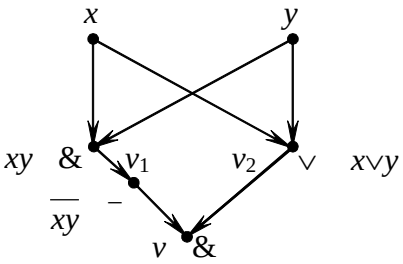
зуются функции $f_1$, $f_2$, …, $f_k$. Пусть вершине $v$ приписана функция $g$ ($x_1$, …, $x_k$). Тогда в $v$ реализуется функция $f_v = g$ ($f_1$, $f_2$, …, $f_k$).

**Определение 7.** Будем говорить, что *схема реализует систему функций, реализуемых в ее выходах*.

**Определение 8.** *Сложностью* схемы из функциональных элементов называется число функциональных элементов в схеме.

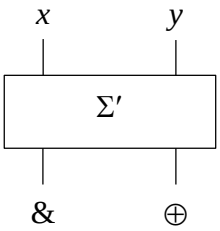
В дальнейшем по умолчанию будем подразумевать под базисом функциональных элементов систему $Б_0 = \left\{\vee, \&, \bar{}\right\}$. Так как все эти функции симметричны относительно своих переменных, то дуги, входящие в каждую вершину, можно не упорядочивать.

**Пример.** *Полусумматор.* Пусть $v$ и $v_1$ — выходы на рисунке, $f_v = \overline{xy}\,\&\,(x \vee y) = x \oplus y$; $f_{v_1} = xy$. Сложность (число элементов) полусумматора равна 4.




Полусумматор $\Sigma'$

В дальнейшем при построении схем ячейку полусумматора будем обозначать просто




Ячейка полусумматора $\Sigma'$

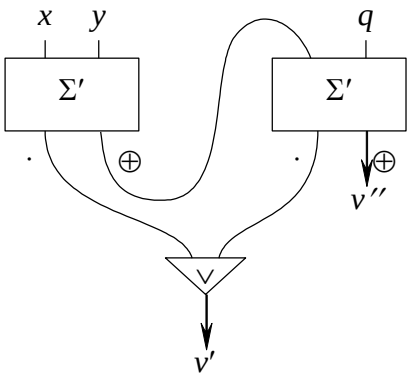
Пусть есть 2 $n$-разрядных числа, и требуется найти их сумму (в дальнейших обозначениях $x_i$, $y_i$ — разряды чисел, а $q_i$ — единицы переноса).

$$\begin{array}{ccccccc} q_0 & q_1 & q_2 & \text{K} & q_{n-1} & & \\ & x_1 & x_2 & \text{K} & x_{n-1} & x_n & \\ + & y_1 & y_2 & \text{K} & y_{n-1} & y_n & \\ \hline z_0 & z_1 & z_2 & \text{K} & z_{n-1} & z_n & \end{array}$$

При $i = 1, 2, \ldots, n-1$ задача решается системой функций

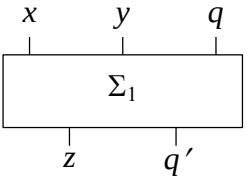
$$\begin{cases} z_i = x_i \oplus y_i \oplus q_i, \\ q_{i-1} = \mathrm{m}(x_i, y_i, q_i) = x_i y_i \vee y_i q_i \vee q_i x_i. \end{cases}$$

Таким образом, ячейку сумматора можно построить следующим образом:




Ячейка сумматора $\Sigma_1$

где $f_{v''} = (x \oplus y) \oplus q$, $f_{v'} = xy \vee (x \oplus y) \cdot q = xy \vee (x \vee y) \cdot q = m(x, y, q)$. Ячейку сумматора будем обозначать $\Sigma_1$ и в дальнейшем в схемах подставлять вместо ячейки сумматора символ $\Sigma_1$ с тремя входами ($x$, $y$, $z$) и двумя выходами ($z$, $q'$).



Ячейка сумматора $\Sigma_1$

Заметим, что сложность схемы, реализующей ячейку сумматора равна $L(\Sigma_1) = 9$. Очевидно, $z_n = x_n \oplus y_n$, $q_{n-1} = x_n y_n$, $z_0 = q_0$.

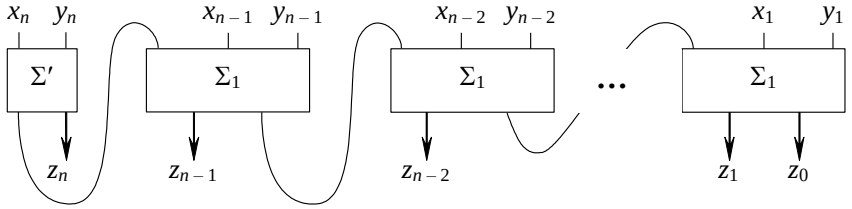
## §23. Сумматор. Верхняя оценка сложности сумматора. Вычитатель

Для набора $\tilde{\alpha} = (\alpha_1 \alpha_2 \ldots \alpha_n)$ будем обозначать $|\tilde{\alpha}| = (\alpha_1 \alpha_2 \ldots \alpha_n)_2$.

**Определение 1.** *Сумматором* $S_n$ порядка $n$ называется схема с $2n$ входами $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n$ и $n + 1$ выходом $z_0, z_1, z_2, \ldots, z_n$ такая, что $|\tilde{z}| = |S_n(\tilde{x}, \tilde{y})| = |\tilde{x}| + |\tilde{y}|$.

**Теорема 1.** Существует схемный сумматор порядка $n$ в базисе $\{\vee, \&, \bar{}\}$ с числом элементов $9n - 5$.

**Доказательство.** Построим искомый схемный сумматор. Для этого возьмём одну ячейку полусумматора, содержащую четыре элемента, и $n - 1$ ячейку сумматора, каждая из которых содержит девять элементов. Построим из этих частей сумматор.



Сумматор $S_n$

Вычислим сложность построенной схемы: $L(S_n) = 9L(\Sigma_1) + L(\Sigma') = 9(n-1) + 4 = 9n - 5$. Теорема доказана.

**Определение 2.** *Вычитателем* $W_n$ порядка $n$ называется схема с $2n$ входами $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n$ и $n$ выходами $z_1, z_2, \ldots, z_n$ такая, что при $|\tilde{x}| \geq |\tilde{y}|$

$$|\tilde{z}| = |W(\tilde{x}, \tilde{y})| = |\tilde{x}| - |\tilde{y}| .$$

**Теорема 2.** Существует схемный вычитатель порядка $n$ в базисе $\{\vee, \&, \bar{}\}$ с числом элементов $11n - 5$.

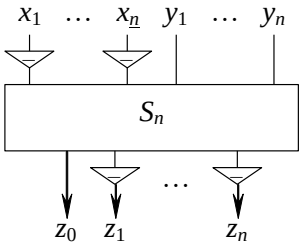
**Доказательство.** Заметим предварительно, что

$$|\bar{\alpha}| = (\bar{\alpha}_1 \bar{\alpha}_2 \ldots \bar{\alpha}_n) = 2^n - 1 - |\alpha|.$$

Действительно,

$$\begin{array}{rl} & (\bar{\alpha}_1 \bar{\alpha}_2 \ldots \bar{\alpha}_n)_2 \\ + & (\alpha_1 \alpha_2 \ldots \alpha_n)_2 \\ \hline & (1\ 1\ \ldots\ 1)_2 \quad = 2^n - 1 \end{array} .$$

Тогда вычитатель реализуется схемой



Вычитатель $W_n$

$$W_n(\tilde{x}, \tilde{y}) = |\tilde{x}| - |\tilde{y}| = 2^n - 1 - \left(\left(2^n - 1 - |\tilde{x}|\right) + |\tilde{y}|\right)$$

и его можно построить, используя $2n$ отрицаний и 1 сумматор порядка $n$. При этом $L(W_n) = 2n + L(S_n) = 2n + (9n - 5) = 11n - 5$. Так как $|x| \geq |y|$, то $\left(2^n - 1 - |x|\right) + y \leq 2^n - 1$, и выход вычитателя определен. Теорема доказана.

## §24. Метод Карацубы построения схемы для умножения, верхняя оценка её сложности

**Определение 1.** *Умножителем* $M_n$ порядка $n$ называется схема с $2n$ входами $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n$ и $2n$ выходами $z_1, \ldots, z_{2n}$ такая, что $|z| = |M_n(xy)| = |x| \cdot |y|$. При этом

$$\begin{cases} 0 \le |\tilde{x}| \le 2^n - 1 < 2^n \\ 0 \le |\tilde{y}| \le 2^n - 1 < 2^n \end{cases} \Rightarrow |\tilde{x}| \cdot |\tilde{y}| < 2^{2n}.$$

**Определение 2.** Через $M(n)$ обозначим наименьшую сложность умножителя порядка $n$ в базисе $\{\vee, \&, \bar{}\}$.

**Утверждение.** Существует схема из функциональных элементов для умножения $n$-разрядного числа $X$ на 1-разрядное число $y$ с числом элементов $n$.

**Доказательство.** Действительно, если $X = |(x_1, x_2, \ldots, x_n)|$ и $Xy = Z = |(z_1, z_2, \ldots, z_n)|$, то $z_i = x_i y$ для всех $i = 1, 2, \ldots, n$. Следовательно, для реализации такой схемы понадобится ровно $n$ элементов, реализующих конъюнкцию. Утверждение доказано.

При умножении двух $n$-разрядных чисел $X$ и $Y$ «в столбик» можно $n$ раз умножить $X$ на 1-разрядное число (всего $n^2$ конъюнкций) и затем $n - 1$ раз сложить числа длиной не более $2n$. Для реализации такой схемы необходим также $n - 1$ сумматор порядка $2n$. Согласно теореме 1, сложность сумматора порядка $2n$ равна $L(S_{2n}) = 9 \cdot 2n - 5 = 18n - 5$, и сложность подобного умножителя составит $n^2 + (n - 1) \cdot (18n - 5) = 19n^2 - 23n + 5$. Такой алгоритм (схема) имеет сложность по порядку $n^2$. Следующая теорема показывает, что такой алгоритм умножения «в столбик» не оптимален по порядку.

**Лемма 1.** Существует такая константа $C_1 > 0$, что

$$M(n + 1) \le M(n) + C_1 n$$

для всех $n$.

**Доказательство.** Пусть требуется перемножить два $(n + 1)$-разрядных числа $x = (x_0 x_1 \ldots x_n)$ и $y = (y_0 y_1 \ldots y_n)$. Тогда

$$\tilde{x}\tilde{y} = \left( x_0 \cdot 2^n + \underbrace{|x_1 \ldots x_n|}_{X} \right)\left( y_0 \cdot 2^n + \underbrace{|y_1 \ldots y_n|}_{Y} \right) =$$
$$= x_0 y_0 \cdot 2^{2n} + \left( x_0 \cdot Y + y_0 \cdot X \right) \cdot 2^n + X \cdot Y.$$

Поэтому для вычисления $\tilde{x}\tilde{y}$ достаточно использовать умножитель $M_n$ со сложностью $M(n)$ для вычисления $XY$, $2n$ элементов конъюнкции для вычисления $x_0Y$ и $y_0X$, 1 элемент конъюнкции для вычисления $x_0y_0$ и 3 сумматора порядка не более $2n + 2$, так как $\tilde{x}\tilde{y} < 2^{2n+2}$. Отметим, что числа $x_0y_0$, $x_0Y$ и $y_0X$ надо подавать на сумматоры со сдвигом, одновременно подавая на младшие разряды 0. При этом 0 можно предварительно получить подсхемой с 2 элементами, реализующей $x_0\overline{x_0} = 0$. Так как сложность каждого сумматора можно сделать не более $9(2n + 2)$, а сложность $M_n$ равна $M(n)$, то сложность полученной схемы будет не больше, чем $M(n) + C_1n$ для некоторой константы $C_1$. Лемма доказана.

**Лемма 2 (основная) [Карацуба А. А.].** Существует константа $C_2$ такая, что

$$M(2n) \le 3M(n) + C_2n$$

для всех $n$.

**Доказательство.** Пусть нужно перемножить два $2n$-разрядных числа $\tilde{x}$ и $\tilde{y}$. Разобьём их на части, содержащие по $n$ разрядов:

$$\tilde{x} = \left( \underbrace{x_1 x_2 \ldots x_n}_{X_1} \underbrace{x_{n+1} x_{n+2} \ldots x_{2n}}_{X_2} \right), \quad \tilde{y} = \left( \underbrace{y_1 y_2 \ldots y_n}_{Y_1} \underbrace{y_{n+1} y_{n+2} \ldots y_{2n}}_{Y_2} \right).$$

Тогда $\tilde{x} = X_1 \cdot 2^n + X_2$, $\tilde{y} = Y_1 \cdot 2^n + Y_2$ и

$$\tilde{x}\tilde{y} = X_1Y_1 \cdot 2^{2n} + (X_1Y_2 + X_2Y_1) \cdot 2^n + X_2Y_2 =$$
$$= X_1Y_1 \cdot 2^{2n} + [(X_1 + X_2)(Y_1 + Y_2) - X_1Y_1 - X_2Y_2] \cdot 2^n + X_2Y_2.$$

Так как $X_1Y_2 + X_2Y_1 \ge 0$, то при вычитании в квадратной скобке не возникнет отрицательных чисел. Таким образом, схему для умножения $\tilde{x}\tilde{y}$ можно построить, используя два умножителя $M_n$ с числом элементов $M(n)$ в каждом для вычисления $X_1Y_1$ и $X_2Y_2$, умножитель $M_{n+1}$ с числом элементов $M(n + 1)$ для вычисления $(X_1 + X_2)(Y_1 + Y_2)$, 4 сумматора

порядка не более $4n$ (так как $xy \le 2^{4n}$) и два вычитателя порядка $2n + 2$. В некоторых сумматорах опять на младшие разряды надо подавать 0, который реализуем подсхемой с 2 элементами: $0 = x\bar{x}$, где $x$ — любая входная переменная. Для построения схемы $M_{2n}$ с учётом леммы 1 получим для некоторых констант $C$ и $C_2$:

$$M(2n) \le 2M(n) + M(n+1) + Cn \le 3M(n) + C_1 n + Cn = 3M(n) + C_2 n.$$

Лемма доказана.

**Лемма 3.** Существует такая константа $C_3 > 0$, что для любого натурального $k$ верно

$$M(2^k) \le C_3 3^k.$$

**Доказательство.** Положим $f(k) = \frac{M(2^k)}{3^k}$. Тогда из леммы 2 имеем

$$\frac{M(2^k)}{3^k} \le \frac{M(2^{k-1})}{3^{k-1}} + \frac{C_2}{3}\left(\frac{2}{3}\right)^{k-1}$$

и

$$f(k) \le f(k-1) + \frac{C_2}{3}\left(\frac{2}{3}\right)^{k-1} \le f(k-2) + \frac{C_2}{3}\left(\frac{2}{3}\right)^{k-2} + \frac{C_2}{3}\left(\frac{2}{3}\right)^{k-1} \le \mathrm{K}$$

$$\mathrm{K} \le f(1) + \frac{C_2}{3}\left[\frac{2}{3} + \left(\frac{2}{3}\right)^2 + \mathrm{K} + \left(\frac{2}{3}\right)^{k-1}\right] \le C_3$$

для некоторой константы $C_3$, поскольку сумма в квадратных скобках не превосходит сумму 2 бесконечно убывающей геометрической прогрессии с первым членом $\frac{2}{3}$ и знаменателем $\frac{2}{3}$. Таким образом, $\frac{M(2^k)}{3^k} \le C_3$ и $M(2^k) \le C_3 3^k$. Лемма доказана.

**Теорема 3.** Существует схемный умножитель в базисе $\{\vee, \&, \bar{}\}$ с числом элементов

$$O\left(n^{\log_2 3}\right).$$

**Доказательство.** Пусть $n$ — любое натуральное число и $n>1$. Тогда существует натуральное $k$ такое, что $2^{k-1} < n \le 2^k$. Для умножения $n$-

разрядных чисел будем использовать схему $M_{2^k}$ с числом элементов $M(2^k)$, подавая на старшие $2^k - n$ разрядов обоих сомножителей 0, предварительно реализованный подсхемой из 2 элементов. Тогда имеем, исходя из леммы 3

$$M(n) \le M\left(2^k\right) + 2 \le C_3 3^k + 2 = 3C_3 3^{k-1} + 2 =$$
$$= 3C_3 2^{(k-1)\log_2 3} + 2 < 3C_3 n^{\log_2 3} + 2 \le Cn^{\log_2 3}$$

для некоторой константы $C$. Теорема доказана.

**Замечание.** Существует практически применимый метод Шёнхаге-Штрассена умножения с оценкой сложности $O(n \log n \cdot \log\log n)$.

## §25. Дешифратор. Асимптотика сложности дешифратора. Верхняя оценка сложности реализации произвольной функции алгебры логики

**Определение.** *Дешифратором* $Q_n$ порядка $n$ называется схема из функциональных элементов с $n$ входами $x_1$, $x_2$, …, $x_n$ и $2^n$ выходами $z_0, z_1, \ldots, z_{2^n-1}$ такая, что если $|x_1x_2\ldots x_n| = i$, то $z_i = 1$ и $z_j = 0$ при $i \ne j$:

$$z_i\left(x_1, \ldots, x_n\right) = \begin{cases} 1, & \left|x_1 \ldots x_n\right| = i, \\ 0, & \left|x_1 \ldots x_n\right| \ne i. \end{cases}$$

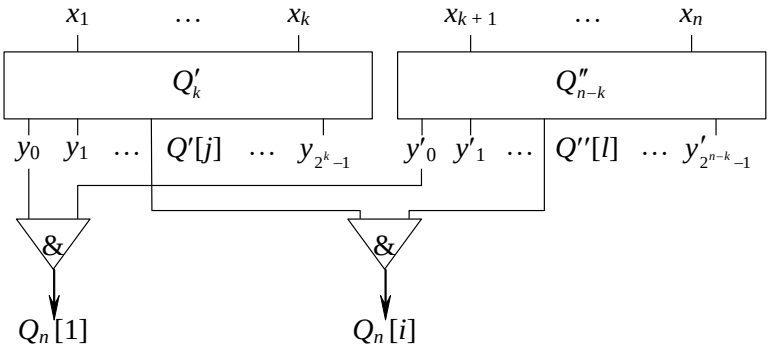
Заметим, что если $i = (i_1, i_2, \ldots, i_n)_2$, то $z_i\left(x_1, \ldots, x_n\right) = x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$.

**Лемма 4.** Существует дешифратор $Q_n$ с числом элементов, не превосходящим $n2^{n+1}$.

**Доказательство.** Для реализации каждой $z_i$ достаточно взять ровно $n-1$ конъюнкций и не более $n$ отрицаний, то есть всего менее, чем $2n$ функциональных элементов. Всего различных конъюнкций ровно $2^n$, и сложность дешифратора не превосходит $n2^{n+1}$. Лемма доказана.

**Теорема 4.** Сложность минимального схемного дешифратора порядка $n$ не меньше, чем $2^n$ и асимптотически не больше, чем $2^n + O\left(n \cdot 2^{\frac{n}{2}}\right)$.

**Доказательство.** 1) Поскольку у дешифратора $Q_n$ ровно $2^n$ выходов, на которых реализуются различные функции, не равные входным переменным, сложность минимального дешифратора не меньше, чем $2^n$.




2) Докажем существование дешифратора со сложностью $2^n + O\left(n \cdot 2^{\frac{n}{2}}\right)$. Разобьём набор входных переменных $x = (x_1, \ldots, x_n)$ на поднаборы $x' = (x_1, \ldots, x_k)$ и $x'' = (x_{k+1}, \ldots, x_n)$, где $k$ — некоторый параметр и $1 \le k \le n - 1$. Пусть $Q'$ и $Q''$ —функциональные дешифраторы порядка $k$ и $n - k$ от базовых переменных $x'$ и $x''$, а $\Sigma'$ и $\Sigma''$ — соответствующие им схемные дешифраторы, построенные по лемме. Легко видеть, что любую конъюнкцию $Q_n[i]$, $1 \le i \le 2^n$, можно представить в виде $Q_n[i] = Q'[j] \cdot Q''[l]$, где $i = 2^{n-k}(j - 1) + l$ и $1 \le j \le 2^k$, $1 \le l \le 2^{n-k}$. Дешифратор $\Sigma$ порядка $n$ от базовых переменных $x$ содержит дешифраторы $\Sigma'$ и $\Sigma''$ в качестве подсхем и реализует каждую функцию алгебры логики $Q_n[i]$, $1 \le i \le 2^n$, с помощью одного функционального элемента &, входы которого присоединены к выходам $\Sigma'$ и $\Sigma''$ в соответствии с формулой $Q_n[i] = Q'[j] \cdot Q''[l]$. Из построения $\Sigma$ следует, что $L(\Sigma) = 2^n + L(\Sigma') + L(\Sigma'') \le 2^n + k \cdot 2^{k+1} + (n - k)2^{n-k+1}$, и поэтому при $k = \left\lfloor \frac{n}{2} \right\rfloor$ получим: $L(\Sigma) \le 2^n + O\left(n \cdot 2^{\frac{n}{2}}\right)$. Теорема доказана.

**Следствие.** Для любой функции алгебры логики $f(x_1,\ldots,x_n)$ существует реализация её схемой из функциональных элементов в базисе $\{\vee, \&, \bar{}\}$ со сложностью, не превосходящей $2 \cdot 2^n + O\left(n \cdot 2^{\frac{n}{2}}\right)$.

**Доказательство.** Если $f \equiv 0$, то реализуем $f = x_1 \cdot \overline{x_1}$. Если $f \ne 0$, то $f(x_1, \ldots, x_n) = \bigvee_{(\sigma_1,\ldots,\sigma_n):\, f(\sigma_1,\ldots,\sigma_n)=1} x_1^{\sigma_1} \ldots x_n^{\sigma_n}$, и $L \le L(Q_n) + 2^n - 1 \le 2 \cdot 2^n + O\left(n \cdot 2^{\frac{n}{2}}\right)$. Следствие доказано.

## §26. Мультиплексор. Верхняя оценка сложности мультиплексора. Метод Шеннона

**Определение 1.** *Мультиплексором $\mu_n$ порядка $n$* называется схема из функциональных элементов с $n + 2^n$ входами $\underbrace{x_1, \text{K}\, x_n}_{\text{адресные входы}}$, $\underbrace{y_0, y_1, \text{K}\, y_{2^n-1}}_{\text{информационные входы}}$ и 1 выходом $z$ такая, что если на входы $x_1, \ldots, x_n$ поступает набор $(\alpha_1, \ldots, \alpha_n)$, то $z = y_{(\alpha_1, \text{K}\, ,\alpha_n)_2}$.

**Теорема 5.** Существует мультиплексор $\mu_n$ порядка $n$ с числом элементов

$$L(\mu_n) \le 3 \cdot 2^n + O\left(n \cdot 2^{\frac{n}{2}}\right).$$

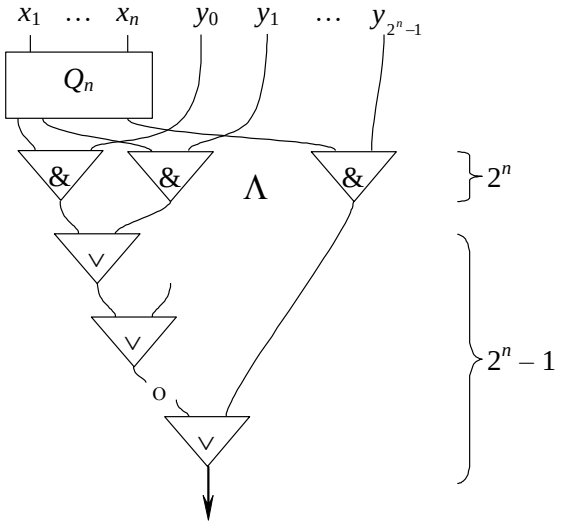
**Доказательство.** Заметим, что задачу решает функция

$$z = \bigvee_{(\alpha_1, \text{K}\, ,\alpha_n)} x_1^{\alpha_1} \cdot x_2^{\alpha_2} \text{L}\ x_n^{\alpha_n} \cdot y_{(\alpha_1 \text{K}\, \alpha_n)_2}.$$

Для её вычисления достаточно использовать один дешифратор, $2^n$ конъюнкций и $2^n - 1$ дизъюнкций и

$$L(\mu_n) \le L(Q_n) + 2^n + 2^n - 1 \le 3 \cdot 2^n + O\left(n 2^{\frac{n}{2}}\right).$$

Теорема доказана.



**Определение 2.** *Сложностью* $L$ ($S$) *схемы* $S$ называется число элементов в ней.

**Определение 3.** *Сложностью функции алгебры логики* $f(x_1, \ldots, x_n)$ называется $L(f) = \min\limits_{S \text{ реализует } f} L(S)$.

**Определение 4.** *Функцией Шеннона* $L(n)$ для схемы из функциональных элементов называется $L(n) = \max\limits_{f \text{ от } x_1, \ldots, x_n} L(f)$.

Обозначения: $g(n) \lesssim h(n) \Leftrightarrow g(n) \le h(n) \cdot (1 + o(1))$; $g(n) \gtrsim h(n) \Leftrightarrow$ $\Leftrightarrow g(n) \ge h(n) \cdot (1 + o(1))$.

**Определение 5.** *Универсальным многополюсником* $U_n$ порядка $n$ называется схема из функциональных элементов с $n$ входами и $2^{2^n}$ выходами, на которых реализуются все $2^{2^n}$ функций от $x_1, \ldots, x_n$.

**Теорема 6**. Минимальная сложность универсального многополюсника порядка $n$ равна $2^{2^n} - n$.

**Доказательство.** 1) Очевидно, что $L(U_n) \ge 2^{2^n} - n$, так как всего функций алгебры логики от $n$ переменных, отличных от входных переменных, ровно $2^{2^n} - n$.

2) Докажем существование универсального многополюсника с числом элементов $2^{2^n} - n$. Для этого построим какую-нибудь схему из функциональных элементов, реализующую все функции алгебры логики. Затем оставим из каждой группы эквивалентных вершин (в которых реализуются одинаковые функции) лишь одну, наиболее близкую к входам, подсоединив выходы удалённых к выходу оставшейся. В результате получим, что в каждой вершине реализуется уникальная функция алгебры логики. Но всего функций, отличных от входных переменных — $2^{2^n} - n$. Следовательно, и вершин — $2^{2^n} - n$. Теорема доказана.

**Теорема 7.** $L(n) \lesssim 6 \cdot 2^n \cdot \frac{1}{n}$.

**Доказательство.** Рассмотрим произвольную функцию $f(x_1, \ldots, x_n)$. Выберем некоторое натуральное $k$ ($1 \le k \le n$) и рассмотрим разложение взятой функции по первым $k$ переменным:

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

Построим схему из функциональных элементов из универсального многополюсника $U_{n-k}$ порядка $n - k$ от базовых переменных $x_{k+1}, \ldots, x_n$ и мультиплексора $\mu_n$ *порядка* $n$ с адресными переменными $x_1, \ldots, x_k$, на информационные входы которого подаются те выходы $U_{n-k}$, на которых реализуются функции $f(\sigma_1,\text{K},\sigma_k,x_{k+1},\text{K},x_n)$. Мультиплексор можно построить так, что его сложность не превзойдёт $3\cdot 2^k + O\left(k\cdot 2^{\frac{n}{2}}\right)$, а универсальный многополюсник так, что его сложность будет не больше, чем $2^{2^{n-k}}$. Итак,

$$L(n) = L(\mu_k) + L(U_{n-k}) \le 3\cdot 2^k + O\left(k\cdot 2^{\frac{n}{2}}\right) + 2^{2^{n-k}}.$$

Полагая $k = \left\lceil n - \log_2\left(n - 2\log_2 n\right)\right\rceil$ (при этом $k \le n - \log_2(n - 2\log_2 n) + 1$, а $n - k \le \log_2(n - 2\log_2 n)$), получим, что

$$2^k \le 2^{n-\log_2(n-2\log_2 n)+1} = 2^{n+1}\cdot\frac{1}{n-2\log_2 n} \sim 2\cdot\frac{2^n}{n},$$

$$2^{2^{n-k}} \le 2^{n-2\log_2 n} = \frac{2^n}{n^2} = o\left(\frac{2^n}{n}\right)$$

и в итоге

$$L(S) \lesssim \left[3\cdot 2\cdot\frac{2^n}{n} + O\left(n2^{\frac{n}{2}}\right) + o\left(\frac{2^n}{n}\right)\right] \sim 6\cdot\frac{2^n}{n}.$$

Теорема доказана.

**Определение 6.** Пусть $\gamma(L, n)$ — *число всех попарно неизоморфных схем из функциональных элементов* с входными переменными $x_1, \ldots, x_n$ и выходной переменной $z_1$, сложность которых не превосходит $L$.

**Лемма 5.** В функциональном базисе $\{\&, \vee, \bar{\ }\}$ $\gamma(L, n) \le (L + n)^{2L+4}$.

**Доказательство.** Можно выбрать целые неотрицательные числа $L_1$, $L_2$, $L_3$ так, чтобы их сумма не превосходила $L$, не более, чем $(L + 1)^3$ способами. Можно взять $L_1$ конъюнкций, $L_2$ дизъюнкций, $L_3$ отрицаний, а затем каждый вход каждого из них «присоединить» к выходу некоторого другого функционального элемента или к входу схемы не более, чем $(L + n)^{2L}$ способами, и пометить в качестве выхода одну из не более, чем $L + n$ точек.

Тогда $\gamma(L, n) \le (L + 1)^3\cdot(L + n)^{2L}\cdot(L + n) \le (L + n)^{2L+4}$. Лемма доказана.

**Теорема 8.** Для функции Шеннона $L(n)$ справедливо $L(n) \gtrsim \frac{1}{2} \cdot \frac{2^n}{n}$.

**Доказательство.** Так как, по определению, схемами сложности не более $L(n)$ реализуются все функции от $n$ переменных, то $\gamma(L(n), n) \geq 2^{2^n}$, но в то же время согласно лемме $\gamma(L, n) \leq (L + n)^{2L+4}$. Следовательно, $(L(n)+n)^{2L(n)+4} \geq 2^{2^n} \Rightarrow (2L(n)+4)\log_2(L(n)+n) \geq 2^n$. Так как $L(n) \lesssim 6 \cdot 2^n \cdot \frac{1}{n}$, то начиная с некоторого номера $n$, $n + L(n) \leq 2^n$ и $2L(n)+4 \geq \frac{2^n}{n}$, откуда $L(n) \gtrsim \frac{1}{2} \cdot \frac{2^n}{n}$. Теорема доказана.

## §27. Шифратор. Верхняя оценка сложности шифратора

**Определение.** *Шифратором $D_n$ порядка $n$* называется схема из функциональных элементов с $2^n$ входами $x_0, x_1, \ldots, x_{2^n-1}$ и $n$ выходами $y_1, y_2, \ldots, y_n$ такая, что если на вход поступает набор с одной единицей по переменной $x_i$, то на выходе образуется набор $(\beta_1, \beta_2, \ldots, \beta_n)_2 = i$.

**Теорема 9.** Существует шифратор $D_n$ порядка $n$ со сложностью, не превосходящей

$$n \cdot 2^{n-1}.$$

**Доказательство.** Задачу решает система функций

$$y_j = \bigvee_{(\sigma_1, \ldots, \sigma_{j-1}, 1, \sigma_{j+1}, \ldots, \sigma_n)} x_{(\sigma_1, \ldots, \sigma_{j-1}, 1, \sigma_{j+1}, \ldots, \sigma_n)}$$

(например, $y_n = x_1 \vee x_3 \vee x_5 \vee x_7 \vee \ldots \vee x_{2^n-1}$). Всего в каждой дизъюнкции $2^{n-1}$ слагаемых, следовательно, необходимо $2^{n-1} - 1$ дизъюнкторов, всего таких функций надо реализовать $n$, то есть получаем оценку сложности шифратора $L(D_n) \leq (2^{n-1} - 1) \cdot n < n \cdot 2^{n-1}$. Теорема доказана.

# Глава IV. Основы теории кодирования

## §28. Алфавитное кодирование. Теорема Маркова о взаимной однозначности алфавитного кодирования

**Определение 1.** Пусть $A = \{a_1, a_2, \ldots, a_r\}$ — *исходный алфавит*, $B = \{b_1, b_2, \ldots, b_m\}$ — *кодирующий алфавит* и

$$A^* = \varnothing \cup A \cup A^2 \cup A^3 \cup \ldots \cup A^n \cup \ldots,$$
$$B^* = \varnothing \cup B \cup B^2 \cup B^3 \cup \ldots \cup B^n \cup \ldots.$$

Тогда *алфавитным кодированием* $A^* \to B^*$ назовём отображение $\varphi : A \to B^*$ такое, что $a_i \to B_i$. Множество $\{B_1, B_2, \ldots, B_r\}$ при этом называется множеством *кодовых слов* (или просто *кодом*). При этом

$$\varphi : a_{i_1} a_{i_2} \text{K } a_{i_s} \to B_{i_1} B_{i_2} \text{K } B_{i_s}.$$

**Определение 2.** Кодирование $A^* \to B^*$ называется *взаимно однозначным* (*декодируемым, разделимым*), если для любых слов $\overline{a_1} \in A^*$ и $\overline{a_2} \in A^*$ выполняется $\overline{a_1} \neq \overline{a_2} \Rightarrow \varphi\left(\overline{a_1}\right) \neq \varphi\left(\overline{a_2}\right)$.

**Определение 3.** Код называется *равномерным*, если длины всех его кодовых слов одинаковы.

**Утверждение 1.** Любой равномерный код является взаимно однозначным.

**Определение 4.** Код называется *префиксным*, если никакое кодовое слово не является началом другого.

**Утверждение 2.** Любое префиксное кодирование является взаимно однозначным.

**Определение 5.** Код называется *постфиксным* (*суффиксным*), если никакое кодовое слово не является концом другого.

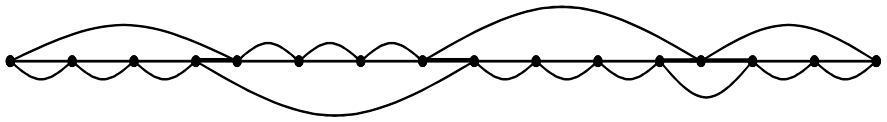
**Утверждение 3.** Любое постфиксное кодирование является взаимно однозначным.

**Определение 6**. Слово $\overline{b} \in B^*$ называется *неприводимым*, если $\overline{b}$ декодируется неоднозначно, однако, при выбрасывании из $\overline{b}$ любого связного непустого куска получается слово, которое декодируется не более, чем одним способом.

**Теорема 1 [Марков А. А.]**. Пусть $\varphi$: $a_i \to B_i$ ($i$ = 1, 2, …, $r$) — некоторое кодирование. Пусть $W$ — максимальное число кодовых слов, которые «помещаются» подряд внутри кодового слова. Пусть $l_i$ — длина слова $B_i$ и $L = \sum_{i=1}^{r} l_i$. Тогда если кодирование $\varphi$ не взаимно однозначно, то существуют два различных слова $a' \in A^*$, $a'' \in A^*$,

$$\text{длина}(a') \le \left\lfloor \frac{(W+1)(L-r+2)}{2} \right\rfloor, \ \text{длина}(a'') \le \left\lfloor \frac{(W+1)(L-r+2)}{2} \right\rfloor \text{ и } \varphi(a') = \varphi(a'').$$

**Доказательство.** Пусть $\varphi$ не является взаимно однозначным. Тогда существует некоторое слово $\overline{b_1}$, которое допускает две расшифровки. Если слово $\overline{b_1}$ не является неприводимым, то выбрасывая из $\overline{b_1}$ куски несколько раз, получим неприводимое слово $\overline{b}$; иначе, положим $\overline{b} = \overline{b_1}$. Очевидно, это всегда можно сделать. Рассмотрим любые две декодировки слова $\overline{b}$. Разрежем слово $\overline{b}$ в концевых точках кодовых слов каждого из разбиений. Слова нового разбиения разделим на два класса: к I классу отнесём слова, являющиеся элементарными кодами, а ко II классу — все остальные слова (то есть слова, являющиеся началами кодовых слов одного разбиения и концами слов второго разбиения).



**Лемма.** Если $\overline{b}$ — неприводимое слово, то все слова $\beta_1, \beta_2, \ldots, \beta_m$ II класса различны.

**Доказательство.** Пусть $\beta' = \beta''$. Тогда, очевидно, слово $\overline{b}$ не будет неприводимым, поскольку при выкидывании отрезка между $\beta'$ и $\beta''$, вместе с любым одним из этих слов, получим снова две различные расшифровки этого слова (проверьте). Лемма доказана.

Таким образом, все $\beta_1, \beta_2, \ldots, \beta_m$ разные. Тогда число слов второго класса не превосходит числа непустых начал элементарных кодов, то есть не превосходит

$$(l_1 - 1) + (l_2 - 1) + \ldots + (l_r - 1) = L - r.$$

Слова из второго класса разбивают слово не более чем на $L - r + 1$ кусков. Рассмотрим пары соседних кусков. Тогда согласно одному разбиению в одной половинке уложится не более одного кодового слова, а в другой — не более $W$ (согласно второму разбиению ситуация симметрична). Всего пар кусков не больше, чем

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

а в каждом из них укладывается слов не более чем $W + 1$. Отсюда число кодовых слов в любом разбиении не превосходит $\frac{L-r+2}{2}(W+1)$, а поскольку число целое, то не превосходит и целой части $\left\lfloor \frac{(W+1)(L-r+2)}{2} \right\rfloor$. Теорема доказана.

## §29. Неравенство Макмиллана

**Теорема 2 (неравенство Макмиллана).** Пусть задано кодирование $\varphi : a_i \to B_i$ ($i$ = 1, 2, …, $r$) и пусть в кодирующем алфавите $B$ — $q$ букв и *длина* ($B_i$) = $l_i$ ($i$ = 1, 2, …, $r$). Тогда если $\varphi$ взаимно однозначно, то

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

**Доказательство.** Положим $x = \sum_{i=1}^{r} \frac{1}{q^{l_i}}$. Тогда для любого натурального $n$

$$x^n = \left( \sum_{i_1=1}^{r} \frac{1}{q^{l_{i_1}}} \right) \left( \sum_{i_2=1}^{r} \frac{1}{q^{l_{i_2}}} \right) \text{L} \left( \sum_{i_n=1}^{r} \frac{1}{q^{l_{i_n}}} \right) = \sum_{i_1=1}^{r} \sum_{i_2=1}^{r} \text{K} \sum_{i_n=1}^{r} \frac{1}{q^{l_{i_1}+l_{i_2}+\text{K}+l_{i_n}}}.$$

Обозначая $l_{\max} = \max_{1 \le i \le r} l_i$ и приводя подобные члены, получим, что эта сумма равна $\sum_{k=1}^{n \cdot l_{\max}} \frac{c_k}{q^k}$.

**Лемма.** $c_k \le q^k$ ($\forall k$).

**Доказательство.** За $c_k$ обозначено, очевидно, число наборов ($i_1$, …, $i_n$) ($1 \le i_j \le r$), для которых $l_{i_1} + l_{i_2} + \text{K} + l_{i_n} = k$. Но такой сумме соответствует слово $B_{i_1} B_{i_2} \text{K}\, B_{i_n}$ и

$$\textit{длина}\left(B_{i_1} B_{i_2} \text{K}\, B_{i_n}\right) = l_{i_1} + l_{i_2} + \text{K} + l_{i_n} = k\,.$$

В силу того, что кодирование взаимно однозначно, различным наборам соответствуют различные сообщения, а различных сообщений длины $k$ в алфавите из $q$ букв не более $q^k \Rightarrow \forall k\ (c_k \le q^k)$.

Лемма доказана.

Согласно лемме $x^n = \sum\limits_{k=1}^{nl_{\max}} \dfrac{c_k}{q^k} \le \sum\limits_{k=1}^{nl_{\max}} 1 = nl_{\max} \Leftrightarrow x \le \sqrt[n]{nl_{\max}}\,,\ \forall n$.

Устремляя $n$ к бесконечности, получаем $x \le 1$. Теорема доказана.

## §30. Существование префиксного кода с заданными длинами кодовых слов

**Теорема 3.** Если $|B| = q$ и натуральные числа $l_1$, $l_2$, …, $l_r$ удовлетворяют неравенству

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

то существует префиксный код $B_1$, $B_2$, …, $B_r$ (в алфавите $B$) такой, что

$$\textit{длина}(B_i) = l_i \ (i = 1, 2, \ldots, r).$$

**Доказательство.** Пусть $\sum\limits_{i=1}^{r} \dfrac{1}{q^{l_i}} \le 1$ и для любого $k$ существует ровно $d_k$ таких $i$, что $l_i = k$, то есть $\sum\limits_{k=1}^{l_{\max}} \dfrac{d_k}{q^k} \le 1$. Тогда надо построить префиксный код, в котором ровно $d_1$ слов длины 1, $d_2$ слов длины 2, и т. д., $d_{l_{\max}}$ слов длины $l_{\max}$. Имеем $\forall m\ (1 \le m \le l_{\max}) \sum\limits_{k=1}^{m} \dfrac{d_k}{q^k} \le 1$, или, что то же самое,

$$\frac{d_1}{q} + \frac{d_2}{q^2} + \text{K} + \frac{d_{m-1}}{q^{m-1}} + \frac{d_m}{q^m} \le 1 \Leftrightarrow d_m \le q^m - \left(d_1 q^{m-1} + d_2 q^{m-2} + \text{K} + d_{m-1} q\right).$$

Рассмотрим это неравенство для $m = 1$: $d_1 \le q$. Для слов длины 1 всего предоставляется возможностей в алфавите мощности $q$ — ровно $q$ вариантов. После выбора $d_1$ слов длины 1 рассмотрим неравенство для $m = 2$: $d_2 \le q^2 - d_1 q$. Всего слов длины 2 — $q^2$, однако все они могут начинаться лишь с тех букв, которые не были выбраны в качестве слов длины 1, следовательно, остаётся ровно $q^2 - d_1 q$ возможностей выбрать слова длины 2, что удовлетворяет условию $d_2 \le q^2 - d_1 q$. Пусть уже выбраны $d_1$ слов длины 1, $d_2$ слов длины 2, и т. д., $d_{m-1}$ слов длины $m - 1$. Тогда для слов длины $m$ разрешено возможностей не меньше, чем

$$q^m - d_{m-1}q - d_{m-2}q^2 - \ldots - d_2 q^{m-2} - d_1 q^{m-1},$$

что удовлетворяет условию. Теорема доказана.

**Следствие.** Если существует взаимно однозначное кодирование со спектром длин слов $l_1, l_2, \ldots, l_r$ в алфавите $B$, то в $B$ существует префиксный код с тем же спектром длин слов.

## §31. Оптимальные коды, их свойства.

Будем рассматривать кодирование $A^* \to \{0, 1\}^*$. Пусть известны некоторые частоты $p_1, p_2, \ldots, p_k$ появления символов кодируемого алфавита в тексте:

$$\begin{array}{c} p_1 - a_1 \to B_1 - l_1 \\ p_2 - a_2 \to B_2 - l_2 \\ \text{M} \\ p_k - a_k \to B_k - l_k \end{array},$$

$l_j$ — длина $j$-го кодового слова, $p_1 + p_2 + \ldots + p_k = 1$, $p_j > 0$.

При кодировании текста длины $N$ его длина становится примерно равной

$$\sum_{i=1}^{k} (Np_i) l_i = N \sum_{i=1}^{k} p_i l_i .$$

**Определение 1.** *Ценой (стоимостью, избыточностью)* кодирования $\varphi$ называется функция $c(\varphi) = \sum_{i=1}^{k} p_i l_i$ .

**Определение 2.** Взаимно однозначное кодирование $\varphi$ называется оптимальным, если на нём достигается $\inf\limits_{\varphi-\text{взаимно однозначное}} c(\varphi)$.

**Утверждение 4.** Если существует оптимальный код, то существует оптимальный префиксный код с тем же спектром длин слов.

**Лемма 1.** Если $\varphi$ — оптимальное кодирование и $p_i > p_j$, то $l_i \le l_j$.

**Доказательство.** Допустим, что $p_i > p_j$ и $l_i > l_j$. Рассмотрим кодирование $\varphi$ и рассмотрим кодирование $\varphi'$, в котором переставим кодовые слова $B_i$ и $B_j$:

$$\varphi: \begin{cases} a_i \to B_i \\ a_j \to B_j \end{cases}, \quad \varphi': \begin{cases} a_i \to B_j \\ a_j \to B_i \end{cases}.$$

Тогда

$$c(\varphi) - c(\varphi') = (p_i l_i + p_j l_j) - (p_i l_j + p_j l_i) = (p_i - p_j)(l_i - l_j) > 0 \Rightarrow c(\varphi') < c(\varphi),$$

следовательно, $\varphi$ не является оптимальным — противоречие.

Лемма доказана.

**Лемма 2.** Если $\varphi$ — оптимальное префиксное кодирование и $l_{\max} = \max\limits_{1 \le i \le k} l_i$, *длина*$(B_j) = l_{\max}$, $B_j = B_j'\alpha$, где $\alpha \in \{0, 1\}$, то в коде $\varphi$ существует слово $B_r$ такое, что $B_r = B_j'\bar{\alpha}$.

**Доказательство.** Допустим, что в $\varphi$ нет слова $B_j'\bar{\alpha}$. Тогда заменим в $\varphi$ $B_j'\alpha$ на $B_j'$. Получим код $\varphi'$, который является префиксным, но

$$c(\varphi) - c(\varphi') = p_j \partial л(B_j'\alpha) - p_j \partial л(B_j') = p_j \Rightarrow c(\varphi') < c(\varphi),$$

следовательно, $\varphi$ не является оптимальным — противоречие. Лемма доказана.

**Лемма 3.** Если $\varphi$ — оптимальное префиксное кодирование и $p_1 \ge p_2 \ge \ldots \ge p_{k-1} \ge p_k$, то можно так переставить слова в коде $\varphi$, что получится оптимальное префиксное кодирование $\varphi'$ такое, что слова $B'_{k-1}$ и $B'_k$ в нём будут различаться только в последнем разряде.

**Доказательство.** Пусть $p_1 \ge p_2 \ge \ldots \ge p_{k-1} \ge p_k$. По лемме 2 в коде $\varphi$ есть слова $B'0$ и $B'1$ максимальной длины. Поменяем их местами с $B_{k-1}$ и $B_k$. Так как $p_{k-1} \le p_i$ и $p_k \le p_i$ для $1 \le i \le k-2$, то цена кодирования не увеличится и код останется оптимальным (префиксным). Лемма доказана.

**Лемма 4.** Рассмотрим кодирования

$$\varphi: \begin{matrix} p_1, p_2, \text{K}, p_k \\ B_1, B_2, \text{K}, B_k \end{matrix} \quad \text{и} \quad \varphi': \begin{matrix} p_1, p_2, \text{K}, p_{k-1}, p', p'' \\ B_1, B_2, \text{K}, B_{k-1}, B_k 0, B_k 1 \end{matrix},$$

где $p' + p'' = p_k$. Если один из этих наборов префиксный, то второй также префиксный и

$$c(\varphi') = c(\varphi) + p_k.$$

**Доказательство.** Первое утверждение легко проверяется. Далее

$$c(\varphi') - c(\varphi) = p' \cdot дл(B_k 0) + p'' \cdot дл(B_k 1) - p_k \cdot дл(B_k) =$$
$$= p'(l_k + 1) + p''(l_k + 1) - p_k l_k = (p' + p'')l_k + (p' + p'') - p_k l_k = p_k.$$

Лемма доказана.

## §32. Теорема редукции

**Теорема 4 (теорема редукции).** Пусть заданы 2 набора частот и 2 набора слов:

$$\varphi: \begin{matrix} p_1, p_2, \text{K}, p_k \\ B_1, B_2, \text{K}, B_k \end{matrix} \quad \text{и} \quad \varphi': \begin{matrix} p_1, p_2, \text{K}, p_{k-1}, p', p'' \\ B_1, B_2, \text{K}, B_{k-1}, B_k 0, B_k 1 \end{matrix}.$$

1) Тогда если $\varphi'$ — оптимальное префиксное кодирование, то и $\varphi$ — оптимальное префиксное кодирование.

2) Если же $\varphi$ — оптимальное префиксное кодирование и $p_1 \geq p_2 \geq \ldots \ldots \geq p_{k-1} \geq p' \geq p''$, то $\varphi'$ — также оптимальное префиксное кодирование.

**Доказательство.** 1) Очевидно, из префиксности $\varphi'$ следует префиксность $\varphi$. Допустим, что $\varphi$ не оптимально. Тогда существует префиксный код $\varphi_1$: $c(\varphi_1) < c(\varphi)$ для тех же распределений частот. Пусть

$$\varphi_1: \begin{matrix} p_1, p_2, \text{K}, p_k \\ D_1, D_2, \text{K}, D_k \end{matrix}.$$

Рассмотрим новое кодирование

$$\varphi_1': \begin{matrix} p_1, p_2, \text{K}, p_{k-1}, p', p'' \\ D_1, D_2, \text{K}, D_{k-1}, D_k 0, D_k 1 \end{matrix}.$$

По лемме 4, кодирование $\varphi_1'$ также является префиксным и

$$\begin{cases} c(\varphi') = c(\varphi) + p_k \\ c(\varphi_1') = c(\varphi_1) + p_k \end{cases} \Rightarrow$$

$$\Rightarrow \left( \left\{ c(\varphi_1) < c(\varphi) \right\} \Rightarrow c(\varphi_1') = c(\varphi_1) + p_k < c(\varphi) + p_k = c(\varphi') \right)$$

Следовательно, $\varphi'$ не является оптимальным кодированием, что противоречит условию. Остаётся предположить, что $\varphi$ оптимально.

2) Пусть $\varphi$ — оптимальное префиксное кодирование и $p_1 \geq p_2 \geq \ldots \ldots \geq p_{k-1} \geq p' \geq p''$. Допустим, что $\varphi'$ не оптимально. Тогда по лемме 3 для частот $p_1, p_2, \ldots, p_{k-1}, p', p''$ существует оптимальное префиксное кодирование $\varphi_1'$: $D_1, \ldots, D_{k-1}, D_k0, D_k1$ и $c(\varphi_1') < c(\varphi)$. Тогда для частот $p_1, p_2, \ldots, p_k$ рассмотрим кодирование $\varphi_1$: $D_1, \ldots, D_{k-1}, D_k$. Получим

$$c(\varphi_1) = c(\varphi_1') - p_k < c(\varphi') - p_k = c(\varphi) \Rightarrow c(\varphi_1) < c(\varphi)$$

и $\varphi$ не оптимально, что противоречит условию. Теорема доказана.

## §33. Коды с исправлением $r$ ошибок. Оценка функции $M_r(n)$

Будем рассматривать равномерные коды в алфавите {0, 1}, длины всех слов, равные $n$, и ошибки типа замещения, то есть изменение разрядов $0 \to 1$ и $1 \to 0$.

**Определение 1.** Код называется *исправляющим $r$ ошибок*, если при наличии в любом кодовом слове не более $r$ ошибок типа замещения можно восстановить исходное кодовое слово.

**Определение 2.** *Расстоянием Хэмминга* между 2 наборами длины $n$ называется число разрядов, в которых эти наборы различаются.

**Определение 3.** *Шаром (сферой) радиуса $r$ с центром в точке* $\alpha = (\alpha_1, \ldots, \alpha_n)$ называется множество всех наборов длины $n$, расстояние от которых до $\alpha$ не превосходит $r$ (в точности равно $r$).

**Определение 4.** Кодовым расстоянием называется расстояние по Хэммингу

$$\rho_{\min} = \min_{\alpha_i, \alpha_j \text{ из кода, } \alpha_i \neq \alpha_j} \rho(\alpha_i, \alpha_j).$$

**Утверждение 1.** Код $K = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ исправляет $r$ ошибок тогда и только тогда, когда

$$\rho_{\min}(K) \geq 2r + 1.$$

**Доказательство.** Заметим, что условие утверждения эквивалентно тому, что расстояние между центрами шаров радиуса $r$ (кодовыми словами) не меньше, чем $2r + 1$, что эквивалентно тому, что эти шары не пересекаются. Таким образом, на выходе получится слово, принадлежащее единственному однозначно определённому шару (если в слове не более $r$ ошибок), что позволяет точно восстановить слово, так как известен центр этого шара. Утверждение доказано.

**Определение 5.** Код *обнаруживает* $r$ ошибок, если при наличии в нём не более $r$ ошибок типа замещения можно сказать, были ошибки, или их не было.

**Утверждение 2.** Код $K = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ обнаруживает $r$ ошибок тогда и только тогда, когда

$$\rho_{\min}(K) \geq r + 1.$$

**Доказательство.** Условие утверждения эквивалентно тому, что ни один из центров шаров (кодовое слово) не содержится в каком-либо другом шаре, то есть если произошло не более $r$ ошибок, можно в точности установить, что полученное на выходе слово не совпадает с центром одного из шаров. Утверждение доказано.

**Определение 6.** Функция $M_r(n)$ есть *максимальное число слов длины n, образующих код, исправляющий r ошибок*. $S_r(n)$ — число точек (наборов длины $n$) в шаре радиуса $r$.

**Утверждение 3.** $S_r(n) = 1 + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{r}$.

**Доказательство.** Точки шара радиуса $r$ — это его центр, множество наборов, отличающихся от центра в одной координате — $\binom{n}{1}$, множество наборов, отличающихся от центра в 2 координатах — $\binom{n}{2}$, и т. д. Получаем утверждение.

**Теорема 5.** $\frac{2^n}{S_{2r}(n)} \le M_r(n) \le \frac{2^n}{S_r(n)}$.

**Доказательство.** Рассмотрим произвольный код $K = \{a_1, a_2, \ldots, a_m\}$, исправляющий $r$ ошибок. Из утверждения 1 следует, что шары радиуса $r$ с центрами в $a_i$ не пересекаются, следовательно, число всех точек всех шаров не превосходит числа точек $n$-мерного куба и

$$m \cdot S_r(n) \le 2^n \Leftrightarrow m \le \frac{2^n}{S_r(n)} \Rightarrow M_r(n) \le \frac{2^n}{S_r(n)}.$$

Теперь будем строить код $K = \{a_1, a_2, \ldots\}$, исправляющий $r$ ошибок. Выберем произвольно точку $a_1$. Для выбора точки $a_2$ запрещено $S_{2r}(n)$ точек, так как запрещены все точки одного шара и все точки, расположенные от любой граничной точки на расстояние, не больше, чем $r$, то есть все точки шара радиуса $2r$ с центром в точке $a_1$. Пусть уже выбраны наборы $a_1, \ldots, a_k$. Для выбора набора $a_{k+1}$ запрещено точек не больше, чем $k \cdot S_{2r}(n)$, то есть, если $k \cdot S_{2r}(n) < 2^n$, то можно выбрать $a_{k+1}$. Если тупик наступит после выбора $m$-го набора, то

$$m \cdot S_{2r}(n) \ge 2^n \Leftrightarrow m \ge \frac{2^n}{S_{2r}(n)} \Rightarrow M_r(n) \ge \frac{2^n}{S_{2r}(n)}.$$

Теорема доказана.

## §34. Коды Хэмминга. Оценка функции $M_1(n)$.

Рассмотрим коды, исправляющие одну ошибку типа замещения в словах длины $n$. Выберем натуральное $k$ таким, что

$$2^{k-1} \le n \le 2^k - 1 \Leftrightarrow \begin{cases} k \le \log_2 n + 1 \\ k \ge \log_2 (n+1) \end{cases} \Leftrightarrow k = \lfloor \log_2 n + 1 \rfloor = \lceil \log_2 (n+1) \rceil.$$

Разобьём номера всех разрядов исходного слова на $k$ классов:

$$D_i = \{m \mid m = (m_{k-1} m_{k-2} \ldots m_0)_2,\ m_i = 1\},\ 1 \le m \le n.$$

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

**Определение.** *Кодом Хэмминга* порядка $n$ называется множество наборов

$$\alpha = (\alpha_1, \alpha_2, \text{K}, \alpha_n) \in E_2^k,$$

удовлетворяющих системе уравнений (суммы по модулю 2):

$$\begin{cases} \sum_{j \in D_0} \alpha_j = 0 \\ \sum_{j \in D_1} \alpha_j = 0 \\ \text{M} \\ \sum_{j \in D_{k-1}} \alpha_j = 0 \end{cases}.$$

**Теорема 6.** Код Хэмминга порядка $n$ содержит $2^{n-k}$ наборов, где $k = \lfloor \log_2 n \rfloor + 1$ и исправляет одну ошибку.

**Доказательство.** Рассмотрим систему уравнений из определения кода Хэмминга

$$\begin{cases} \alpha_1 \oplus (\alpha_3 \oplus \text{K}) = 0 \\ \alpha_2 \oplus (\text{K}) = 0 \\ \text{M} \\ \alpha_{2^{k-1}} \oplus (\text{K}) = 0 \end{cases}.$$

Задаём произвольно $\alpha_j$, кроме $\alpha_1, \alpha_2, \alpha_4, \text{K}, \alpha_{2^{k-1}}$. Это можно сделать $2^{n-k}$ способами. Так как $\alpha_1, \alpha_2, \alpha_4, \text{K}, \alpha_{2^{k-1}}$ в скобках не встречаются, то они однозначно определяются из системы.

Пусть передано кодовое слово $\alpha = (\alpha_1 \alpha_2 \text{K}\ \alpha_n)$, ошибка произошла в $d$-ом разряде и пусть $d = (\gamma_{k-1}\gamma_{k-2}\ldots\gamma_1\gamma_0)_2$. Пусть на выходе получено слово $\beta = (\beta_1 \beta_2 \text{K}\ \beta_n)$, при этом $\beta_i = \alpha_i$ при $i \neq d$, $\beta_d = \alpha_d \oplus 1$. Обозначим

$$\delta_0 = \sum_{j \in D_0} \beta_j,$$

$$\delta_1 = \sum_{j \in D_1} \beta_j,$$

$$\text{K},$$

$$\delta_{k-1} = \sum_{j \in D_{k-1}} \beta_j.$$

**Утверждение.** $(\delta_{k-1}\delta_{k-2}\ldots\delta_1\delta_0)_2 = d$.

**Доказательство.** Пусть $\gamma_i = 0 \Rightarrow d \notin D_i$, тогда $\sum_{j\in D_i}\beta_j = \sum_{j\in D_i}\alpha_j$, следовательно, $\delta_i = 0$ и $\delta_i = \gamma_i$. Пусть теперь $\gamma_i = 1$ и $d \in D_i$. Тогда $\sum_{j\in D_i}\beta_i = \sum_{j\in D_i}\alpha_i \oplus 1 = 1 \Rightarrow \delta_i = 1 \Rightarrow \delta_i = \gamma_i$.

Утверждение доказано.

Таким образом, по выходному слову можно определить номер искаженного разряда и восстановить исходное слово.

Теорема доказана.

**Замечание.** Обычно разряды с номерами 1, 2, 4, 8, …, $2^{k-1}$ называют *проверочными* (или *контрольными*), остальные — *информационными*.

**Теорема 7.** $\dfrac{2^n}{2n} \le M_1(n) \le \dfrac{2^n}{n+1}$.

**Доказательство.** Имеем $\dfrac{2^n}{S_{2r}(n)} \le M_r(n) \le \dfrac{2^n}{S_r(n)}$ (теорема 5). Правое неравенство в теореме 7 следует из того, что $S_1(n) = n + 1$. Заметим предварительно, что аналогично нельзя получить и левое неравенство, так как

$$S_2(n) = 1 + n + \binom{n}{2} = 1 + n + \frac{n(n-1)}{2} \sim \frac{n^2}{2}.$$

По теореме 6 всего различных слов в коде Хэмминга, исправляющем одну ошибку — $m = 2^{n-k}$. Поскольку $k = \lfloor \log_2 n \rfloor + 1$, имеем

$$k \le \log_2 n + 1 \Rightarrow m \ge 2^{n-\log_2 n - 1} = \frac{2^n}{2n} \Rightarrow M_1(n) \ge m \ge \frac{2^n}{2n}.$$

Теорема доказана.

# Глава V. Основы теории конечных автоматов

## §35. Понятие ограниченно детерминированных (автоматных) функций, их представление диаграммой Мура. Единичная задержка

Пусть даны $A = \{a_1, a_2, \ldots, a_r\}$ — входной алфавит и $B = \{b_1, b_2, \ldots, b_m\}$ — выходной алфавит. Определим множества $A^\infty$ и $B^\infty$ как множества всевозможных последовательностей в алфавитах $A$ и $B$ соответственно.

**Определение 1.** Отображение $\varphi: A^\infty \to B^\infty$ называется *детерминированной функцией (д.-функцией)*, если $b(t)$ для любого $t = 1, 2, \ldots$ однозначно определяется по $a(1), a(2), \ldots, a(t)$. Обозначать д.-функции будем так: $\varphi: \begin{matrix} a_1(1)\text{K}\ a_1(t)\text{K} \to b_1(1)\text{K}\ b_1(t)\text{K} \\ a_2(1)\text{K}\ a_2(t)\text{K} \to b_2(1)\text{K}\ b_2(t)\text{K} \end{matrix}$, причём,

если $a_1(1) = a_2(1)$, то $b_1(1) = b_2(1)$;

если $\begin{cases} a_1(1) = a_2(1) \\ a_1(2) = a_2(2) \\ \text{M} \\ a_1(t) = a_2(t) \end{cases}$, то $b_1(t) = b_2(t)$.

**Определение 2.** Пусть задана д.-функция $\varphi: A^\infty \to B^\infty$. Рассмотрим произвольное слово $\overline{a} = a_1 a_2 \text{K}\ a_k \in A^*$. Определим функцию $\varphi_{\overline{a}}$ следующим образом: пусть $a(1), a(2), \ldots, a(t)\ldots$ — произвольная входная последовательность. Рассмотрим

$$\varphi(a_1 a_2 \ldots a_k a(1) a(2) \ldots a(t)\ldots) = b_1 b_2 \ldots b_k b(1) b(2) \ldots b(t)\ldots.$$

Тогда положим $\varphi_{\overline{a}}\big(a(1)a(2)\text{K}\ a(t)\text{K}\big) = b(1)b(2)\text{K}\ b(t)\text{K}$ . $\varphi_{\overline{a}}$ при этом называется *остаточной функцией для* $\varphi$ по слову $\overline{a} \in A^*$.

**Определение 3.** Детерминированная функция $\varphi: A^\infty \to B^\infty$ называется *ограниченно детерминированной*, если у неё имеется лишь конечное число различных остаточных функций.

**Определение 4.** *Автоматом (инициальным)* называется любая шестёрка ($A$, $B$, $Q$, $G$, $F$, $q_0$), где $A$, $B$, $Q$ — конечные алфавиты ($A$ называют входным алфавитом, $B$ — выходным алфавитом, $Q$ — множеством состояний), $G$: $A \times Q \to Q$, $F$: $A \times Q \to B$, $q_0 \in Q$ — начальное состояние.

Входом автомата служит последовательность $a(1)a(2)a(3)\ldots a(t)\ldots \in A^*$ (конечная или бесконечная), выходом автомата служит последовательность $z(t)$, при этом автомат задаётся системой канонических уравнений

$$\begin{cases} z(t) = F\big(x(t), q(t-1)\big), \\ q(t) = G\big(x(t), q(t-1)\big), \\ q(0) = q_0. \end{cases}$$

**Определение 5.** Отображение $\varphi$: $A^\infty \to B^\infty$ называется *автоматной функцией*, если существует автомат, который реализует это отображение.

**Утверждение.** Функция является автоматной тогда и только тогда, когда она является ограниченно детерминированной.

**Пример.** Пусть $A = B = Q = \{0, 1\}$ и система канонических уравнений выглядит следующим образом:

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

Такой автомат, очевидно, осуществляет отображение $a(1)a(2)\ldots \to 0a(1)a(2)\ldots$ и называется *единичной задержкой*.

| | | | | |
|---|---|---|---|---|
| $x(t)$ | | $a(1)$ | $a(2)$ | $a(3)$ |
| $q(t)$ | 0 | $a(1)$ | $a(2)$ | $a(3)$ |
| $z(t)$ | | 0 | $a(1)$ | $a(2)$ |

**Определение 6.** *Диаграммой Мура* для автомата называется ориентированный граф с множеством вершин $Q$, у которого каждой паре $(a, q)$ сопоставляется дуга, идущая из вершины $q$ в вершину, соответствующую $G(a, q)$. Этой дуге приписывается пометка $(a, F(a, q))$. Особым образом помечена вершина, соответствующая начальному состоянию. Диаграмма Мура однозначно задаёт автомат.

## §36. Схемы из функциональных элементов и элементов задержки. Автоматность осуществляемых ими отображений

**Определение.** *Схемой из функциональных элементов и элемента задержки* называется схема из функциональных элементов в функциональном базисе, к которому добавлен элемент, реализующий функцию единичной задержки. В схеме из функциональных элементов и элементов задержки допускаются ориентированные циклы, но любой ориентированный цикл должен проходить хотя бы через одну задержку.

Пусть $A = B = \{0, 1\}$, $E_2^n$ — множество всех булевых векторов длины $n$.

**Теорема 1.** Схема из функциональных элементов и задержки осуществляет автоматное отображение.

**Доказательство.** 1) Пусть в схеме имеется $r$ элементов задержки. Пусть $i$-я задержка $R_i$ приписана вершине $v_i$, в которую идёт дуга из вершины $w_i$. Для всех $i = 1, \ldots, r$ удалим из СФЭЗ дуги $(w_i, v_i)$. По определению СФЭЗ в полученном после этого графе не будет ориентированных циклов и он, тем самым будет представлять собой СФЭ. Входами этой СФЭ будут все входы исходной схемы, а также все вершины $v_i$, $i = 1, \ldots, r$ (заметим, что все они различны и отличны от входов исходной схемы). Выходами полученной СФЭ объявим все выходы исходной схемы и вершины $w_i$, $i = 1, \ldots, r$. Пусть в исходной схеме выходам приписаны переменные $z_1, \ldots, z_m$, входам — переменные $x_1, \ldots, x_n$. Вершинам $v_i$ припишем переменные $q'_1, \ldots, q'_r$, а вершинам $w_i$ — переменные $q_1, \ldots, q_r$. В соответствии с определением функционирования СФЭ, для некоторых функций алгебры логики $f_i$, $g_j$ справедливо:

$$\begin{cases} z_i = f_i\left(x_1,\text{K},x_n,q'_1,\text{K},q'_r\right), \ \ i=1,\text{K},m, \\ q_j = g_j\left(x_1,\text{K},x_n,q'_1,\text{K},q'_r\right), \ \ j=1,\text{K},r. \end{cases} \tag{1}$$

Естественно считать, что равенства (1) выполняются в каждый момент времени $t = 1, 2, 3, \ldots$, то есть

$$\begin{cases} z_i(t) = f_i\left(x_1(t),\text{K},x_n(t),q'_1(t),\text{K},q'_r(t)\right), \ \ i=1,\text{K}\ m, \\ q_j(t) = g_j\left(x_1(t),\text{K},x_n(t),q'_1(t),\text{K},q'_r(t)\right), \ \ j=1,\text{K},r. \end{cases} \tag{2}$$

Так как, в соответствии с каноническими уравнениями элемента единичной задержки его выход в момент $t$ совпадает с его входом в момент $t-1$, то естественно считать, что в исходной схеме $q'_i(t) = q_i(t-1)$ при $t = 1, 2, \ldots$ для всех $i = 1, \ldots, r$, где $q_i(0) = 0$. Тогда равенства (2) принимают вид (где $i = 1, \ldots, m$ и $j = 1, \ldots, r$):

$$\begin{cases} z_i(t) = f_i\left(x_1(t), \text{K}, x_n(t), q_1(t-1), \text{K}, q_r(t-1)\right), \\ q_j(t) = g_j\left(x_1(t), \text{K}, x_n(t), q_1(t-1), \text{K}, q_r(t-1)\right), \\ q_j(0) = 0. \end{cases} \qquad (3)$$

Полученные равенства определяют функционирование СФЭЗ и называются её каноническими уравнениями.

2) Пусть отображение $\psi$, осуществляемое схемой $\Sigma$, задаётся каноническими уравнениями (3). Введём переменные $X = (x_1, \ldots, x_n)$, $Q = (q_1, \ldots, q_r)$, $Z = (z_1, \ldots, z_m)$, принимающие значения, соответственно в $E_2^n$, $E_2^r$, $E_2^m$. Положим $q_0 = (0, \ldots, 0)$. Тогда (3) можно переписать в виде

$$\begin{cases} Z(t) = F\left(X(t), Q(t-1)\right), \\ Q(t) = G\left(X(t), Q(t-1)\right), \\ Q(0) = q_0, \end{cases}$$

где функции $F$, $G$ не зависят явно от $t$. Отсюда видно, что отображение, осуществляемое схемой, совпадает с отображением, задаваемым автоматом $\left(E_2^n, E_2^m, E_2^r, G, F, q_0\right)$, то есть является автоматной функцией. Теорема доказана.

## §37. Моделирование автоматной функции схемой из функциональных элементов и элементов задержки

**Определение.** Пусть автоматная функция $\varphi$ отображает последовательности в конечном алфавите $A$ в последовательности в конечном алфавите $B$. Пусть СФЭЗ $\Sigma$ осуществляет преобразование $\psi$ последовательностей с элементами из $E_2^n$ в последовательности с элементами из $E_2^m$. Будем говорить, что $\Sigma$ *моделирует* $\varphi$, если существуют отображе-

ния (кодирования) $K_1 : A \to E_2^n$ и $K_2 : B \to E_2^m$, сопоставляющие разным элементам разные элементы и обладающие свойством: для любой последовательности $P = a(1)a(2)\ldots a(t)$ в алфавите $A$, если

$$\varphi(P) = T = b(1)b(2)\ldots b(t), \text{ то } \psi(K_1(P)) = K_2(T),$$
$$\text{где } K_1(P) = K_1(a(1))K_1(a(2))\ldots K_1(a(t)),$$
$$K_2(T) = K_2(b(1))K_2(b(2))\ldots K_2(b(t)).$$

**Теорема 2.** Для любой автоматной функции существует моделирующая её СФЭЗ в базисе из функциональных элементов дизъюнкции, конъюнкции, отрицания и элемента задержки.

**Доказательство.** Пусть автоматная функция дана автоматом $D = (A, B, Q, G, F, q_0)$. Выберем $n, m, r$ так, что $2^n \geq |A|$, $2^m \geq |B|$, $2^r \geq |Q|$. Рассмотрим произвольные отображения (кодирования) $K_1 : A \to E_2^n$, $K_2 : B \to E_2^m$, $K_3 : Q \to E_2^r$, при которых разные элементы отображаются в разные элементы. Дополнительно потребуем, чтобы $K_3(q_0) = (0, \ldots, 0)$. Рассмотрим отображения $G' : E_2^n \times E_2^r \to E_2^r$ и $F' : E_2^n \times E_2^r \to E_2^m$ такие, что для любых $a \in A$ и $q \in Q$ выполняется

$$\begin{cases} G'\left(K_1(a), K_3(q)\right) = K_3\left(G(a,q)\right), \\ F'\left(K_1(a), K_3(q)\right) = K_2\left(F(a,q)\right). \end{cases} \qquad (1)$$

Равенства (1) определяют отображения $G'$ и $F'$ только для пар $\alpha \in E_2^n$, $\beta \in E_2^r$ таких, что $\alpha$ является кодом некоторой буквы из $A$, а $\beta$ является кодом некоторой буквы из $B$. Для остальных пар отображения $G'$ и $F'$ доопределим произвольно. Пусть $\theta = (0, \ldots, 0)$. Рассмотрим автомат $H = \left(E_2^n, E_2^m, E_2^r, G', F', \theta\right)$ с каноническими уравнениями

$$\begin{cases} Z(t) = F'\left(X(t), Q(t-1)\right), \\ Q(t) = G'\left(X(t), Q(t-1)\right), \\ \qquad Q(0) = \theta. \end{cases} \qquad (2)$$

Из (1) вытекает, что если автомат $D$ преобразует последовательность $P$ в алфавите $A$ в последовательность $T$ в алфавите $B$, то $H$ преобразует код $K_1(P)$ последовательности $P$ в код $K_2(T)$ последовательности $T$. Таким образом, достаточно показать, что автоматную функцию, за-

даваемую равенствами (2), можно реализовать схемой. Так как значением переменной $X$ являются наборы длины $n$ из $E_2^n$, то её можно рассматривать как набор переменных ($x_1$, …, $x_n$), принимающих значения из $E_2$. Аналогично для переменных $Q$ и $Z$. Тогда (2) можно переписать в эквивалентном виде для некоторых функций алгебры логики $f_i$, $g_j$:

$$\begin{cases} z_i(t) = f_i\left(x_1(t),\text{K},x_n(t),q_1'(t),\text{K},q_r'(t)\right), \ i=1,\text{K},m, \\ q_j(t) = g_j\left(x_1(t),\text{K},x_n(t),q_1'(t),\text{K},q_r'(t)\right), \ j=1,\text{K},r. \end{cases}$$

Тогда можно построить схему из функциональных элементов в базисе $\{\vee,\&,\bar{}\}$ с $n + r$ входами и $m + r$ выходами, реализующую семейство функций

$$\begin{cases} z_i = f_i\left(x_1,\text{K},x_n,q_1',\text{K},q_r'\right), \ i=1,\text{K},m, \\ q_j = g_j\left(x_1,\text{K},x_n,q_1',\text{K},q_r'\right), \ j=1,\text{K},r. \end{cases}$$

Пусть в этой СФЭ входная переменная $q_j'$ приписана вершине $v_j$, а выходная переменная $q_j$ — вершине $w_j$. Добавим дугу ($w_j$, $v_j$) и сопоставим вершине $v_j$ элемент задержки. Проделав это для всех пар $q_j, q_j' \ \ (j=1,\text{K},r)$, получим СФЭЗ, функционирование которой описывается каноническими уравнениями

$$\begin{cases} z_i(t) = f_i\left(x_1(t),\text{K},x_n(t),q_1(t-1),\text{K},q_r(t-1)\right), \ i=1,\text{K},m, \\ q_j(t) = g_j\left(x_1(t),\text{K},x_n(t),q_1(t-1),\text{K},q_r(t-1)\right), \ j=1,\text{K},r, \\ q_j(0) = 0. \end{cases}$$

Эта схема является искомой. Теорема доказана.

## §38. Теорема Мура. Теорема об отличимости состояний двух автоматов

Будем рассматривать автоматы, в которых не выделено начальное состояние, то есть автомат задаётся пятёркой ($A$, $B$, $Q$, $G$, $F$).

Через $A^*$ будем обозначать множество всех конечных слов в алфавите $A$. Расширим функции $F$ и $G$, определив $F(\bar{a},q_i)$ и $G(\bar{a},q_i)$ для любого состояния $q_i \in Q$ и любого слова $\bar{a} = \left(a(1),a(2),\text{K},a(m)\right) \in A^*$.

Пусть автомат (*A, B, Q, G, F*) находится в состоянии $q_i \in Q$ и на вход подаётся слово $\bar{a} = (a(1), a(2), \text{К}, a(m))$. Тогда на выходе будет последовательно выдаваться некоторое слово $\bar{b} = (b(1), b(2), \text{К}, b(m))$ и после подачи всего слова $\bar{a}$ автомат окажется в некотором состоянии $q_k$. Расширим функции *F* и *G*, положив $F(\bar{a}, q_i) = \bar{b}$, $G(\bar{a}, q_i) = q_k$.

**Определение 1.** Два состояния $q_i$ и $q_j$ автомата (*A, B, Q, G, F*) называются *отличимыми*, если существует входное слово $\bar{a} \in A^*$ такое, что $F(\bar{a}, q_i) \neq F(\bar{a}, q_j)$. При этом слово $\bar{a}$ называют *экспериментом*, отличающим $q_i$ и $q_j$, а длину $l(\bar{a})$ — длиной этого эксперимента.

**Лемма.** Пусть в автомате (*A, B, Q, G, F*) есть 2 состояния $q_u$ и $q_v$, отличимые экспериментом длины *p* и не отличимые более коротким экспериментом. Тогда для любого *k*, где $1 \le k \le p$, существуют 2 состояния, отличимые экспериментом длины *k* и не отличимые более коротким экспериментом.

**Доказательство.** Пусть состояния $q_u$, $q_v$ отличимы экспериментом $\bar{a}$ длины *p* и не отличимы экспериментом меньшей длины. Пусть $F(\bar{a}, q_u) = \bar{b}$, $F(\bar{a}, q_v) = \bar{c}$. Тогда $\bar{b} \neq \bar{c}$, причём $\bar{b}$ и $\bar{c}$ различаются только последней буквой. Разобьём все слова $\bar{a}$, $\bar{b}$, $\bar{c}$ на 2 подслова $\bar{a} = \bar{a}_1\bar{a}_2$, $\bar{b} = \bar{b}_1\bar{b}_2$, $\bar{c} = \bar{c}_1\bar{c}_2$, где $l(\bar{a}_2) = l(\bar{b}_2) = l(\bar{c}_2) = k$. Пусть $G(\bar{a}_1, q_u) = q'$, $G(\bar{a}_1, q_v) = q''$. Тогда $F(\bar{a}_2, q') = \bar{b}_2$, $F(\bar{a}_2, q'') = \bar{c}_2$. Так как $\bar{b}_2$ и $\bar{c}_2$ различаются последней буквой, то $q'$ и $q''$ отличимы экспериментом длины $l(\bar{a}_2) = k$. Допустим, что $q'$ и $q''$ отличимы экспериментом $\bar{a}_3$ длины $l(\bar{a}_3) < k$. Тогда $F(\bar{a}_3, q') = \bar{b}_3$, $F(\bar{a}_3, q'') = \bar{c}_3$ и $\bar{b}_3 \neq \bar{c}_3$. Но тогда $F(\bar{a}_1\bar{a}_3, q_u) = \bar{b}_1\bar{b}_3$, $F(\bar{a}_1\bar{a}_3, q_v) = \bar{c}_1\bar{c}_3$ и $\bar{b}_1\bar{b}_3 \neq \bar{c}_1\bar{c}_3$. Следовательно, $q_u$ и $q_v$ отличимы экспериментом $\bar{a}_1\bar{a}_3$ длины $l(\bar{a}_1\bar{a}_3) = l(\bar{a}_1) + l(\bar{a}_3) < (p-k) + k = p$. Это противоречит условию. Значит (от противного), $q'$ и $q''$ не отличимы экспериментом длины меньшей, чем *k*. Лемма доказана.

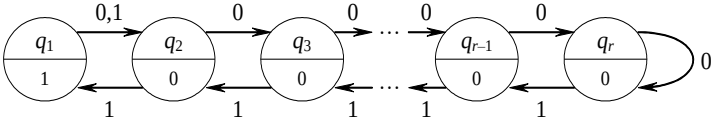
**Теорема 3 (Теорема Мура).** Если в автомате ($A$, $B$, $Q$, $G$, $F$) состояния $q_i$ и $q_j$ отличимы и $|Q| = r$, то существует эксперимент $\bar{a}$, отличающий $q_i$ и $q_j$, длины $l(\bar{a}) \le r-1$.

**Доказательство.** Пусть состояния $q_i$ и $q_j$ отличимы экспериментом длины $p$ и не отличимы более коротким экспериментом. Рассмотрим в данном автомате следующее отношение $R_m$ на множестве состояний $Q$ ($m$ = 0, 1, …, $p$): состояния $q_i$ и $q_j$ не отличимы экспериментом длины $m$ (считаем, что любые 2 состояния не отличимы экспериментом длины 0). Если для любого слова $\bar{a} \in A^*$ длины $m$ $F(\bar{a}, q_i) = F(\bar{a}, q_j)$ и $F(\bar{a}, q_j) = F(\bar{a}, q_k)$, то $F(\bar{a}, q_i) = F(\bar{a}, q_k)$, поэтому $R_m$ — это отношение эквивалентности для каждого $m$ = 0, 1, …, $p$. Относительно $R_m$ $Q$ разбивается на классы эквивалентности $Q_1^{(m)}, Q_2^{(m)}, \text{K}, Q_{s(m)}^{(m)}$, так что любые два состояния из одного класса не отличимы экспериментом длины $m$, а любые два состояния из разных классов отличимы экспериментом длины $m$. При этом $s(0) = 1$ и $Q = Q_1^{(0)}$. Посмотрим, как меняются эти классы при переходе от $m$ к $m + 1$. Если 2 состояния отличимы экспериментом длины $m$, то они отличимы и экспериментом длины $m + 1$, поэтому состояния из разных классов остаются в разных классах. По лемме для любого $m$ = 0, 1, …, $p - 1$ существуют 2 состояния, отличимые экспериментом длины $m + 1$ и не отличимые экспериментом длины $m$. Следовательно, хотя бы один из классов эквивалентности относительно $R_m$ распадается не менее чем на 2 класса эквивалентности относительно $R_{m+1}$. Отсюда

$$1 = s(0) < s(1) < s(2) < \ldots < s(p-1) < s(p) \le r.$$

Так как все $s(i)$ — натуральные числа, то $p \le r - 1$. Теорема доказана.

Следующий пример автомата показывает, что оценку $r - 1$ в теореме Мура в общем случае улучшить нельзя. Здесь, независимо от входного символа $a$ $F(a, q_i) = 0$, для $i$ = 2, 3, …, $r$ и $F(a, q_1) = 1$.



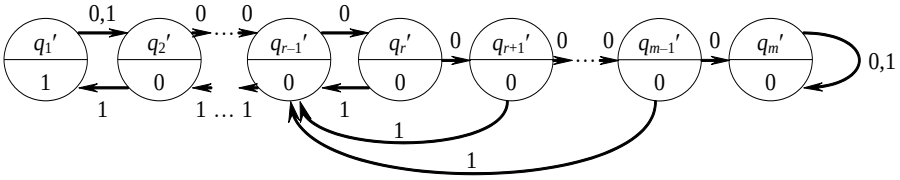
Для того, чтобы отличить состояния $q_{r-1}$ и $q_r$ надо перевести хотя бы одно из них в $q_1$ (входным словом длины $r-2$) и затем подать ещё один входной символ. Следовательно, минимальная длина эксперимента, отличающего $q_{r-1}$ и $q_r$, равна $r-1$.

**Определение 2.** Пусть 2 автомата $(A, B, Q_1, G_1, F_1)$ и $(A, B, Q_2, G_2, F_2)$ имеют одинаковые входной и выходной алфавиты. Пусть $q_i \in Q_1$ и $q_j \in Q_2$. Будем говорить, что эксперимент $\bar{a} \in A^*$ *отличает* состояния $q_i$ и $q_j$, если $F_1(\bar{a}, q_i) \neq F_2(\bar{a}, q_j)$.

**Теорема 4.** Пусть даны 2 автомата $(A, B, Q_1, G_1, F_1)$ и $(A, B, Q_2, G_2, F_2)$. Пусть $|Q_1| = r$, $|Q_2| = m$ и $q_i \in Q_1$, $q_j \in Q_2$. Тогда, если $q_i$ и $q_j$ отличимы, то существует отличающий их эксперимент $\bar{a}$ длины $l(\bar{a}) \le r+m-1$.

**Доказательство.** Можно считать, что $Q_1 \cap Q_2 = \varnothing$. Рассмотрим автомат $(A, B, Q, G, F)$, в котором $Q = Q_1 \cup Q_2$ и диаграмма которого получается объединением диаграмм исходных автоматов. Тогда $|Q| = r + m$ и по теореме Мура $q_i$, $q_j$ отличимы экспериментом $\bar{a}$ длины $l(\bar{a}) \le r+m-1$. Теорема доказана.

Следующий пример автомата показывает, что оценка $r + m - 1$ в общем случае не улучшаема. Здесь предполагается $m \ge r$ и опять выходной символ зависит только от текущего состояния и не зависит от входного символа.




Легко видеть, что если не использовать состояние $q_m'$ второго автомата, то нельзя отличить состояния $q_1$ и $q_1'$. Поэтому для того, чтобы отличить $q_1$ и $q_1'$ сначала надо перевести второй автомат словом $\bar{a}$ из $q_1'$ в $q_m'$. При этом $l(\bar{a}_1) \ge m-1$ и первый автомат под действием $\bar{a}$ перейдёт из $q_1$ в $q_r$. Чтобы далее получить различные выходные последовательности, надо перевести первый автомат из $q_r$ в $q_1$ и подать ещё один символ. Всего для того, чтобы отличить $q_1$ от $q_1'$ потребуется входное слово длины $(m-1)+(r-1)+1 = m+r-1$.