

# Содержание

<b>1</b>	<b>Часть А.</b>	<b>4</b>
1.1	Функции алгебры логики. Полиномы Жегалкина. Быстрый алгоритм построения полинома Жегалкина функции алгебры логики (с обоснованием).	4
1.2	Функции алгебры логики. Двойственность. Самодвойственные функции. Замкнутость класса самодвойственных функций. . . . .	7
1.3	Функции алгебры логики. Монотонные функции. Замкнутость класса монотонных функций. . . . .	8
1.4	Функции алгебры логики. Линейные функции. Лемма о нелинейной функции. . . . .	8
1.5	Функции алгебры логики. Полнота. Теорема Поста о полноте системы функций алгебры логики. . . . .	9
1.6	Функции алгебры логики. Предполные классы. Теорема о предполных классах. . . . .	10
1.7	Деревья. Теорема о равносильных определениях дерева. . . . .	11
1.8	Остовные деревья. Алгоритм построения кратчайшего остовного дерева в связном графе (с обоснованием). . . . .	12
1.9	todo Раскраски вершин графов. Теорема о раскраске вершин планарных графов в 5 цветов. . . . .	13
1.10	todo Алфавитные коды. Однозначность (разделимость) алфавитного кода. Алгоритм Маркова распознавания однозначности алфавитного кода (с обоснованием). . . . .	13
1.11	todo Алфавитные коды. Теорема Маркова об алфавитных кодах. . . . .	13
1.12	todo Алфавитные коды. Неравенство Макмиллана. . . . .	14
1.13	todo Алфавитные коды. Префиксные коды. Существование префиксного кода с заданными длинами кодовых слов. . . . .	14
1.14	todo Коды с минимальной избыточностью (оптимальные коды). Теорема редукции. . . . .	14
1.15	todo Коды, обнаруживающие и исправляющие ошибки. Критерии кодов, обнаруживающих и исправляющих $t$ ошибок замещения. Функция $M_t(n)$ , ее оценки. . . . .	14
1.16	todo Коды, исправляющие одну ошибку. Коды Хэмминга. Оценка функции $M_1(n)$ . . . . .	14
1.17	todo Схемы из функциональных элементов и элементов задержки (СФ-ЭЗ). Автоматность осуществляемых ими отображений. . . . .	14
1.18	todo Схемы из функциональных элементов и элементов задержки (СФ-ЭЗ). Моделирование автоматной функции схемой из функциональных элементов и элементов задержки. . . . .	14
1.19	todo Конечные автоматы. Отличимость состояний конечного автомата. Теорема Мура. Достижимость оценки теоремы Мура. . . . .	15

1.20	todo Схемы из функциональных элементов. Сумматор, верхняя оценка его сложности. . . . .	15
1.21	todo Схемы из функциональных элементов. Вычитатель, верхняя оценка его сложности. . . . .	15
1.22	todo Схемы из функциональных элементов (СФЭ). Умножитель. Метод Карацубы построения умножителя, верхняя оценка его сложности. . . .	15
<b>2</b>	<b>Часть Б.</b>	<b>15</b>
2.1	Функции алгебры логики. Существенность переменных. Формулы. Тождества. . . . .	15
2.2	Функции алгебры логики. Теорема о разложении функции алгебры логики по переменным. Теорема о совершенной дизъюнктивной нормальной форме (ДНФ). Теорема о совершенной конъюнктивной нормальной форме (КНФ). . . . .	16
2.3	Функции алгебры логики. Полные системы. Примеры полных систем (с доказательством полноты). . . . .	18
2.4	Функции алгебры логики. Теорема Жегалкина о выразимости функции алгебры логики полиномом Жегалкина. . . . .	19
2.5	Функции алгебры логики. Замыкание, замкнутый класс. Функции, сохраняющие константу, и линейные функции. Замкнутость классов функций, сохраняющих константу, и линейных функций. . . . .	20
2.6	Функции алгебры логики. Самодвойственные функции. Лемма о несамодвойственной функции. . . . .	22
2.7	Функции алгебры логики. Монотонные функции. Лемма о немонотонной функции. . . . .	22
2.8	Функции алгебры логики. Базис. Теорема о числе функций в базисе в алгебре логики. . . . .	23
2.9	Графы. Изоморфизм графов. Связность. Формула Эйлера для степеней вершин. Теорема о соотношении между числом вершин, ребер и компонент связности в графе. . . . .	24
2.10	Деревья. Корневые деревья, упорядоченные корневые деревья. Верхняя оценка числа деревьев с заданным числом ребер. . . . .	25
2.11	Геометрическое представление графов. Теорема о геометрическом представлении графов в трехмерном пространстве. . . . .	26
2.12	Планарные графы. Формула Эйлера для планарных графов. Верхняя оценка числа ребер в планарном графе. . . . .	26
2.13	todo Графы $K_5$ и $K_{3,3}$ . Непланарность графов $K_5$ и $K_{3,3}$ . Теорема Понтрягина-Куратовского (доказательство в одну сторону). . . . .	27
2.14	todo Раскраски вершин графов. Теорема о раскраске вершин графа в 2 цвета (теорема Кенига). . . . .	27
2.15	todo Коды с минимальной избыточностью (оптимальные коды). Три леммы о свойствах кодов с минимальной избыточностью. . . . .	28

2.16	todo Коды с минимальной избыточностью (оптимальные коды). Алгоритм Хаффмена построения кода с минимальной избыточностью. . . . .	28
2.17	todo Коды, исправляющие одну ошибку. Алгоритмы кодирования, исправления ошибки и декодирования в коде Хэмминга. . . . .	28
2.18	todo Линейные двоичные коды. Теорема о кодовом расстоянии линейных кодов. . . . .	28
2.19	todo Конечные автоматы. Функционирование конечного автомата. Автоматные функции. Канонические уравнения и диаграмма Мура конечного автомата. Единичная задержка, ее автоматность. . . . .	28
2.20	todo Схемы из функциональных элементов. Выразимость функции алгебры логики схемой из функциональных элементов в базисе из конъюнкции, дизъюнкции и отрицания. . . . .	28

# 1 Часть А.

## 1.1 Функции алгебры логики. Полиномы Жегалкина. Быстрый алгоритм построения полинома Жегалкина функции алгебры логики (с обоснованием).

**Опр.** Пусть  $E_2 = \{0, 1\}$ . Функцией алгебры логики называется произвольное отображение из  $E_2^n$  в  $E_2$ ,  $n \geq 1$ . Множество всех функций алгебры логики, зависящих от  $n$  переменных, обозначит  $P_2^{(n)}$ , а множество всех функций алгебры логики —  $P_2 = \bigcup_{n \geq 1} P_2^{(n)}$ .

**Опр.** Элементарная конъюнкция, не содержащая отрицаний переменных, называется монотонной ЭК, или мономом, или одночленом.

**Опр.** Полиномом Жегалкина длины  $l$ ,  $l \geq 1$ , назовем сумму по модулю два  $l$  различных монотонных ЭК. Полиномом Жегалкина длины 0 назовем константу 0.

**Теорема.** Каждая функция  $f(x_1, \dots, x_n) \in P_2$  может быть единственным образом представлена в виде полинома Жегалкина  $P_f$ .

*Д-во. Существование.* Применим полиномиальное разложение функции  $f(x_1, \dots, x_n)$  по всем  $n$  переменным:

$$f(x_1, \dots, x_n) = \bigoplus_{\sigma \in E_2^n} x_1^{\sigma_1} \cdot \dots \cdot x_n^{\sigma_n} \cdot f(\sigma).$$

Затем пользуясь тождеством  $x^\sigma = x \oplus \sigma \oplus 1$  везде в правой части заменим выражение  $x_i^{\sigma_i}$  на выражение  $x_i \oplus \sigma_i \oplus 1$ . Далее по правилам коммутативности и ассоциативности  $\&$  и  $\oplus$  и дистрибутивности вида  $x \cdot (y \oplus z) = x \cdot y \oplus x \cdot z$  перемножим все скобки. После этого приведем подобные слагаемые по правилам  $x \oplus x = x$ ,  $x \oplus 0 = x$ . В итоге получим полином Жегалкина, который представляет исходную функцию  $f$ .

*Единственность.* Покажем, что число полиномов Жегалкина над переменными  $x_1, \dots, x_n$  совпадает с числом функций из  $P_2^{(n)}$ . Монотонных элементарных конъюнкций над переменными  $x_1, \dots, x_n$  всего найдется  $2^n$ , т.к. каждая переменная  $x_i$ ,  $i = \overline{1, n}$ , может либо входить, либо не входить в такую монотонную ЭК. Далее, полиномов Жегалкина над переменными  $x_1, \dots, x_n$  всего найдется  $2^{2^n}$ , т.к. каждая из  $2^n$  монотонных ЭК может либо входить, либо не входить в такой полином Жегалкина. Значит, учитывая то, что каждая функция  $f$  из  $P_2^{(n)}$  может быть представлена в виде полинома Жегалкина, это представление единственно.  $\square$

Набору  $\alpha \in E_2^n$ ,  $n \geq 2$ , взаимно однозначно сопоставим монотонную ЭК над переменными  $x_1, \dots, x_n$ :

$$x^\alpha = \begin{cases} 1 & , \alpha = (0, \dots, 0) \\ \prod_{\alpha_i=1} x_i & , \alpha \neq (0, \dots, 0) \end{cases}.$$

Если  $\alpha$  пробегает по всем возможным наборам из  $E_2^n$ , то  $x^\alpha$  перечисляет все возможные монотонные ЭК над  $x_1, \dots, x_n$ .

Пусть  $c_f(\alpha)$  обозначает коэффициент при мономе  $x^\alpha$ ,  $\alpha \in E_2^n$ , в полиноме Жегалкина функции  $f \in P_2^{(n)}$ . Тогда

$$f(x_1, \dots, x_n) = \bigoplus_{\alpha \in E_2^n} c_f(\alpha) \cdot x^\alpha.$$

Для нахождения полинома Жегалкина функции  $f$  нужно найти коэффициенты  $c_f(\alpha)$  для всех  $\alpha \in E_2^n$ .

### Вычисление коэффициентов при $n = 1$ .

Если  $f(x) \in P_2^{(1)}$ , то

$$\begin{aligned} f(x) &= \bar{x} \cdot f(0) \oplus x \cdot f(1) = (x \oplus 1) \cdot f(0) \oplus x \cdot f(1) = \\ &= x \cdot f(0) \oplus f(0) \oplus x \cdot f(1) = (f(0) \oplus f(1)) \cdot x \oplus f(0). \end{aligned}$$

Поэтому  $c_f(0) = f(0)$ ,  $c_f(1) = f(0) \oplus f(1)$ .

**Теорема.** Если  $n \geq 1$ ,  $f(y, x_1, \dots, x_n) \in P_2^{(n+1)}$ ,  $f_a(x_1, \dots, x_n) = f(a, x_1, \dots, x_n)$ , где  $a \in E_2$ , то для каждого  $\alpha \in E_2^n$  верны равенства:

$$\begin{aligned} c_f(0, \alpha_1, \dots, \alpha_n) &= c_{f_0}(\alpha), \\ c_f(1, \alpha_1, \dots, \alpha_n) &= c_{f_0}(\alpha) \oplus c_{f_1}(\alpha). \end{aligned}$$

*Д-во.* Применим полиномиальное разложение функции  $f(y, x_1, \dots, x_n)$  по переменной  $y$ :

$$\begin{aligned} f(y, x_1, \dots, x_n) &= \bar{y} \cdot f(0, x_1, \dots, x_n) \oplus y \cdot f(1, x_1, \dots, x_n) = \\ &= \bar{y} \cdot f_0 \oplus y \cdot f_1 = (y \oplus 1) \cdot f_0 \oplus y \cdot f_1 = \\ &= y \cdot f_0 \oplus f_0 \oplus y \cdot f_1 = y(f_0 \oplus f_1) \oplus f_0. \end{aligned}$$

Но

$$\begin{aligned} f_0 &= \bigoplus_{\alpha \in E_2^n} c_{f_0}(\alpha) \cdot x^\alpha, \\ f_1 &= \bigoplus_{\alpha \in E_2^n} c_{f_1}(\alpha) \cdot x^\alpha. \end{aligned}$$

Поэтому:

$$f = y \cdot \left( \bigoplus_{\alpha \in E_2^n} c_{f_0}(\alpha) \cdot x^\alpha \oplus \bigoplus_{\alpha \in E_2^n} c_{f_1}(\alpha) \cdot x^\alpha \right) \oplus \bigoplus_{\alpha \in E_2^n} c_{f_0}(\alpha) \cdot x^\alpha.$$

Значит,

$$f = \bigoplus_{\alpha \in E_2^n} (c_{f_0}(\alpha) \oplus c_{f_1}(\alpha)) \cdot y \cdot x^\alpha \oplus \bigoplus_{\alpha \in E_2^n} c_{f_0}(\alpha) \cdot x^\alpha.$$

Перепишем следующим образом:

$$f = \bigoplus_{(1,\alpha) \in E_2^{n+1}} (c_{f_0}(\alpha) \oplus c_{f_1}(\alpha)) \cdot (y^1 \cdot x^\alpha) \oplus \bigoplus_{(0,\alpha) \in E_2^{n+1}} c_{f_0}(\alpha) \cdot (y^0 \cdot x^\alpha).$$

Из полученного находим:

$$\begin{aligned} c_f(0, \alpha_1, \dots, \alpha_n) &= c_{f_0}(\alpha), \\ c_f(1, \alpha_1, \dots, \alpha_n) &= c_{f_0}(\alpha) \oplus c_{f_1}(\alpha). \end{aligned}$$

□

Пользуясь формулами предыдущей теоремы, найдем Жегалкина функции  $f(x_1, x_2, x_3)$ :

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

На шаге 1 вычисляем коэффициенты полиномов Жегалкина всех подфункций  $f_\sigma(x_3)$ ,  $\sigma \in E_2^2$ , функции  $f(x_1, x_2, x_3)$  по переменным  $x_1, x_2$ .

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

На шаге 2, пользуясь полученными значениями на шаге 1, вычисляем коэффициенты полиномов Жегалкина всех подфункций  $f_\delta(x_2, x_3)$ ,  $\delta \in E_2^1$ , функции  $f(x_1, x_2, x_3)$  по переменной  $x_1$ :

$x_1$	$x_2$	$x_3$	$f$	1	2
0	0	0	0	0	0
0	0	1	0	0	0
0	1	0	0	0	0
0	1	1	1	1	1
1	0	0	0	0	0
1	0	1	1	1	1
1	1	0	1	1	1
1	1	1	1	0	1

Наконец, на шаге 3, пользуясь полученными значениями на шаге 2, вычисляем коэффициенты полиномов Жегалкина функции  $f(x_1, x_2, x_3)$ :

$x_1$	$x_2$	$x_3$	$f$	1	2	3
0	0	0	0	0	0	0
0	0	1	0	0	0	0
0	1	0	0	0	0	0
0	1	1	1	1	1	1
1	0	0	0	0	0	0
1	0	1	1	1	1	1
1	1	0	1	1	1	1
1	1	1	1	0	1	0

Получаем:

$$f(x_1, x_2, x_3) = x_2x_3 \oplus x_1x_3 \oplus x_1x_2.$$

## 1.2 Функции алгебры логики. Двойственность. Самодвойственные функции. Замкнутость класса самодвойственных функций.

**Опр.** Функция  $f^*(x_1, \dots, x_n) \in P_2$  называется двойственной к функции  $f(x_1, \dots, x_n) \in P_2$ , если

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

Отметим, что для любой функции  $f \in P_2$  верно  $(f^*)^* = f$ .

**Опр.** Функция  $f(x_1, \dots, x_n) \in P_2$  называется самодвойственной, если  $f^*(x_1, \dots, x_n) = f(x_1, \dots, x_n)$ . Заметим, что данное определение эквивалентно тому, что функция  $f$  на всех парах противоположных наборов принимает противоположные значения, т.е.  $\forall \alpha \in E_2^n : f(\overline{\alpha}) = \overline{f(\alpha)}$ . Множество всех самодвойственных функций обозначим  $S$ .

**Теорема.** Множество  $S$  является замкнутым классом.

Д-во. Применим лемму о замкнутом классе. Пусть  $f_0(y_1, \dots, y_m) \in S$ ,  $f_i(x_1, \dots, x_n) \in S$ ,  $i = \overline{1, m}$ . Рассмотрим функцию

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

Получаем:

$$\begin{aligned} \overline{f(\overline{x}_1, \dots, \overline{x}_n)} &= \overline{f_0(f_1(\overline{x}_1, \dots, \overline{x}_n), \dots, f_m(\overline{x}_1, \dots, \overline{x}_n))} = \\ &= \overline{f_0(\overline{f_1(x_1, \dots, x_n)}, \dots, \overline{f_m(x_1, \dots, x_n)})} = \\ &= \overline{f_0(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n))} = \\ &= \overline{f(x_1, \dots, x_n)}. \end{aligned}$$

Значит,  $f \in S$ . □

### 1.3 Функции алгебры логики. Монотонные функции. Замкнутость класса монотонных функций.

Пусть  $\alpha, \beta \in E_2^n$ . Будем говорить, что  $\alpha \leq \beta$ , если  $\alpha_i \leq \beta_i$ ,  $i = \overline{1, n}$ .

**Опр.** Функция  $f(x_1, \dots, x_n) \in P_2$  называется монотонной, если для любых наборов  $\alpha, \beta \in E_2^n$  из  $\alpha \leq \beta$  следует  $f(\alpha) \leq f(\beta)$ . Множество всех монотонных функций обозначим  $M$ .

**Теорема.** Множество  $M$  является замкнутым классом.

Д-во. Применим лемму о замкнутом классе. Пусть  $f_0(y_1, \dots, y_m) \in M$ ,  $f_i(x_1, \dots, x_n) \in M$ ,  $i = \overline{1, m}$ . Рассмотрим функцию

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

Пусть  $\alpha, \beta \in E_2^n$  и  $\alpha \leq \beta$ . Тогда:

$$f(\alpha) = f_0(f_1(\alpha), \dots, f_m(\alpha)) = f_0(\gamma).f(\beta) = f_0(f_1(\beta), \dots, f_m(\beta)) = f_0(\delta).$$

Заметим, что  $\gamma \leq \delta \implies f(\alpha) \leq f(\beta) \implies f \in M$ . □

### 1.4 Функции алгебры логики. Линейные функции. Лемма о нелинейной функции.

**Опр.** Функция  $f(x_1, \dots, x_n) \in P_2$  называется линейной, если она может быть представлена в виде:

$$f(x_1, \dots, x_n) = c_0 \oplus c_1 x_1 \oplus \dots \oplus x_n x_n,$$

где коэффициенты  $c_0, c_1, \dots, c_n \in E_2$ . Множество всех линейных функций обозначим  $L$ .



**Лемма.** Если  $f \notin L$ , то, подставляя вместо ее переменных функции  $0, 1, x, \bar{x}, y, \bar{y}$  можно получить функцию  $x \cdot y$  или функцию  $\overline{x \cdot y}$ .

*Д-во.* Если  $f(x_1, \dots, x_n) \notin L$ , то в ее полиноме Жегалкина найдется слагаемое ранга, не меньше двух. Не ограничивая общности, пусть в полиноме Жегалкина функции  $f$  содержится слагаемое  $x_1 \cdot \dots \cdot x_k$ , где  $k \geq 2$ . Представим полином Жегалкина функции  $f$  в виде:

$$\begin{aligned} f(x_1, \dots, x_n) &= x_1 x_2 \cdot g_1(x_3, \dots, x_n) \oplus x_1 \cdot g_2(x_3, \dots, x_n) \oplus \\ &= \oplus x_2 \cdot g_3(x_3, \dots, x_n) \oplus g_4(x_3, \dots, x_n), \end{aligned}$$

где  $g_1, \dots, g_4 \in P_2$ , причем  $g_1 \neq 0$ . Значит, найдется такой набор  $\alpha \in E_2^{n-2}$ , что  $g_1(\alpha) = 1$ . Пусть  $g_2(\alpha) = a, g_3(\alpha) = b, g_4(\alpha) = c$ , где  $a, b, c \in E_2$ . Тогда

$$f(x_1, x_2, \alpha_1, \dots, \alpha_{n-2}) = x_1 x_2 \oplus a x_1 \oplus b x_2 \oplus c.$$

Положим:

$$\varphi(x, y) = f(x \oplus b, y \oplus a, \alpha_1, \dots, \alpha_{n-2}).$$

Получаем:

$$\begin{aligned} \varphi(x, y) &= (x \oplus b)(y \oplus a) \oplus a(x \oplus b) \oplus b(y \oplus a) \oplus c = \\ &= (xy \oplus ax \oplus by \oplus ab) \oplus (ax \oplus ab) \oplus (by \oplus ab) \oplus c = \\ &= xy \oplus (ab \oplus c). \end{aligned}$$

□

## 1.5 Функции алгебры логики. Полнота. Теорема Поста о полноте системы функций алгебры логики.

**Теорема (Поста).** Пусть  $A \subseteq P_2$ . Множество  $A$  является полной системой тогда и только тогда, когда  $A$  не содержится ни в одном из классов  $T_0, T_1, L, S, M$ .

*Д-во.* ( $\Rightarrow$ ) От противного. Пусть  $A$  является полной системой, но содержится в одном из классов  $T_0, T_1, L, S, M$ , пусть, например,  $A \subseteq T_0$ . Тогда  $[A] \subseteq [T_0] = T_0 \neq P_2$ . Противоречие. Значит  $A$  не содержится ни в одном из классов  $T_0, T_1, L, S, M$ .

( $\Leftarrow$ ) Пусть  $A$  не содержится ни в одном из классов  $T_0, T_1, L, S, M$ . Докажем, что в этом случае  $A$  — полная система.

$A$  не содержится в классах  $T_0, T_1, L, S, M \Rightarrow$  в  $A$  найдутся такие функции  $f_0, f_1, f_l, f_s, f_m$ , что  $f_0 \notin T_0, f_1 \notin T_1, f_l \notin L, f_s \notin S, f_m \notin M$ . Отметим что функции  $f_0, f_1, f_l, f_s, f_m$  не обязательно различны. Покажем, что функциями над  $A$  можно выразить все функции из полной системы  $\{0, 1, \bar{x}, x, x \cdot y\}$ .

**1.** Построение констант 0 и 1.

Рассмотрим функции  $f_0$  и  $f_1$ . Положим  $\varphi_0(x) = f_0(x, \dots, x), \varphi_1(x) = f_1(x, \dots, x)$ . Тогда:

$x$	$\varphi_0$	$\varphi_1$
0	1	$b$
1	$a$	0

Теперь, если  $a = 1$  и  $b = 0$ , то  $\varphi_0(x) = 1$ ,  $\varphi_1(x) = 0$ .

Если же  $a = 0$  или  $b = 1$ , то получена функция  $\bar{x}$ . Тогда по лемме о несамодвойственной функции из  $f_s \in S$ , подставляя вместо ее переменных функции  $x$ ,  $\bar{x}$ , получаем некоторую константу  $c \in E_2$ , а затем  $\bar{x} \in E_2$ .

**2. Построение отрицания  $\bar{x}$ .**

По лемме о немонотонной функции из  $f_m$ , подставляя вместо ее переменных функции 0, 1,  $x$ , получаем отрицание  $\bar{x}$ .

**3. Построение конъюнкции.**

По лемме о нелинейной функции из  $f_l$  подставляя вместо ее переменных функции 0, 1,  $x$ ,  $\bar{x}$ ,  $y$ ,  $\bar{y}$  и, возможно навешивая отрицание над функцией, получаем конъюнкцию  $x \cdot y$ .  $\square$

## 1.6 Функции алгебры логики. Предполные классы. Теорема о предполных классах.

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

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

**Утверждение.** Любой предполный класс является замкнутым классом.

*Д-во.* От противного. Пусть  $A \subseteq P_2$  — предполный класс, но  $[A] \neq A$ . Тогда  $\exists f \in [A] \setminus A$ . Получаем:  $[A] = [A \cup \{f\}] = P_2$ . Противоречие. Значит  $[A] = A$ .  $\square$

**Теорема.** В  $P_2$  найдется всего пять предполных классов:  $T_0$ ,  $T_1$ ,  $L$ ,  $S$ ,  $M$ .

*Д-во.* Сначала покажем, что каждый из классов  $T_0$ ,  $T_1$ ,  $L$ ,  $S$ ,  $M$  не содержится ни в каком из этих классов. Для этого построим таблицу, в которой строки и столбцы соответствуют этим классам, а на пересечении строки и столбца указана функция, принадлежащая классу, которым обозначена эта строка, и не принадлежащая классу, которым обозначен этот столбец:

	$T_0$	$T_1$	$L$	$S$	$M$
$T_0$	—	0	$x \cdot y$	0	$x \oplus y$
$T_1$	1	—	$x \cdot y$	1	$x \sim y$
$L$	$\bar{x}$	$\bar{x}$	—	0	$\bar{x}$
$S$	$\bar{x}$	$\bar{x}$	$m(x, y, z)$	—	$\bar{x}$
$M$	1	0	$x \cdot y$	0	—

где  $m(x, y, z) = xy \oplus xz \oplus yz$ .

Теперь докажем, что каждый из классов  $T_0, T_1, L, S, M$  является предполным. Например, рассмотрим класс  $T_0$ . Тогда:

1.  $[T_0] = T_0 \neq P_2$ ;
2. если  $f \notin T_0$ , то по теореме Поста:  $[T_0 \cup \{f\}] = P_2$ .

Значит  $T_0$  — предполный класс. Аналогично проводятся рассуждения для остальных классов.

Наконец, докажем от противного, что других предполных классов нет. Пусть  $A \subseteq P_2$  — предполный класс, причем  $A \neq T_0, T_1, L, S, M$ . Значит либо  $A$  не содержится ни в одном из этих классов, либо строго содержится в каком-то из них.

Если  $A$  не содержится ни в одном из этих классов, то по теореме Поста  $[A] = P_2$ . Получаем противоречие с п.1 определения предполного класса.

Пусть  $A$  строго содержится в каком-то из этих классов, например, пусть  $A \subseteq T_0, A \neq T_0$ . Тогда  $\exists f \in T_0 \setminus A$ , откуда  $[A \cup \{f\}] \subseteq T_0 \neq P_2$ . Получаем противоречие с п.2 определения предполного класса.

Значит других предполных классов нет. □

## 1.7 Деревья. Теорема о равносильных определениях дерева.

**Опр.** *Деревом называется связный граф без циклов.*

**Теорема.** *Пусть  $G = (V, E)$  — граф с  $p$  вершинами и  $q$  ребрами. Тогда следующие утверждения равносильны:*

1.  $G$  — дерево;
2.  $G$  — связный граф и  $q = p - 1$ ;
3.  $G$  — граф без циклов и  $q = p - 1$ ;
4.  $G$  — граф без циклов, но при соединении любой пары несмежных вершин ребром появляется цикл;
5.  $G$  — связный граф, но при удалении любого ребра остается несвязный граф.

*Д-во.*  $(1 \implies 2)$   $G$  — без циклов, поэтому по соотношению для  $G$  между числом вершин  $p$ , числом ребер  $q$  и числом компонент связности  $s = 1$  получаем:  $1 = s = p - q$ . Значит,  $q = p - 1$ .

$(2 \implies 3)$  Если в связном графе  $G$  найдется цикл, то удалим из  $G$  некоторое ребро  $e$  из цикла. Останется связный граф  $G'$ . По соотношению для  $G'$  между числом вершин  $p$ , числом ребер  $q - 1$  и числом компонент связности  $s' = 1$  получаем:  $s' \geq p - (q - 1) = (p - q) + 1 = 2$  — противоречие. Значит,  $G$  без циклов.

$(3 \implies 4)$  По соотношению для  $G$  между числом вершин  $p$ , числом ребер  $q$  и числом

компонент связности  $s$  получаем:  $s = p - q = 1$ , т. е.  $G$  связный. Значит, при соединении в  $G$  любой пары несмежных вершин ребром появится цикл.

(4  $\implies$  5) Если  $G$  не связный, то при соединении двух вершин из разных компонент связности цикл не появится. Значит,  $G$  связный. Пусть при удалении из  $G$  некоторого ребра  $e$  остался связный граф  $G'$ . Тогда  $G$  получается из связного графа  $G'$  добавлением нового ребра  $e$ . Поэтому в  $G$  найдется цикл — противоречие. Значит, при удалении из  $G$  любого ребра останется несвязный граф.

(5  $\implies$  1) Если в  $G$  найдется цикл, то удалим из  $G$  любое ребро из цикла. Останется связный граф — противоречие. Значит,  $G$  без циклов.  $\square$

## 1.8 Остовные деревья. Алгоритм построения кратчайшего остовного дерева в связном графе (с обоснованием).

**Опр.** *Остовным деревом графа называется его остовный подграф, являющийся деревом.*

Значит,  $D$  — остовное дерево графа  $G$ , если выполняются три свойства:

- 1)  $D$  — остовный подграф, т.е. содержит все вершины графа  $G$ ;
- 2)  $D$  — связный граф;
- 3)  $D$  — граф без циклов.

**Опр.** *Граф  $G = (V, E)$  называется взвешенным, если задана функция весов  $w : E \rightarrow \mathbb{R}_+$ , которая ставит в соответствие каждому ребру  $e \in E$  неотрицательное действительное число  $w(e)$ , называемое весом этого ребра  $e$ .*

**Опр.** *Пусть  $G = (V, E)$  — взвешенный связный граф с функцией весов  $w$  и  $D = (V, E')$  — его остовное дерево,  $E' \subseteq E$ . Тогда весом  $w(D)$  дерева  $D$  называется сумма весов всех его ребер, т.е.  $w(D) = \sum_{e \in E'} w(e)$ .*

**Опр.** *Остовное дерево  $D^*$  связного графа  $G$  называется кратчайшим, если его вес  $w(D^*)$  является наименьшим среди весов всех остовных деревьев графа  $G$ .*

### Алгоритм построения кратчайшего остовного дерева.

1. Положить  $H_1 = (V_1, E_1)$ , где  $V_1 = \{v\}$ ,  $v \in V$  — произвольная вершина,  $E_1 = \emptyset$ .
2. Для всех  $i = 1, \forall, p - 1$  повторить: выбрать произвольное ребро  $e_i \in E$  наименьшего веса в множестве  $\{e = (v, w) \in E : v \in V_i, w \in V \setminus V_i\}$ , и положить  $H_{i+1} = (V_i \cup \{w_i\}, E_i \cup \{e_i\})$ .
3. Положить  $D^* = H_p$ .

**Теорема.** *Предложенный выше алгоритм для заданного графа и для заданной функции весов  $w$  находит какое-то кратчайшее дерево  $D^*$  графа  $G$ .*

*Д-во.* Пусть алгоритм строит граф  $D^* = (V, E^*)$ ,  $E^* \subseteq E$ .

1. Сначала покажем, что граф  $D^*$  — остовное дерево графа  $G$ . Действительно, начинаем

с дерева  $H_1$ , состоящего из одной вершины. На каждом шаге добавляем одну вершину и одно ребро, получая дерево  $H_{i+1}$ ,  $i = 1, \dots, p-1$ . Дерево  $H_p = D^*$  содержит  $p$  вершин, поэтому является остовным.

**2.** Теперь покажем, что граф  $D^*$  — кратчайшее остовное дерево графа  $G$ . Пусть  $D' = (V, E')$ ,  $E' \subseteq E$  — какое-то кратчайшее остовное дерево графа  $G$ . Пусть при построении дерева  $D^*$  ребра добавлялись в следующем порядке:  $e_1, e_2, \dots, e_{p-1}$ .

Пусть  $k$  — такое число,  $1 \leq k \leq p$ , что ребра  $e_1, \dots, e_{k-1}$  принадлежит дереву  $D'$ , а ребро  $e_k$  не принадлежит дереву  $D'$ . Если  $k = p$ , то  $D^* = D'$  и все доказано.

Пусть  $k < p$ . Рассмотрим дерево  $H_k = (V_k, E_k)$ ,  $E_k = \{e_1, \dots, e_{k-1}\} \subseteq E$ , полученное при применении алгоритма. Пусть  $e_k = (v_k, w_k)$ , где  $v_k \in V_k$ ,  $w_k \in V \setminus V_k$ . Заметим, что  $H_k$  является поддеревом дерева  $D'$ . В дереве  $D'$  найдется простая  $(v_k, w_k)$ -цепь  $P$ . Пусть  $e' = (v', w') \in E'$  — первое такое ребро этой цепи при движении от вершины  $v_k$  к вершине  $w_k$ , что  $v' \in V_k$ ,  $w' \in V \setminus V_k$ . При этом  $e' \neq e_k$ . Отметим, что  $w(e_k) \leq w(e')$ , т.к. иначе при применении алгоритма к дереву  $H_k$  было бы добавлено ребро  $e'$ , а не ребро  $e_k$ . Рассмотрим подграф  $G' = D' + e_k$ . Граф  $G'$  содержит ровно один цикл  $C = v_k P_1 e' P_2 w_k e_k v_k$ , где  $P_1$  и  $P_2$  — части, на которых ребро  $e'$  разбивает цепь  $P$ , причем  $v_k P_1 v'$  — проста цепь в дереве  $H_k$ . Значит, подграф  $H = G' - e'$  является связным и не содержит циклов. Итак,  $H$  — остовный связный подграф без циклов. Значит,  $H$  — остовное дерево графа  $G$ . Кроме того,  $w(H) = w(D') - w(e') + w(e_k) \leq w(D')$ . Но  $D'$  — кратчайшее дерево, поэтому  $w(H) = w(D')$ .

Таким образом, построили кратчайшее остовное дерево  $H$ , у которого с остовным деревом  $D^*$  совпадает уже не менее  $k$  первых добавляемых по алгоритму ребер. Повторим рассуждения, положив  $D' = H$ . Через конечное число повторов получим, что  $D^*$  — кратчайшее остовное дерево графа  $G$ .  $\square$

## 1.9 todo Раскраски вершин графов. Теорема о раскраске вершин планарных графов в 5 цветов.

text

## 1.10 todo Алфавитные коды. Однозначность (разделимость) алфавитного кода. Алгоритм Маркова распознавания однозначности алфавитного кода (с обоснованием).

text

## 1.11 todo Алфавитные коды. Теорема Маркова об алфавитных кодах.

text

**1.12    todo Алфавитные коды. Неравенство Макмиллана.**

text

**1.13    todo Алфавитные коды. Префиксные коды. Существование префиксного кода с заданными длинами кодовых слов.**

text

**1.14    todo Коды с минимальной избыточностью (оптимальные коды). Теорема редукции.**

text

**1.15    todo Коды, обнаруживающие и исправляющие ошибки. Критерии кодов, обнаруживающих и исправляющих  $t$  ошибок замещения. Функция  $M_t(n)$ , ее оценки.**

text

**1.16    todo Коды, исправляющие одну ошибку. Коды Хэмминга. Оценка функции  $M_1(n)$ .**

text

**1.17    todo Схемы из функциональных элементов и элементов задержки (СФЭЗ). Автоматность осуществляемых ими отображений.**

text

**1.18    todo Схемы из функциональных элементов и элементов задержки (СФЭЗ). Моделирование автоматной функции схемой из функциональных элементов и элементов задержки.**

text

**1.19** todo Конечные автоматы. Отличимость состояний конечно-го автомата. Теорема Мура. Достижимость оценки теоремы Мура.

text

**1.20** todo Схемы из функциональных элементов. Сумматор, верхняя оценка его сложности.

text

**1.21** todo Схемы из функциональных элементов. Вычитатель, верхняя оценка его сложности.

text

**1.22** todo Схемы из функциональных элементов (СФЭ). Умножитель. Метод Карацубы построения умножителя, верхняя оценка его сложности.

text

## 2 Часть Б.

**2.1** Функции алгебры логики. Существенность переменных. Формулы. Тождества.

**Опр.** Пусть  $E_2 = \{0, 1\}$ . Функцией алгебры логики называется произвольное отображение из  $E_2^n$  в  $E_2$ ,  $n \geq 1$ . Множество всех функций алгебры логики, зависящих от  $n$  переменных, обозначит  $P_2^{(n)}$ , а множество всех функций алгебры логики —  $P_2 = \bigcup_{n \geq 1} P_2^{(n)}$ .

**Опр.** Переменная  $x_i$  называется существенной для функции  $f(x_1, \dots, x_n) \in P_2$ , если найдутся такие элементы  $a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n \in E_2$ , что

$$f(a_1, \dots, a_{i-1}, 0, a_{i+1}, \dots, a_n) \neq f(a_1, \dots, a_{i-1}, 1, a_{i+1}, \dots, a_n).$$

Переменная, не являющаяся существенной, называется несущественной, или фиктивной. Как правило, мы будем рассматривать функции с точностью до несущественных переменных. Т.е. будем считать, что несущественные переменные можно добавлять и убирать.

**Опр.** Формула над множеством  $A$  определяется по индукции.

*Базис индукции.* Если  $f$  — обозначение  $m$ -местной функции из  $A$  и  $x_1, \dots, x_m$  — переменные (из  $X$ ), причем не обязательно различные, то выражение  $f(x_1, \dots, x_m)$  — формула.

*Индуктивный переход.* Если  $f$  — обозначение  $m$ -местной функции из  $A$  и  $F_1, \dots, F_m$  — уже построенные формулы или переменные (не обязательно различные), то выражение  $f(F_1, \dots, F_m)$  — формула.

**Опр.** Формулы  $F_1$  и  $F_2$  называются эквивалентными, если они определяют равные функции, т.е. функции  $f_{F_1}$  и  $f_{F_2}$  равны. Обозначение эквивалентных формул:  $F_1 = F_2$ ; при этом равенство  $F_1 = F_2$  называется тождеством.

Верны следующие тождества:

- коммутативность связок  $\cdot, \vee, \oplus, \sim, /, \downarrow$ ;
- ассоциативность связок  $\cdot, \vee, \oplus$ ;
- дистрибутивность видов

$$\begin{aligned}(x \vee y) \cdot z &= x \cdot z \vee y \cdot z; \\ (x \cdot y) \vee z &= (x \vee z) \cdot (y \vee z); \\ (x \oplus y) \cdot z &= z \cdot z \oplus y \cdot z.\end{aligned}$$

## 2.2 Функции алгебры логики. Теорема о разложении функции алгебры логики по переменным. Теорема о совершенной дизъюнктивной нормальной форме (ДНФ). Теорема о совершенной конъюнктивной нормальной форме (КНФ).

**Опр.** Если  $f(x_1, \dots, x_n) \in P_2^{(n)}$  и  $\sigma \in E_2^k$ ,  $1 \leq k \leq n$ , то положим

$$f_\sigma(x_{k+1}, \dots, x_n) = f(\sigma_1, \dots, \sigma_k, x_{k+1}, \dots, x_n).$$

Функция  $f_\sigma$  называется  $\sigma$ -подфункцией функции  $f$  по  $k$  первым переменным.

Если  $\sigma \in E_2$ , то введем обозначение:  $x^\sigma = \begin{cases} x, & \sigma = 1 \\ \bar{x}, & \sigma = 0 \end{cases}$ . Отметим, что  $x^\sigma = 1$  в том и только в том случае, когда  $x = \sigma$ .

**Теорема.** При  $1 \leq k \leq n$  каждая функция  $f(x_1, \dots, x_n) \in P_2$  может быть представлена в виде:

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



Д-во. Рассмотрим произвольный набор  $\alpha \in E_2^n$  и подставим его в левую часть равенства из утверждения. Получаем:

$$f(\alpha) = \bigvee_{\sigma \in E_2^k} \alpha_1^{\sigma_1} \cdot \dots \cdot \alpha_k^{\sigma_k} f(\sigma_1, \dots, \sigma_k, \alpha_{k+1}, \dots, \alpha_n).$$

Рассмотрим набор  $\beta \in E_2^k$ , где  $\beta_i = \alpha_i$ ,  $i = \overline{1, k}$ . Набор  $\sigma$  пробегает все наборы множества  $E_2^k$ , а набор  $\beta$  — какой-то набор из  $E_2^k$ .

1. Если  $\sigma \neq \beta$ , то найдется такое  $i$ ,  $1 \leq i \leq k$ , что  $\sigma_i \neq \alpha_i$ . Значит,  $\alpha_i^{\sigma_i} = 0$ , откуда в этом случае

$$\alpha_1^{\sigma_1} \cdot \dots \cdot \alpha_{i-1}^{\sigma_{i-1}} \cdot 0 \cdot \alpha_{i+1}^{\sigma_{i+1}} \cdot \dots \cdot \alpha_k^{\sigma_k} \cdot f(\sigma_1, \dots, \sigma_k, \alpha_{k+1}, \dots, \alpha_n) = 0.$$

2. Если  $\sigma = \beta$ , то для всех  $i$ ,  $i = \overline{1, k}$ , верно  $\sigma_i = \alpha_i$ , а значит,  $\alpha_i^{\sigma_i} = 1$ . Поэтому в этом случае

$$\alpha_1^{\sigma_1} \cdot \dots \cdot \alpha_k^{\sigma_k} f(\sigma_1, \dots, \sigma_k, \alpha_{k+1}, \dots, \alpha_n) = f(\alpha).$$

Следовательно,

$$f(\alpha) = 0 \vee \dots \vee 0 \vee f(\alpha) \vee 0 \vee \dots \vee 0 = f(\alpha).$$

□

**Опр.** Выражение (формула) вида

$$x_{i_1}^{\sigma_1} \cdot \dots \cdot x_{i_k}^{\sigma_k},$$

где  $x_{i_1}, \dots, x_{i_k}$  — различные переменные и  $\sigma_1, \dots, \sigma_k \in E_n$ , называется элементарной конъюнкцией (ЭК) ранга  $k$ ,  $k \geq 1$ .

**Опр.** Дизъюнктивной нормальной формой (ДНФ) длины  $l$ ,  $l \geq 1$ , назовем дизъюнкцию  $l$  различных ЭК. ДНФ длины 0 назовем константу 0. Если каждая переменная содержится все переменные этой ДНФ, то такая ДНФ называется совершенной.

**Теорема.** Каждая функция  $f(x_1, \dots, x_n) \in P_2$ ,  $F \neq 0$ , может быть представлена в виде совершенной ДНФ  $D_f$ , а именно:

$$f(x_1, \dots, x_n) = \bigvee_{\sigma \in E_2^n: f(\sigma)=1} x_1^{\sigma_1} \cdot \dots \cdot x_n^{\sigma_n}.$$

Д-во. Прямое следствие теоремы о дизъюнктивном разложении. □

**Теорема.** При  $1 \leq k \leq n$  каждая функция  $f(x_1, \dots, x_n) \in P_2$  может быть представлена в виде:

$$f(x_1, \dots, x_n) = \bigwedge_{\sigma \in E_2^k} (x_1^{\bar{\sigma}_1} \vee \dots \vee x_k^{\bar{\sigma}_k} \vee f(\sigma_1, \dots, \sigma_k, x_{k+1}, \dots, x_n)).$$

Д-во. Аналогично доказательству теоремы о дизъюнктивном разложении.  $\square$

**Опр.** Выражение (формула) вида

$$x_{i_1}^{\sigma_1} \wedge \dots \wedge x_{i_k}^{\sigma_k},$$

где  $x_{i_1}, \dots, x_{i_k}$  — различные переменные и  $\sigma_1, \dots, \sigma_k \in E_2$  называется элементарной дизъюнкцией (ЭД) ранга  $k$ ,  $k \geq 1$ .

**Опр.** Конъюнктивной нормальной формой (КНФ) длины  $l$ ,  $l \geq 1$ , назовем конъюнкцию  $l$  различных ЭД. КНФ длины 0 назовем константу 1. Если каждая ЭД в КНФ содержит все переменные этой КНФ, то такая КНФ называется совершенной.

**Теорема.** Каждая функция  $f(x_1, \dots, x_n) \in P_2$ ,  $f \neq 0$ , может быть представлена в виде совершенной КНФ  $K_f$ , а именно:

$$f(x_1, \dots, x_n) = \bigwedge_{\sigma \in E_2^n: f(\sigma)=0} (x_1^{\bar{\sigma}_1} \vee \dots \vee x_n^{\bar{\sigma}_n}).$$

Д-во. Прямое следствие из теоремы о конъюнктивном разложении.  $\square$

## 2.3 Функции алгебры логики. Полные системы. Примеры полных систем (с доказательством полноты).

**Опр.** Пусть  $A \subseteq P_2$ . Множество  $A$  называется полной системой, если формулами над  $A$  можно выразить любую функцию алгебры логики.

**Утверждение.** Система  $A = \{x \cdot y, x \vee y, \bar{x}\}$  является полной.

Д-во. Рассмотрим произвольную функцию  $f \in P_2$ .

1. Если  $f = 0$ , то  $f = \bar{x} \cdot x$ .

2. Если  $f \neq 0$ , то представим  $f$  ее совершенной ДНФ.  $\square$

**Утверждение.** Следующие множества являются полными системами:

1.  $A = \{\bar{x}, x \cdot y\};$

2.  $A = \{\bar{x}, x \vee y\};$

3.  $A = \{x/y\};$

4.  $A = \{x \downarrow y\}.$

Д-во. Система  $B = \{x \cdot y, x \vee y, \bar{x}\}$  полная. Выразим все ее функции через функции систем их условия.

1.  $x \vee y = \overline{\bar{x} \cdot \bar{y}}.$

2.  $x \cdot y = \overline{\overline{x} \vee \overline{y}}$ .
3.  $\overline{x} = x/x, \quad x \cdot y = \overline{x/y}$ .
4.  $\overline{x} = x \downarrow x, \quad x \vee y = \overline{x \downarrow y}$ .

□

## 2.4 Функции алгебры логики. Теорема Жегалкина о выразимости функции алгебры логики полиномом Жегалкина.

**Опр.** Элементарная конъюнкция, не содержащая отрицаний переменных, называется монотонной (ЭК), или мономом, или одночленом.

**Опр.** Полиномом Жегалкина длины  $l$ ,  $l \geq 1$ , назовем сумму по модулю два  $l$  различных монотонных ЭК. Полиномом Жегалкина длины 0 назовем константу 0.

**Теорема.** Каждая функция  $f(x_1, \dots, x_n) \in P_2$  может быть единственным образом представлена в виде полинома Жегалкина  $P_f$ .

*Д-во. Существование.* Применим полиномиальное разложение функции  $f(x_1, \dots, x_n)$  по всем  $n$  переменным:

$$f(x_1, \dots, x_n) = \bigoplus_{\sigma \in E_2^n} x_1^{\sigma_1} \cdot \dots \cdot x_n^{\sigma_n} \cdot f(\sigma).$$

Затем пользуясь тождеством  $x^\sigma = x \oplus \sigma \oplus 1$  везде в правой части заменим выражение  $x_i^{\sigma_i}$  на выражение  $x_i \oplus \sigma_i \oplus 1$ . Далее по правилам коммутативности и ассоциативности  $\&$  и  $\oplus$  и дистрибутивности вида  $x \cdot (y \oplus z) = x \cdot y \oplus x \cdot z$  перемножим все скобки. После этого приведем подобные слагаемые по правилам  $x \oplus x = x$ ,  $x \oplus 0 = x$ . В итоге получим полином Жегалкина, который представляет исходную функцию  $f$ .

*Единственность.* Покажем, что число полиномов Жегалкина над переменными  $x_1, \dots, x_n$  совпадает с числом функций из  $P_2^{(n)}$ . Монотонных элементарных конъюнкций над переменными  $x_1, \dots, x_n$  всего найдется  $2^n$ , т.к. каждая переменная  $x_i$ ,  $i = \overline{1, n}$ , может либо входить, либо не входить в такую монотонную ЭК. Далее, полиномов Жегалкина над переменными  $x_1, \dots, x_n$  всего найдется  $2^{2^n}$ , т.к. каждая из  $2^n$  монотонных ЭК может либо входить, либо не входить в такой полином Жегалкина. Значит, учитывая то, что каждая функция  $f$  из  $P_2^{(n)}$  может быть представлена в виде полинома Жегалкина, это представление единственно. □

## 2.5 Функции алгебры логики. Замыкание, замкнутый класс. Функции, сохраняющие константу, и линейные функции. Замкнутость классов функций, сохраняющих константу, и линейных функций.

**Опр.** Пусть  $A \subseteq P_2$ . Замыканием  $[A]$  множества  $A$  называется множество всех функций, который могут быть выражены формулами над  $A$ .

**Опр.** Замыкание множества  $A$  можно определить по-другому. Замыкание  $[A]$  называется множеством всех функций из  $P_2$ , которые можно получить из функций множества  $A$  применением следующих операций:

1. добавлением или удалением несущественных переменных;
2. подстановкой в функции из  $A$  вместо переменных других переменных (не обязательно различных);
3. подстановкой в функции из  $A$  вместо переменных функций из  $A$  или функций, который уже получены.

Операции 1–3 называем операциями суперпозиции.

**Утверждение.** Два приведенных определения замыкания  $A$ ,  $A \subseteq P_2$ , равносильны.

Для произвольных множеств  $A, B \subseteq P_2$  верны следующие утверждения:

1.  $[P_2] = P_2$ ;
2.  $A \subseteq [A]$ ;
3. если  $A \subseteq B$ , то  $[A] \subseteq [B]$ ;
4.  $[[A]] = [A]$ .

**Опр.** Пусть  $A \subseteq P_2$ . Множество  $A$  называется замкнутым классом, если  $[A] = A$ .

**Утверждение.** Пусть  $A \subseteq P_2$ ,  $A$  — замкнутый класс и  $A \neq P_2$ . Тогда для любого множества  $B$ ,  $B \subseteq P_2$ , верно: если  $B \subseteq A$ , то  $B$  — не полная система.

*Д-во.* Итак,  $B \subseteq A$ . По свойствам замыкания и из условия получаем:  $[B] \subseteq [A] = A \neq P_2$ . Значит  $[B] \neq P_2$ , т.е.  $B$  — не полная система.  $\square$

**Опр.** Функция  $f(x_1, \dots, x_n) \in P_2$  сохраняет 0, если  $f(0, \dots, 0) = 0$ . Множество всех функций, сохраняющих 0, обозначим  $T_0$ .

**Опр.** Пусть  $e_i^n \subseteq P_2^{(n)}$  и  $e_i^n(x_1, \dots, x_n) = x_i$ ,  $i = \overline{1, n}$ ,  $n \geq 1$ . Положим  $I = \{e_i^n : i = \overline{1, n}, n \geq 1\}$ , т.е.  $I$  — множество всех функций конгруэнтных тождественной функции.

**Лемма.** Пусть  $A \subseteq P_2$  и  $I \subseteq A$ . Если для любых функций  $f_0(y_1, \dots, y_m) \in A$ ,  $f_i(x_1, \dots, x_n) \in A$ ,  $i = \overline{1, m}$ , причем функции  $f_i$  могут зависеть несущественно от некоторых своих переменных, верно

$$f_0(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)) \in A,$$

то множество  $A$  является замкнутым классом.

*Д-во.* Рассмотрим произвольную функцию  $f \in [A]$ . Она выражается некоторой формулой  $F$  над множеством  $A$ . Докажем индукцией по числу  $d$  вхождений в формулу  $F$  обозначений функций из  $A \setminus I$ , что  $f \in A$ .

1. Базис индукции:  $d = 0$ . Если  $F = x_i$ , то  $f \in A$  по условию утверждения.
2. Индуктивный переход. Пусть любая функция, которая может быть выражена формулой не более чем с  $d_0$  вхождениями обозначений функции из  $A \setminus I$ , содержится в  $A$ . Рассмотрим функцию  $f(x_1, \dots, x_n) \in [A]$ , которая выражается формулой  $F$  с  $d_0 + 1$  вхождениями обозначений функций из  $A \setminus I$ . Тогда  $F = F_0(F_1, \dots, F_m)$ , где  $f_0 \in A \setminus I$ ,  $F_i$  — формулы не более чем с  $d_0$  вхождениями функций из  $A \setminus I$ . По предположению индукции  $f_{F_i} \in A \implies$

$$f(x_1, \dots, x_n) = f_0(f_{F_1}(x_1, \dots, x_n), \dots, f_{F_m}(x_1, \dots, x_n)).$$

Далее, по условию утверждения  $f \in A$ . □

**Теорема.** Множество  $T_0$  является замкнутым классом.

*Д-во.* Применим лемму о замкнутом классе. Пусть  $f_0(y_1, \dots, y_m) \in T_0$ ,  $f_i(x_1, \dots, x_n) \in T_0$ ,  $i = \overline{1, m}$ . Рассмотрим функцию

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

Получаем:

$$f(0, \dots, 0) = f_0(f_1(0, \dots, 0), \dots, f_m(0, \dots, 0)) = f_0(0, \dots, 0) = 0.$$

Значит,  $f \in T_0$ . □

**Опр.** Функция  $f(x_1, \dots, x_n) \in P_2$  сохраняет 1, если  $f(1, \dots, 1) = 1$ . Множество всех функций, сохраняющих 1, обозначим  $T_1$ .

**Теорема.** Множество  $T_1$  является замкнутым классом.

*Д-во.* Полностью аналогично доказательству предыдущего утверждения. □

**Опр.** Функция  $f(x_1, \dots, x_n) \in P_2$  называется линейной, если она может быть представлена в виде:

$$f(x_1, \dots, x_n) = c_0 \oplus c_1 x_1 \oplus \dots \oplus c_n x_n,$$

где коэффициенты  $c_0, c_1, \dots, c_n \in E_2$ . Множество всех линейных функций обозначим  $L$ .

**Теорема.** Множество  $L$  является замкнутым классом.

*Д-во.* Достаточно заметить, что при подстановке вместо переменных линейной функции каких-то других линейных функций не могут появиться конъюнкции переменных в слагаемых. □

## 2.6 Функции алгебры логики. Самодвойственные функции. Лемма о несамодвойственной функции.

**Опр.** Функция  $f(x_1, \dots, x_n) \in P_2$  называется самодвойственной, если  $f^*(x_1, \dots, x_n) = f(x_1, \dots, x_n)$ . Заметим, что данное определение эквивалентно тому, что функция  $f$  на всех парах противоположных наборов принимает противоположные значения, т.е.  $\forall \alpha \in E_2^n : f(\bar{\alpha}) = \overline{f(\alpha)}$ . Множество всех самодвойственных функций обозначим  $S$ .

**Лемма.** Если  $f \notin S$ , то, подставляя вместо ее переменных функции  $x, \bar{x}$ , можно получить функцию, равную константе.

*Д-во.* Если  $f(x_1, \dots, x_n) \notin S$ , то найдется такая пара противоположных наборов  $\alpha, \bar{\alpha} \in E_2^n$ , что  $f(\alpha) = f(\bar{\alpha}) = c \in E_2$ . Положим:

$$\varphi(x) = f(x \oplus \alpha_1, \dots, x \oplus \alpha_n).$$

Получаем:

$$\varphi(0) = f(\alpha) = c, \varphi(1) = f(\bar{\alpha}) = c.$$

Значит,  $\varphi(x) = c$ . □

## 2.7 Функции алгебры логики. Монотонные функции. Лемма о немонотонной функции.

Пусть  $\alpha, \beta \in E_2^n$ . Будем говорить, что  $\alpha \leq \beta$ , если  $\alpha_i \leq \beta_i, i = \overline{1, n}$ .

**Опр.** Функция  $f(x_1, \dots, x_n) \in P_2$  называется монотонной, если для любых наборов  $\alpha, \beta \in E_2^n$  из  $\alpha \leq \beta$  следует  $f(\alpha) \leq f(\beta)$ . Множество всех монотонных функций обозначим  $M$ .

**Лемма.** Если  $f \notin M$ , то, подставляя вместо ее переменных функции  $0, 1, x$  можно получить функцию  $\bar{x}$ .

*Д-во.* Если  $f(x_1, \dots, x_n) \notin M$ , то найдется такая пара наборов  $\alpha, \beta \in E_2^n$ , что  $\alpha \leq \beta$ , но  $f(\alpha) > f(\beta)$ . Значит,  $f(\alpha) = 1$  и  $f(\beta) = 0$ . Не ограничивая общности, пусть  $\alpha_1 = 0, \beta_i = 1, i = \overline{1, k}$  и  $\alpha_i = \beta_i, i = k+1, n$ . Положим:

$$\varphi(x) = f(\underbrace{x, \dots, x}_k, \alpha_{k+1}, \dots, \alpha_n).$$

Получаем:

$$\varphi(0) = f(\underbrace{0, \dots, 0}_k, \alpha_{k+1}, \dots, \alpha_n) = f(\alpha) = 1,$$

$$\varphi(1) = f(\underbrace{1, \dots, 1}_k, \alpha_{k+1}, \dots, \alpha_n) = f(\beta) = 0.$$

Значит,  $\varphi(x) = \bar{x}$ . □

## 2.8 Функции алгебры логики. Базис. Теорема о числе функций в базисе в алгебре логики.

**Опр.** Пусть  $B \subseteq P_2$ . Множество  $B$  называется базисом  $P_2$ , если

1.  $[B] = P_2$ ;
2.  $\forall f \in B : [B \setminus \{f\}] \neq P_2$ .

**Теорема.**

1. Любой базис  $P_2$  содержит не больше четырех функций.
2. Для любого числа  $k$ ,  $1 \leq k \leq 4$ , в  $P_2$  найдется базис, содержащий ровно  $k$  функций.

*Д-во.* **1.** Пусть  $B \subseteq P_2$  — базис  $P_2$ . Тогда  $B$  — полная система. Значит, по теореме Поста в  $B$  найдутся следующие (не обязательно различные) функции:  $f_0 \notin T_0$ ,  $f_1 \notin T_1$ ,  $f_l \notin L$ ,  $f_s \notin S$ ,  $f_m \notin M$ . Система  $\{f_0, f_1, f_l, f_s, f_m\}$  — полна, а  $B$  — избыточна, поэтому  $B = \{f_0, f_1, f_l, f_s, f_m\}$ . Значит,  $|B| \leq 5$ .

Рассмотрим функцию  $f_0 \in B$ ,  $f_0 \notin T_0$ :

$x_1$	$\dots$	$x_n$	$f_0$
0	$\dots$	0	1
	$\dots$		
1	$\dots$	1	$a$

Теперь

- 1) если  $a = 0$ , то  $f_0 \notin T_1, M$ , а значит,  $f_1 = f_m = f_0$  и  $|B| \leq 3$ ;
- 2) если  $a = 1$ , то  $f_0 \notin S$ , а значит,  $f_s = f_0$ , и  $|B| \leq 4$ .

Следовательно,  $|B| \leq 4$ .

**2.** Для каждого числа  $k$ ,  $1 \leq k \leq 4$ , приведем примеры базисов  $B$  из  $k$  функций:

1. если  $k = 1$ , то, например,  $B = \{x/y\}$  или  $B = \{x \downarrow y\}$ ;
2. если  $k = 2$ , то, например,  $B = \{\bar{x}, x \cdot y\}$  или  $B = \{\bar{x}, x \vee y\}$ ;
3. если  $k = 3$ , то, например,  $B = \{1, x \oplus y, x \cdot y\}$ ;
4. если  $k = 4$ , то, например,  $B = \{0, 1, x \oplus y \oplus z, x \cdot y\}$ .

□

## 2.9 Графы. Изоморфизм графов. Связность. Формула Эйлера для степеней вершин. Теорема о соотношении между числом вершин, ребер и компонент связности в графе.

**Опр.** (Неориентированным) графом  $G$  называется пара  $(V, E)$ , где  $V$  — непустое множество вершин;  $E$  — конечное множество ребер, причем каждому ребру  $e \in E$  сопоставлена неупорядоченная пара вершин, т.е.  $e = (v, w)$ , где  $v, w \in V$ .

Ребро  $e = (v, v)$ , где  $v \in V$ , называется петлей. Ребра  $e_1 = (v, w)$  и  $e_2 = (v, w)$ , где  $v, w \in V$  и  $e_1 \neq e_2$ , называются кратными ребрами. Граф, в котором допускаются и петли, и кратные ребра иногда называется псевдографом. Граф без петель, но, возможно, с кратными ребрами называется мультиграфом. Граф без петель и кратных ребер называется простым, или обыкновенным графом.

**Опр.** Два графа без петель и кратных ребер  $G_1 = (V_1, E_1)$  и  $G_2 = (V_2, E_2)$  называются изоморфными, если найдется взаимно однозначное отображение  $\varphi : V_1 \rightarrow V_2$ , сохраняющее ребра, т.е. для любых вершин  $v, w \in V_1$  выполняется соотношение:

$$(v, w) \in E_1 \Leftrightarrow (\varphi(v), \varphi(w)) \in E_2.$$

**Опр.** Степенью  $d_G(v)$  вершины  $v \in V$  в графе  $G = (V, E)$  называется число исходящих из нее ребер (причем петля вносит двойной вклад в степень вершины).

**Утверждение.** Пусть  $G = (V, E)$  — граф без петель и кратных ребер. Тогда

1.  $\sum_{v \in V} d_G(v) = 2 \cdot |E|;$

2. в графе  $G$  число вершин, имеющих нечетную степень, четно.

*Д-во.* 1. Рассмотрим сумму в левой части равенства. Т.к. любое ребро графа имеет ровно два конца, каждое ребро в этой сумме будет подсчитано ровно два раза. Получаем выражение в правой части равенства.

2. Свойство непосредственно следует из равенства п.1. □

**Опр.** Граф  $G = (V, E)$  называется связным, если для каждой пары вершин графа  $G$  найдется путь, соединяющий эти вершины (а значит, и простая цепь, соединяющая эти вершины). Максимальный (по включению) связный подграф графа  $G$  называется его компонентой связности.

**Теорема.** Пусть  $G = (V, E)$  — граф без петель и кратных ребер с  $p$  вершинами,  $q$  ребер и  $s$  компонентами связности. Тогда

1.  $s \geq p - 1;$

2. если в графе  $G$  отсутствуют циклы, то  $s = p - q$ .



*Д-во.* 1. Рассмотрим переход от графа  $G_i = (V, E_i)$  к графу  $G_{i+1} + e$ , где  $E_i \subseteq E$ ,  $e \in E \setminus E_i$ . Пусть в графах  $G_i, G_{i+1}$  соответственно  $s_i, s_{i+1}$  компонент связности. Тогда если ребро  $e$  соединяет вершины из одной компоненты связности графа  $G_i$ , то  $s_{i+1} = s_i$ ; и если ребро  $e$  соединяет вершины из разных компонент связности графа  $G_i$ , то  $s_{i+1} = s_i - 1$ . Поэтому  $s_{i+1} \geq s_i - 1$ . Граф  $G$  можно получить из графа  $G_0 = (V, \emptyset)$  с  $p$  компонентами связности добавлением всех ребер множества  $E$ . Поэтому  $s \geq p - q$ .

2. Если же в графе  $G$  нет циклов, то в предыдущих рассуждениях верно  $s_{i+1} = s_i - 1$ . Поэтому  $s = p - q$ .  $\square$

## 2.10 Деревья. Корневые деревья, упорядоченные корневые деревья. Верхняя оценка числа деревьев с заданным числом ребер.

**Опр.** *Деревом называется связный граф без циклов.*

**Опр.** *Корневым деревом называется пара  $(D; v_0)$ , где  $D = (V, E)$  — дерево,  $v_0 \in V$  — выделенная вершина, называемая корнем. При изоморфизме корневых деревьев корень обязан переходить в корень. Всякая вершина корневого дерева, не являющаяся корнем, называется листом.*

**Опр.** *Пусть  $(D; v_0)$  — корневое дерево и  $D_1, \dots, D_m$  — все его поддеревья. Корневое дерево  $D$  называется упорядоченным, если задан порядок его поддеревьев, а каждое его поддерево  $D_i, i = \overline{1, m}$ , также является упорядоченным корневым деревом.*

**Теорема.** *Для числа  $\delta''(q)$  неизоморфных упорядоченных корневых деревьев с  $q$  ребрами справедлива оценка:  $\delta''(q) \leq 4^q$ .*

*Д-во.* Пусть  $(D, v_0)$  — упорядоченное корневое дерево с  $q$  ребрами. Обойдем дерево  $D$  в глубину из вершины  $v_0 \in V$  по порядку его поддеревьев. При таком обходе по каждому ребру пройдем два раза: первый раз при обходе в соответствующее поддерево, второй раз при возвращении из него.

По этому обходу построим код дерева  $D$  — набор  $k(D)$  из нулей и единиц длины  $2q$ . Сначала этот код не заполнен. При проходе по очередному ребру заполняем в коде  $k(D)$  первый незаполненный разряд по следующим правилам:

- 1) если по ребру переходим в поддерево, то в код  $k(D)$  пишем ноль;
- 2) если по ребру возвращаемся из поддерева, то в код  $k(D)$  пишем единицу.

Тогда различным упорядоченным корневым деревьям соответствуют разные коды. Поэтому  $\delta''(q)$  не превосходит числа наборов из нулей и единиц длины  $2q$ , т.е.

$$\delta''(q) \leq 2^{2q} = 4^q.$$

$\square$

## 2.11 Геометрическое представление графов. Теорема о геометрическом представлении графов в трехмерном пространстве.

**Опр.** Геометрическим представлением графа  $G = (V, E)$  в пространстве  $\mathbb{R}^n$  называется такое его отображение в  $\mathbb{R}^n$ , при котором:

1. каждой вершине  $v \in V$  сопоставлена точка в  $\mathbb{R}^n$ , причем разным вершинам — разные точки;
2. каждому ребру  $(v, w) \in E$  сопоставлена непрерывная кривая, соединяющая точки, соответствующие вершинам  $v$  и  $w$ , и не проходящая через точки, соответствующие другим вершинам;
3. кроме того, кривые, соответствующие различным ребрам, не пересекаются за исключением своих концов.

**Теорема.** Любой граф  $G$  допускает геометрическое представление в  $\mathbb{R}^3$ .

*Д-во.* Пусть  $G = (V, E)$ , где  $V = \{v_1, \dots, v_p\}$ ,  $E = \{e_1, \dots, e_q\}$ . Возьмем в  $\mathbb{R}^3$  произвольную прямую  $l$  и отметим на ней  $p$  различных точек, которые обозначим  $v_1, \dots, v_p$ . Сопоставим их вершинам графа  $G$ . Возьмем  $q$  различных плоскостей  $\pi_1, \dots, \pi_q$ , содержащих прямую  $l$ . Ребру  $e_i = (v_{i_1}, v_{i_2})$  графа  $G$  сопоставим кривую, соединяющую точки  $v_{i_1}$  и  $v_{i_2}$ , которую проведем в плоскости  $\pi_i$ ,  $i = 1, \dots, q$ . По построению кривые, сопоставленные ребрам, могут пересекаться только в концевых точках. Значит, получили геометрическое представление  $G$  в  $\mathbb{R}^3$ .  $\square$

## 2.12 Планарные графы. Формула Эйлера для планарных графов. Верхняя оценка числа ребер в планарном графе.

**Опр.** Граф  $G$  называется планарным, если найдется его геометрическое представление на плоскости (т.е. в  $\mathbb{R}^2$ ). В обратном случае граф  $G$  называется непланарным. Геометрическое представление планарного графа в  $\mathbb{R}^2$  назовем его укладкой на плоскости. Связные области плоскости, ограниченные ребрами планарного графа при его укладке на плоскости, называются гранями, неограниченная область называется также внешней гранью.

**Теорема** (формула Эйлера для планарных графов). Если  $G = (V, E)$  — связный планарный граф с  $p$  вершинами и  $q$  ребрами, то для каждой его укладки на плоскости верно равенство:  $p - q + r = 2$ , где  $r$  — число граней в этой укладке.

*Д-во.* Проведем индукцию по  $q$  при заданном  $p$ .

*Базис индукции.* Если  $q = p - 1$ , то  $G$  — дерево. Каждое дерево — планарный граф с одной гранью. Поэтому формула верна.

*Индуктивный переход.* Рассмотрим связный планарный граф  $G$  с  $p$  вершинами и  $q \geq p$  ребрами. Пусть задана его укладка на плоскости, в которой  $r$  граней.

В графе  $G$  найдется хотя бы один цикл, и пусть  $e$  — любое ребро какого-то его цикла. Тогда граф  $G' = G - e$  — связный и планарный с  $p$  вершинами и  $q - 1$  ребрами, и его укладка на плоскости содержит  $r - 1$  грань, т.к. при удалении ребра  $e$  из укладки графа  $G$  две грани соединяются в одну. Для графа  $G'$  верно предположение индукции, т.е.  $p - (q - 1) + (r - 1) = 2 \implies p - q + r = 2$ .  $\square$

**Теорема.** *Наибольшее число ребер в планарном графе (без петель и кратных ребер) с  $p \geq 3$  вершинами равно  $3p - 6$ .*

*Д-во.* Можно рассматривать связные графы.

**1. Верхняя граница.** Пусть  $G = (V, E)$  — связный планарный граф с  $p$  вершинами и  $q$  ребрами. Рассмотрим укладку графа  $G$  на плоскость, и пусть  $q_i$  — число ребер, встречающихся при обходе границы  $i$ -й грани в этой кладке,  $i = \overline{1, r}$ . Тогда  $\sum_{i=1}^r q_i = 2q$ , т.к.

каждое ребро:

- 1) либо разделяет две грани, а значит, считается при обходе границ этих двух граней;
- 2) либо лежит в одной грани, а значит, при обходе ее границы считается два раза.

Из связности графа и  $p \geq 3$  получаем  $q_i \geq 3$ , откуда  $3r \leq 2q$ , или  $r \leq \frac{2}{3}q$ . По формуле Эйлера  $r = q - p + 2$ , поэтому  $q - p + 2 \leq \frac{2}{3}q$ , а значит

$$1 \leq 3p - 6.$$

**2. Достижимость верхней оценки.** Построим графы, на которых достигается эта оценка. Это связные планарные графы, в которых любая грань (включая внешнюю) ограничена циклом длины три. Такие графы называются триангуляциями.

Если  $p = 3$ , то  $G_p = K_3$ . Пусть уже построен связный планарный граф  $G_p$  с  $p$  вершинами и  $3p - 6$  ребрами, каждая грань которого ограничена треугольником. Тогда граф  $G_{p+1}$  получается из  $G_p$  добавлением новой вершины внутри какой-то грани и ребер, соединяющих эту вершину с тремя вершинами границы этой грани.  $\square$

## 2.13 todo Графы $K_5$ и $K_{3,3}$ . Непланарность графов $K_5$ и $K_{3,3}$ . Теорема Понтрягина-Куратовского (доказательство в одну сторону).

text

## 2.14 todo Раскраски вершин графов. Теорема о раскраске вершин графа в 2 цвета (теорема Кенига).

text

**2.15** todo Коды с минимальной избыточностью (оптимальные коды). Три леммы о свойствах кодов с минимальной избыточностью.

text

**2.16** todo Коды с минимальной избыточностью (оптимальные коды). Алгоритм Хаффмена построения кода с минимальной избыточностью.

text

**2.17** todo Коды, исправляющие одну ошибку. Алгоритмы кодирования, исправления ошибки и декодирования в коде Хэмминга.

text

**2.18** todo Линейные двоичные коды. Теорема о кодовом расстоянии линейных кодов.

text

**2.19** todo Конечные автоматы. Функционирование конечного автомата. Автоматные функции. Канонические уравнения и диаграмма Мура конечного автомата. Единичная задержка, ее автоматность.

text

**2.20** todo Схемы из функциональных элементов. Выразимость функции алгебры логики схемой из функциональных элементов в базисе из конъюнкции, дизъюнкции и отрицания.

text