МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

В.Н. Кудашов

БУЛЕВЫ ФУНКЦИИ

РЕКОМЕНДОВАНО К ИСПОЛЬЗОВАНИЮ В УНИВЕРСИТЕТЕ ИТМО
по направлению подготовки (специальности) **09.03.04**
в качестве учебного пособия для реализации основных
профессиональных образовательных программ
высшего образования бакалавриата

УНИВЕРСИТЕТ ИТМО

Санкт-Петербург

2018

Кудашов В.Н. Булевы функции. – СПб: Университет ИТМО, 2018. – 33 с.

Рецензенты: Муромцев Д.И., кандидат техн. наук,
Симоненко З.Г., кандидат техн. наук

Пособие содержит введение в теорию булевых функций. Изложены основные свойства булевых функций и доказан критерий функциональной полноты.

Рассчитано на бакалавров 09.03.04 Программная инженерия.

УНИВЕРСИТЕТ ИТМО

Университет ИТМО – ведущий вуз России в области информационных и фотонных технологий, один из немногих российских вузов, получивших в 2009 году статус национального исследовательского университета. С 2013 года Университет ИТМО – участник программы повышения конкурентоспособности российских университетов среди ведущих мировых научно-образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО – становление исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

1. Основные понятия

1.1. Булев куб

Обозначим $E_2 = \{0, 1\}$ и пусть E_2^n — n-я декартова степень множества E_2. Элементами E_2^n являются наборы $(\alpha_1, \ldots, \alpha_n)$, где каждое α_i равно либо 0 либо 1. Кратко набор $(\alpha_1, \ldots, \alpha_n)$ обозначают через $\widetilde{\alpha}^n$ или $\widetilde{\alpha}$. Множество E_2^n называют *n-мерным булевым (двоичным) кубом*. Множество E_2^n часто обозначают через B^n, при этом наборы $\widetilde{\alpha}^n$ называют *вершинами куба B^n*.

Набор $\widetilde{\alpha}^n = (\alpha_1, \ldots, \alpha_n) \in E_2^n$ называется *булевым* или *двоичным набором* (*вектором*). Элементы набора называются *компонентами* или *координатами*. Число n называется *длиной набора* $\widetilde{\alpha}^n$. *Весом* $|\widetilde{\alpha}^n|$ *набора* $\widetilde{\alpha}^n$ называется число его координат равных 1, т. е.

$$|\widetilde{\alpha}^n| = \sum_{i=1}^{n} \alpha_i.$$

Каждому двоичному набору $\widetilde{\alpha}^n$ сопоставим число

$$\nu(\widetilde{\alpha}^n) = \sum_{i=1}^{n} \alpha_i \cdot 2^{n-i},$$

называемое *номером набора* $\widetilde{\alpha}^n$. Набор $\widetilde{\alpha}^n$ является двоичным разложением своего номера $\nu(\widetilde{\alpha}^n)$.

Пример 1. Пусть $\widetilde{\alpha} = (1, 0, 1, 1, 1, 0, 0, 1)$. Тогда длина набора $\widetilde{\alpha}$ равна 8 и вес $|\widetilde{\alpha}| = 5$. Найдём $\nu(\widetilde{\alpha})$:

$$\nu(\widetilde{\alpha}^n) = 2^7 + 2^5 + 2^4 + 2^3 + 1 = 128 + 32 + 16 + 8 + 1 = 185.$$

Расстоянием (*Хэмминга*) между вершинами куба B^n называется число

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

оно равно числу координат, в которых наборы $\widetilde{\alpha}$ и $\widetilde{\beta}$ отличаются друг от друга. Нетрудно проверить, что функция $\rho(\widetilde{\alpha}, \widetilde{\beta})$ удовлетворяет условиям:

M_1) $\rho(\widetilde{\alpha}, \widetilde{\beta}) = 0 \Leftrightarrow \widetilde{\alpha} = \widetilde{\beta}$,

M_2) $\rho(\widetilde{\alpha}, \widetilde{\beta}) = \rho(\widetilde{\beta}, \widetilde{\alpha})$ (симметричность),

M_3) $\rho(\widetilde{\alpha}, \widetilde{\beta}) \le \rho(\widetilde{\alpha}, \widetilde{\gamma}) + \rho(\widetilde{\gamma}, \widetilde{\beta})$ (неравенство треугольника).

Из свойств M_1, M_2, M_3 следует, что булев куб B^n является *метрическим пространством* с метрикой $\rho(\widetilde{\alpha}, \widetilde{\beta})$.

Наборы $\widetilde{\alpha}$, $\widetilde{\beta} \in B^n$ называются *соседними*, если $\rho(\widetilde{\alpha}, \widetilde{\beta}) = 1$, и *противоположными*, если $\rho(\widetilde{\alpha}, \widetilde{\beta}) = n$. Соседние наборы различаются только в одной координате, а противоположные — во всех координатах.

Пример 2. Пусть

$$\widetilde{\alpha}_1 = (0, 0, 1, 0, 1),\ \widetilde{\alpha}_2 = (0, 1, 1, 0, 1),\ \widetilde{\alpha}_3 = (1, 1, 0, 1, 0).$$

Наборы $\widetilde{\alpha}_1$, $\widetilde{\alpha}_2$ являются соседними, а $\widetilde{\alpha}_1$, $\widetilde{\alpha}_3$ — противоположными.

Набор $\widetilde{\alpha}^n$ *предшествует* набору $\widetilde{\beta}^n$, и обозначают $\widetilde{\alpha} \preccurlyeq \widetilde{\beta}$, если $\alpha_i \le \beta_i$ для всех $i = 1, \ldots, n$. Отношение предшествования $\preccurlyeq$ удовлетворяет условиям:

U_1) $\widetilde{\alpha} \preccurlyeq \widetilde{\alpha}$,

U_2) если $\widetilde{\alpha} \preccurlyeq \widetilde{\beta}$ и $\widetilde{\beta} \preccurlyeq \widetilde{\gamma}$, то $\widetilde{\alpha} \preccurlyeq \widetilde{\gamma}$

Из свойств U_1, U_2 следует, что булев куб B^n является *частично упорядоченным множеством* относительно отношения $\preccurlyeq$. Вместо $\widetilde{\alpha}^n \preccurlyeq \widetilde{\beta}^n$ иногда пишут $\widetilde{\beta}^n \succcurlyeq \widetilde{\alpha}^n$.

Если $\widetilde{\alpha}^n \preccurlyeq \widetilde{\beta}^n$ и $\widetilde{\alpha}^n \ne \widetilde{\beta}^n$, то говорят, что набор $\widetilde{\alpha}^n$ *строго предшествует* набору $\widetilde{\beta}^n$, и пишут $\widetilde{\alpha}^n \prec \widetilde{\beta}^n$.

Наборы $\widetilde{\alpha}^n$ и $\widetilde{\beta}^n$ называются *сравнимыми*, если либо $\widetilde{\alpha}^n \preccurlyeq \widetilde{\beta}^n$, либо $\widetilde{\beta}^n \preccurlyeq \widetilde{\alpha}^n$. Говорят, что набор $\widetilde{\alpha}^n$ *непосредственно предшествует* набору $\widetilde{\beta}^n$, если $\widetilde{\alpha}^n \prec \widetilde{\beta}^n$ и $\rho(\widetilde{\alpha}^n, \widetilde{\beta}^n) = 1$.

Пример 3. Возьмём наборы $\widetilde{\alpha}_1$, $\widetilde{\alpha}_2$, $\widetilde{\alpha}_3$ из примера 2. Набор $\widetilde{\alpha}_1$ непосредственно предшествует набору $\widetilde{\alpha}_2$, а набор $\widetilde{\alpha}_3$ не сравним ни с набором $\widetilde{\alpha}_1$, ни с набором $\widetilde{\alpha}_2$.

Задачи.

1. Найти номера следующих наборов:

1) (10101101); 2) (010111101);

3) $(\underbrace{1\ldots1}_{m}\underbrace{0\ldots0}_{2m})$, $m \ge 1$;

4) $(1\underbrace{0\ldots0}_{m}\underbrace{1\ldots1}_{m}\underbrace{0\ldots0}_{m}1)$, $m \ge 1$.

Решение. 4) Пусть $\widetilde{\alpha} = (1\underbrace{0\ldots0}_{m}\underbrace{1\ldots1}_{m}\underbrace{0\ldots0}_{m}1)$. Имеем

$$\nu(\widetilde{\alpha}) = 2^{3m+1} + \sum_{k=m+1}^{2m} 2^k + 1 = 2^{3m+1} + 2^{2m+1} - 2^{m+1} + 1. \quad \blacksquare$$

2. Найти двоичный набор длины l, являющийся разложением числа n:

1) $l = 5$, $n = 28$; 2) $l = 8$, $n = 231$;

3) $l = m + 1$, $n = 2^m + 1$ $(m \geq 1)$;

4) $l = m$, $n = 3 \cdot 2^{m-2} - 1$ $(m \geq 2)$.

Решение. 4) Очевидно, что при $m = 2$ имеем (10), а при $m = 3$ имеем (101). Пусть $m \geq 4$. Тогда

$$n = 2^{m-1} + 2^{m-2} - 1 = 11\underbrace{0\ldots0}_{m-2} - 1 = 10\underbrace{1\ldots1}_{m-2}.$$

Следовательно, искомый набор имеет вид $(10\underbrace{1\ldots1}_{m-2})$. ■

3. На множестве наборов A из B^n указать естественный порядок $\preccurlyeq$. Выяснить, есть ли в множестве A соседние и противоположные наборы, и, если они имеются, выписать их.

1) $A = \{(0011), (0101), (0111), (1001), (1100), (1101)\}$;

2) $A = \{(00011), (01101), (01111), (10001), (11000), (11001)\}$;

3) $A = \{(00110), (00111), (01010), (01011), (10110), (11010), (11011)\}$;

4) $A = \{(000011), (011101), (011111), (100001), (110000), (110001)\}$;

Решение. 4) Обозначим через $\widetilde{\alpha}_1 = (000011)$, $\widetilde{\alpha}_2 = (011101)$, $\widetilde{\alpha}_3 = (011111)$, $\widetilde{\alpha}_4 = (100001)$, $\widetilde{\alpha}_5 = (110000)$, $\widetilde{\alpha}_6 = (110001)$. Имеем соотношения

$$\widetilde{\alpha}_1 \prec \widetilde{\alpha}_3, \quad \widetilde{\alpha}_4 \prec \widetilde{\alpha}_6,$$
$$\widetilde{\alpha}_2 \prec \widetilde{\alpha}_3, \quad \widetilde{\alpha}_5 \prec \widetilde{\alpha}_6.$$

Соседними являются наборы $\widetilde{\alpha}_2$ и $\widetilde{\alpha}_3$, $\widetilde{\alpha}_4$ и $\widetilde{\alpha}_5$, $\widetilde{\alpha}_5$ и $\widetilde{\alpha}_6$. Противоположных наборов нет. ■

1.2. Определение булевых функций.

Функция $f(x_1, \ldots, x_n)$, определённая на множестве E_2^n и принимающая значения из E_2 называется *булевой функцией*. Булевы функции также называют *функциями алгебры логики*. Через $P_2^{(n)}$ обозначим множество всех n-местных булевых функций, т. е. булевых функций, зависящих от n аргументов. *Нульместными* булевыми функциями, соответствующими $n = 0$, являются константы 0 и 1. Пусть P_2 — множество всех булевых функций.

Для задания булевой функции $f(x_1, \ldots, x_n)$ достаточно указать, какое значение функции соответствует каждому из наборов $(\alpha_1, \ldots, \alpha_n)$. Составим таблицу (см. табл. 1) Употребляется стандартное расположение строк

x_1	...	x_{n-1}	x_n	$f(x_1,\ldots,x_{n-1},x_n)$
0	...	0	0	$f(0,\ldots,0,0)$
0	...	0	1	$f(0,\ldots,0,1)$
0	...	1	0	$f(0,\ldots,1,0)$
1	...	1	1	$f(1,\ldots,1,1)$

Таблица 1.

таблицы. Наборы $(\alpha_1,\ldots,\alpha_n)$ расположены в порядке возрастания их номеров $\nu(\widetilde{\alpha})$.

Теорема 1. *Число $p_2(n)$ всех функций из $P_2^{(n)}$ равно 2^{2^n}.*

Доказательство. Различные таблицы отличаются лишь значениями правого столбца. Имеется взаимно однозначное соответствие между множеством $P_2^{(n)}$ и двоичными столбцами высоты 2^n. Всего таких столбцов 2^{2^n}. ■

Функция $f(x_1,\ldots,x_{i-1},x_i,x_{i+1},\ldots,x_n)$ из $P_2^{(n)}$ зависит *существенным образом* от аргумента x_i, если существуют такие значения α_1, ..., α_{i-1}, α_{i+1}, ..., α_n переменных x_1,..., x_{i-1}, x_{i+1},..., x_n, что

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

В этом случае переменная x_i называется *существенной*. Если x_i не является *существенной*. то она называется *несущественной* или *фиктивной*.

Число всех переменных, от которых булева функция f зависит существенно, называется *порядком* этой функции. Существуют два типа функций, не имеющих существенных переменных. Функции первого типа равны тождественно 0, а второго — 1. Порядок этих функций равен нулю.

Пусть для функции $f(x_1,\ldots,x_n)$ аргумент x_i является фиктивным. Зададим функцию $(n-1)$-го аргумента

$$g(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n)=f(x_1,\ldots,x_{i-1},0,x_{i+1},\ldots,x_n).$$

Будем говорить, что функция $g(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n)$ получена из функции $f(x_1,\ldots,x_n)$ *путём удаления фиктивной переменной* x_i, а также, что функция $f(x_1,\ldots,x_n)$ получается из $g(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n)$ *путём введения фиктивной переменной*.

Функции $f_1(x_1,\ldots,x_n)$ и $f_2(x_1,\ldots,x_m)$ называются *равными*, если функцию f_2 можно получить из f_1 путём введения и удаления некоторых фиктивных аргументов.

Если задана конечная система функций из P_2: $\{f_1,\ldots,f_s\}$, $s\geq 1$, то можно считать, что все эти функции зависят от одних и тех же переменных x_1, ..., x_n, т. е. имеют вид $f_1(x_1,\ldots,x_n)$, ..., $f_s(x_1,\ldots,x_n)$.

Приведём примеры наиболее употребительных булевых функций. В таблице 1.2 приведены все функции одной переменной, т. е. функций из $P_2^{(1)}$. В таблице 1.2 приведены функции из из $P_2^{(2)}$.

x	0	1	f_1	f_2
0	0	1	0	1
1	0	1	1	0

Таблица 2. Функции одной переменной.

x_1	x_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9
0	0	0	0	0	1	1	1	1
0	1	0	1	1	0	1	1	0
1	0	0	1	1	0	0	1	0
1	1	1	1	0	1	1	0	0

Таблица 3. Функции двух переменных.

- Функция 0 называется (*тождественным*) *нулём.*
- Функция 1 называется (*тождественной*) *единицей.*
- Функция f_1 называется *тождественной функцией* и обозначается через x;
- Функция f_2 называется *отрицанием*, обозначается $\overline{x}$ или $\neg x$.
- Функция f_3 называется *конъюнкцией* x_1 и x_2, обозначается $x_1 \wedge x_2$. Вместо знака $\wedge$ также употребляются знаки $\cdot$, & или вообще знак опускается, т. е. пишут $x_1 x_2$. Эту функцию часто называют *логическим умножением.* Заметим, что $x_1 \wedge x_2 = \min(x_1, x_2)$.
- Функция f_4 называется *дизъюнкцией* x_1 и x_2, обозначается $x_1 \vee x_2$. Эту функцию часто называют *логическим сложением.* Заметим, что $x_1 \vee x_2 = \max(x_1, x_2)$.
- Функция f_5 называется *сложением по модулю* 2 x_1 и x_2, обозначается $x_1 \oplus x_2$ или $x_1 + x_2$.
- Функция f_6 называется *эквиваленцией* x_1 и x_2, обозначается $x_1 \sim x_2$ или $x_1 \leftrightarrow x_2$.
- Функция f_7 называется *импликацией* x_1 и x_2, обозначается $x_1 \to x_2$. Эту функцию часто называют *логическим следованием*;

- Функция f_8 называется *функцией Шеффера* x_1 и x_2, обозначается $x_1|\,x_2$.
- Функция f_9 называется *стрелкой Пирса* x_1 и x_2, обозначается $x_1\downarrow x_2$.

Функции f_1 — f_9 будем называть *элементарными*.

Символы $\neg$, $\wedge$, $\vee$, $\oplus$, $\sim$, $\to$, $|$, $\downarrow$, участвующие в обозначениях элементарных функций, называются *логическими связками* (или просто *связками*).

Для любого натурального n и любого i, $1 \le i \le n$, обозначим через $e_i^n(x_1, \ldots, x_n)$ *селекторную* функцию, значения которой совпадают со значениями переменной x_i. Вместо функции $e_i^n(x_1, \ldots, x_n)$ часто пишут просто x_i.

Задачи.

1. Представить заданную функцию f в виде истинностной таблицы и указать все фиктивные переменные:

1) $f(\widetilde{x}^3) = (10101010)$; 2) $f(\widetilde{x}^3) = (01100110)$;
3) $f(\widetilde{x}^3) = (11110011)$; 4) $f(\widetilde{x}^4) = (1011010110110101)$.

Решение. 4) Запишем таблицу истинности для $f(x_1, x_2, x_3)$.

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	0

Легко видеть, что переменная x_1 является фиктивной. Пусть $f_1(x_2, x_3) = (1010)$. Запишем таблицу истинности для $f_1(x_2, x_3)$.

x_2	x_3	$f(x_1, x_2, x_3)$
0	0	1
0	1	0
1	0	1
1	1	0

Очевидно, что переменная x_2 является фиктивной. Пусть $f_2(x_3) = (10)$. Переменная x_3 существенная. В результате переменные x_1 и x_2 фиктивные, а x_3 существенная. ■

1.3. Формулы и реализация булевых функций формулами

Зафиксируем некоторый алфавит переменных X (конечный или счётно-бесконечный). Пусть $\mathcal{F} = \{f_1^{(n_1)}, f_2^{(n_2)}, \ldots\}$ — непустое множество функциональных символов. Верхние индексы здесь указывают число аргументов (местность) функциональных символов. Верхние индексы часто опускаются, но при этом местности предполагаются известными.

Формула над множеством $\mathcal{F}$ определяется индукцией по построению.

1) *Базис индукции.* Выражения вида f_k и $f_j(x_{i_1}, \ldots, x_{i_n})$ являются *формулами над* $\mathcal{F}$. Здесь f_k — нульместный, f_j — n-местный ($n \geq 1$) функциональные символы, $x_{i_1}, \ldots, x_{i_n}$ — переменные из множества X.

2) *Индуктивный переход.* Пусть $f_m \in \mathcal{F}$ — s-местный ($s \geq 1$) функциональный символ и каждое H_i, $i = 1, \ldots, s$, есть либо формула над $\mathcal{F}$, либо переменная из множества X. Тогда выражение $f_m(H_1, \ldots, H_m)$ является формулой над $\mathcal{F}$.

3) Только те объекты называются формулами над $\mathcal{F}$, которые можно построить с помощью пунктов 1) и 2).

В алгебре логики в качестве связок употребляют символы из множества

$$\Upsilon = \{\, \neg, \wedge, \vee, \oplus, \sim, \to, |, \downarrow \,\}.$$

Формулой над множеством Υ называется всякое выражение вида:

1) x — любая переменная из множества X;

2) $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \oplus B)$, $(A \sim B)$, $(A \to B)$, $(A \,|\, B)$, $(A \downarrow B)$, где A, B — формулы над Υ.

Для сокращения записи формул над множеством Υ используют соглашения:

а) внешние скобки у формул опускаются;

б) формула $(\neg A)$ записывается как $\overline{A}$;

в) формула $(A \wedge B)$ записывается как $(A \cdot B)$ или (AB);

г) связка $\neg$ сильнее любой связки из Υ;

д) связка $\wedge$ сильнее любой двухместной связки из Υ.

Пример 1. Пусть $\mathcal{F} = \{\vee, \to\}$, $X = \{x_1, x_2, x_3\}$. Выражения

$$((x_2 \to x_3) \to (x_3 \vee x_1)), \quad (x_2 \to ((x_1 \to x_2) \vee x_3))$$

являются формулами над $\mathcal{F}$.

Запись

$$A[f_1, \ldots, f_s]$$

будет означать, что формула A построена из функций $f_1, \ldots, f_s$. В случаях, когда нужно обратить внимание на переменные, участвующие в построении формулы, пишут

$$A(x_1, \ldots, x_n).$$

Пусть A — произвольная формула над $\mathcal{F}$, тогда формулы, которые использовались для её построения, называются *подформулами* формулы A.

Пусть каждому функциональному символу $f_i^{(n_i)}$ из множества $\mathcal{F} = \{f_1^{(n_1)}, f_2^{(n_2)}, \ldots\}$ сопоставлена функция

$$F_i : E_2^{(n_i)} \to E_2.$$

Каждой формуле A над $\mathcal{F}$ сопоставим функцию φ_A из P_2, опираясь на индуктивное определение формул.

1) *Базис индукции.* Если $A = f_i^{(n_i)}(x_{j_1}, \ldots, x_{j_{n_i}})$, то для всякого набора $(\alpha_1, \ldots, \alpha_{n_i})$ значений переменных $x_{j_1}, \ldots, x_{j_{n_i}}$ значение функции φ_A равно $F_i(\alpha_1, \ldots, \alpha_{n_i})$.

2) *Индуктивный переход.* Если $A = A(y_1, \ldots, y_k) = f(H_1, \ldots, H_m)$, где $f \in \mathcal{F}$ и H_i, $i = 1, \ldots, m$, является либо формулой над $\mathcal{F}$, либо переменной из X. Тогда

$$\varphi_A(\alpha_1, \ldots, \alpha_k) = F(\beta_1, \ldots, \beta_m),$$

где F — функция, сопоставленная функциональному символу f и

$$\beta_p = \begin{cases} \alpha_q, & \text{если } H_p = y_q, \\ \varphi_{A_p}(\alpha_1, \ldots, \alpha_{p_s}), & \text{если } H_p = H_p(y_1, \ldots, y_{p_s}) \end{cases}$$

для $p = 1, \ldots, m$. Здесь s зависит, естественно, от p.

Если функция f соответствует формуле A, то говорят также, что формула A *реализует функцию* f.

Пусть функция f реализуется формулой $A[f_1, \ldots, f_s]$. Тогда говорят, что функция f является *суперпозицией* функций $f_1, \ldots, f_s$.

Формулы A и B над $\mathcal{F}$ называются *эквивалентными*, если соответствующие им функции f_A и f_B равны, т. е. $f_A = f_B$. Запись $A = B$ будет означать, что формулы A и B эквивалентными.

Для функций от одной и двух переменных, определённых в п. 1.2, существует большое число связывающих их эквивалентностей. Ниже приведены наиболее употребительные из них.

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

2. $\overline{0} = x \vee 1 = x \vee \overline{x} = x \to x = 1$.

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

4. $x \oplus 1 = x \to 0 = x \,|\, x = \overline{x}$.

5. $x \circ y = y \circ x$, где $\circ$ есть любая из функций $\cdot$, $\vee$, $\oplus$ (*коммутативность* функции $\circ$).

6. $(x \circ y) \circ z = x \circ (y \circ z)$, где $\circ$ есть любая из функций $\cdot$, $\vee$, $\oplus$ (*ассоциативность* функции $\circ$).

7. $x \cdot (y \vee z) = (x \cdot y) \vee (x \cdot z)$ (*дистрибутивность* конъюнкции относительно дизъюнкции).

8. $x \vee (y \cdot z) = (x \vee y) \cdot (x \vee z)$ (*дистрибутивность* дизъюнкции относительно конъюнкции).

9. $x \cdot (y \oplus z) = (x \cdot y) \oplus (x \cdot z)$ (*дистрибутивность* конъюнкции относительно $\oplus$).

10. $\overline{x \cdot y} = \overline{x} \vee \overline{y}$, $\overline{x \vee y} = \overline{x} \cdot \overline{y}$ (*законы де Моргана*).

11. $x \vee (x \cdot y) = x \cdot (x \vee y) = x$ (*правила поглощения*).

12. $x \oplus 1 = x \to 0 = x \,|\, x = \overline{x}$,
$x \vee y = ((x \cdot y) \oplus x) \oplus y = \overline{x} \to y$,
$x \to y = \overline{x} \vee y = ((x \cdot y) \oplus x) \oplus 1$,
$x \,|\, y = \overline{x \cdot y}$.

Справедливость эквивалентностей 1 — 12 проверяется непосредственно пр помощи таблиц 1 — 3.

Задачи.

1. Выяснить, какие из нижеприводимых выражений являются формулами над множеством логических связок $S = \{\neg, \wedge, \vee, \oplus, \sim, \to\}$. Проверить, можно ли некоторые из приведённых ниже выражений, не являющиеся формулами над S, превратить в формулы, добавляя скобки:

1) $x \vee (\neg y)$; 2) $x \oplus (\wedge y)$;

3) $(x \vee y) \to (x \oplus (\neg z))$; 4) $\neg(x \to ((\neg x) \wedge y))$;

5) $(x \sim y)\, \neg y$; 6) $(\neg x \to y)$.

2. Выяснить, является ли выражение A формулой над множеством $\mathcal{F}$. Проверить, можно ли, добавляя скобки, запятые и переменные, превратить некоторые из приведённых ниже выражений в формулы над соответствующими множествами $\mathcal{F}$:

1) $A = g^{(1)}(f^{(2)}(1, x))$, $\mathcal{F} = \{f^{(2)}, g^{(1)}\}$;

2) $A = f^{(2)}(g^{(2)}(xy), h^{(2)}(1, y))$, $\mathcal{F} = \{1, f^{(2)}, g^{(2)}, h^{(2)}\}$;
3) $A = h^{(1)}(f^{(2)}(g^{(2)}(x, h^{(1)}(x)), h^{(1)}(y)))$, $\mathcal{F} = \{0, f^{(2)}, g^{(2)}, h^{(1)}\}$;
4) $A = (\varphi^{(1)}(f^{(2)}(x, \varphi^{(1)}(x))))$, $\mathcal{F} = \{f^{(2)}, \varphi^{(1)}\}$.

1.4. Разложения булевых функций по переменным

Введём обозначение

$$x^{\sigma} = x\sigma \vee x\overline{\sigma},$$

где параметр σ равен 0 или 1. Легко проверить, что

$$x^{\sigma} = \begin{cases} \overline{x} & \text{при } \sigma = 0, \\ x & \text{при } \sigma = 1. \end{cases} \tag{1}$$

Отсюда следует, что $x^{\sigma} = 1$ тогда и только тогда, когда $x = \sigma$.

Пусть задан алфавит переменных $\{x_1, \ldots, x_n\}$. Выражение

$$K = x_{i_1}^{\sigma_1} \wedge \ldots \wedge x_{i_r}^{\sigma_r}, \quad i_\nu \neq i_\mu \text{ при } \nu \neq \mu.$$

называется *элементарной конъюнкцией*. Число r называется *рангом элементарной конъюнкции*. По определению константа 1 считается элементарной конъюнкцией ранга 0.

Выражение

$$\bigvee_{i=1}^{s} K_i, \quad K_i \neq K_j \text{ при } i \neq j.$$

где K_i, $i = 1, \ldots, s$, является элементарной конъюнкцией ранга r_i, называется *дизъюнктивной нормальной формой* (сокращённо ДНФ).

Дизъюнктивная нормальная форма $K_1 \vee \ldots \vee K_s$ называется *совершенной дизъюнктивной нормальной формой* (сокращённо СДНФ), если каждая элементарная конъюнкция K_i, $i = 1, \ldots, s$, имеет ранг n.

Выражение

$$D = x_{i_1}^{\sigma_1} \vee \ldots \vee x_{i_r}^{\sigma_r}, \quad i_\nu \neq i_\mu \text{ при } \nu \neq \mu.$$

называется *элементарной дизъюнкцией*. Число r называется *рангом элементарной дизъюнкции*. По определению константа 0 считается элементарной дизъюнкцией ранга 0.

Выражение

$$\bigwedge_{i=1}^{s} D_i, \quad D_i \neq D_j \text{ при } i \neq j.$$

где D_i, $i = 1, \ldots, s$, является элементарной дизъюнкцией ранга r_i, называется *конъюнктивной нормальной формой* (сокращённо КНФ).

Конъюнктивная нормальная форма $D_1 \wedge \ldots \wedge D_s$ называется *совершенной конъюнктивной нормальной формой* (сокращённо СКНФ), если каждая элементарная дизъюнкция D_i, $i = 1, \ldots, s$, имеет ранг n.

Теорема 1 (о разложении функций по переменным). *Каждую булеву функцию $f(x_1, \ldots, x_n)$ при любом m, $1 \le m \le n$, можно представить в следующей форме*:

$$f(x_1, \ldots, x_m, x_{m+1}, \ldots, x_n) = \\ = \bigvee_{(\sigma_1, \ldots, \sigma_m)} x_1^{\sigma_1} \wedge \ldots \wedge x_m^{\sigma_m} \wedge f(\sigma_1, \ldots, \sigma_m, x_{m+1}, \ldots, x_n), \quad (2)$$

где дизъюнкция берётся по всевозможным наборам значений переменных $(\sigma_1, \ldots, \sigma_m)$.

Доказательство. Рассмотрим произвольный набор значений переменных $(\alpha_1, \ldots, \alpha_n)$. Левая часть (2) равна $f(\alpha_1, \ldots, \alpha_n)$. Правая —

$$\bigvee_{(\sigma_1, \ldots, \sigma_m)} \alpha_1^{\sigma_1} \wedge \ldots \wedge \alpha_m^{\sigma_m} \wedge f(\sigma_1, \ldots, \sigma_m, \alpha_{m+1}, \ldots, \alpha_n).$$

Т. к. $\alpha_i^{\sigma_i} = 1$ тогда и только тогда, когда $\alpha_i = \sigma_i$, то правая часть равна

$$\alpha_1^{\alpha_1} \wedge \ldots \wedge \alpha_m^{\alpha_m} \wedge f(\alpha_1, \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_n) = f(\alpha_1, \ldots, \alpha_n). \qquad \blacksquare$$

Следствие 1 (разложение по переменной).

$$f(x_1, \ldots, x_{n-1}, x_n) = (x_n \wedge f(x_1, \ldots, x_{n-1}, 1)) \vee (\overline{x}_n \wedge f(x_1, \ldots, x_{n-1}, 0)).$$

Следствие 2 (разложение по всем переменным). *Если булева функция $f(x_1, \ldots, x_n)$ не равна тождественно* 0*, то справедливо представление*

$$f(x_1, \ldots, x_n) = \bigvee_{\substack{(\sigma_1, \ldots, \sigma_n) \\ f(\sigma_1, \ldots, \sigma_n) = 1}} x_1^{\sigma_1} \wedge \ldots \wedge x_n^{\sigma_n}. \quad (3)$$

Доказательство. Запишем формулу (2) при $m = n$:

$$f(x_1, \ldots, x_n) = \bigvee_{(\sigma_1, \ldots, \sigma_n)} x_1^{\sigma_1} \wedge \ldots \wedge x_n^{\sigma_n} \wedge f(\sigma_1, \ldots, \sigma_n).$$

При $f(x_1, \ldots, x_n) \not\equiv 0$ оно может быть преобразовано:

$$\bigvee_{(\sigma_1, \ldots, \sigma_n)} x_1^{\sigma_1} \wedge \ldots \wedge x_n^{\sigma_n} \wedge f(\sigma_1, \ldots, \sigma_n) = \bigvee_{\substack{(\sigma_1, \ldots, \sigma_n) \\ f(\sigma_1, \ldots, \sigma_n) = 1}} x_1^{\sigma_1} \wedge \ldots \wedge x_n^{\sigma_n}.$$

В результате получим (3). ■

Разложение (3) является совершенной дизъюнктивной нормальной формой.

Пример 1. Представим в виде СДНФ функцию $x_1 \to x_2$. Данная функция равна 1 на наборах $(0,0)$, $(0,1)$ и $(1,1)$. Следовательно

$$x_1 \to x_2 = \overline{x}_1\overline{x}_2 \vee \overline{x}_1 x_2 \vee x_1 x_2.$$

Аналогично доказывается следующая теорема.

Теорема 1′ (о разложении функций по переменным). *Каждую булеву функцию $f(x_1, \ldots, x_n)$ при любом m, $1 \le m \le n$, можно представить в следующей форме*:

$$f(x_1, \ldots, x_m, x_{m+1}, \ldots, x_n) = \\ = \bigwedge_{(\sigma_1,\ldots,\sigma_m)} x_1^{\sigma_1} \vee \ldots \vee x_m^{\sigma_m} \vee f(\sigma_1, \ldots, \sigma_m, x_{m+1}, \ldots, x_n), \quad (4)$$

где конъюнкция берётся по всевозможным наборам значений переменных $(\sigma_1, \ldots, \sigma_m)$.

Следствие 1′ (разложение по переменной).

$$f(x_1, \ldots, x_{n-1}, x_n) = (x_n \vee f(x_1, \ldots, x_{n-1}, 1)) \wedge (\overline{x}_n \vee f(x_1, \ldots, x_{n-1}, 0)).$$

Следствие 2′ (разложение по всем переменным). *Если булева функция $f(x_1, \ldots, x_n)$ не равна тождественно* 1, *то справедливо представление*

$$f(x_1, \ldots, x_n) = \bigwedge_{\substack{(\sigma_1,\ldots,\sigma_n) \\ f(\sigma_1,\ldots,\sigma_n)=0}} x_1^{\sigma_1} \vee \ldots \vee x_n^{\sigma_n}. \quad (5)$$

Разложение (5) является совершенной конъюнктивной нормальной формой.

Пример 2. Представим в виде СКНФ функцию $x_1 \to x_2$. Данная функция равна 0 на наборе $(1,0)$. Следовательно

$$x_1 \to x_2 = \overline{x}_1 \vee x_2.$$

Задачи.

1. Провести полные доказательства теоремы 1′ и следствий 1′, 2′.

2. Представить в виде СДНФ и СКНФ следующие функции:

1) $f(\widetilde{x}^3) = (x_1 \vee x_2) \to x_3$; 2) $f(\widetilde{x}^3) = (x_1 \oplus x_2) \to x_2 x_3$;
3) $f(\widetilde{x}^3) = (01101100)$; 4) $f(\widetilde{x}^3) = (10001110)$.

1.5. Полнота и замкнутость

Система функций $F \subset P_2$ называется (*функционально*) *полной*, если любая булева функция может быть представлена в виде формулы через функции системы F.

Теорема 1. *Система функций* $\{\neg, \wedge, \vee\}$ *является полной.*

Доказательство. Пусть $f(x_1, \ldots, x_n) \equiv 0$. Тогда

$$f(x_1, \ldots, x_n) = x_1 \wedge \overline{x}_1.$$

Пусть $f(x_1, \ldots, x_n) \not\equiv 0$. Представим её в виде СДНФ.:

$$f(x_1, \ldots, x_n) = \bigvee_{\substack{(\sigma_1,\ldots,\sigma_n) \\ f(\sigma_1,\ldots,\sigma_n)=1}} x_1^{\sigma_1} \wedge \ldots \wedge x_n^{\sigma_n}.$$

Следовательно, в любом случае функция f выражается в виде формулы через отрицание, конъюнкцию и дизъюнкцию. ■

Теорема 2. *Пусть* $F = \{f_1, f_2, \ldots\}$ *и* $G = \{g_1, g_2, \ldots\}$ *системы булевых функций. Пусть* F *полная система и любая функция из* F *выражается в виде формулы над системой* G*. Тогда* G *является полной системой.*

Доказательство. Рассмотрим произвольную булеву функцию h. Так как система F полная система, то функцию h можно выразить в виде формулы над F:

$$h = C\,[f_1, f_2, \ldots].$$

В скобках выписаны все функции системы F, хотя фактически их в формуле конечное число. По условию теоремы

$$f_i = C_i[g_1, g_2, \ldots], \quad i = 1, 2, \ldots.$$

Заменим в формуле $C\,[f_1, f_2, \ldots]$ вхождения функций f_1, f_2, $\ldots$, заменив их формулами над G. Получим

$$C\,[f_1, f_2, \ldots] = C\,[\,C_1[g_1, g_2, \ldots], C_2[g_1, g_2, \ldots], \ldots].$$

Последнее выражение определяет формулу над G со строением C'. В результате

$$C\,[\,C_1[g_1, g_2, \ldots], C_2[g_1, g_2, \ldots], \ldots] = C'[g_1, g_2, \ldots].$$

Таким образом,

$$h = C'[g_1, g_2, \ldots],$$

т. е. функция h представляется формулой над G. ■

Теорема 3. *Следующие системы булевых функций являются полными в* P_2:

1) $\{\vee,\ \neg\}$;

2) $\{\wedge,\ \neg\}$;

3) $\{|\}$;

4) $\{\wedge,\ \oplus,\ 1\}$;

Доказательство. 1) Из теоремы 1 следует, что система $F = \{\neg,\ \wedge,\ \vee\}$ полна. Из закона де Моргана $\overline{x \wedge y} = \overline{x} \vee \overline{y}$ выводим, что $x \wedge y = \overline{\overline{x} \vee \overline{y}}$. Таким образом, все функции системы F можно выразить формулами над системой $G = \{\vee,\ \neg\}$. Из теоремы 2 заключаем, что система G полна.

2) Как и в пункте 1) из закона де Моргана получаем, что $x \vee y = \overline{\overline{x} \wedge \overline{y}}$ и затем пользуемся теоремой 2.

3) Нетрудно видеть, что

$$\overline{x} = x\,|\,x, \quad x \wedge y = \overline{x\,|\,y} = (x\,|\,y)\,|\,(x\,|\,y).$$

Следовательно, из пункта 2) и теоремы 2 вытекает полнота системы 3).

4) Так как $\overline{x} = x \oplus 1$, то полнота системы 3) следует из пункта 2) и теоремы 2. ■

Пусть F — некоторое непустое множество булевых функций. *Замыканием* F называется множество всех булевых функций, представимых через функции множества F. Замыкание множества F обозначается через $[F]$.

Теорема 4 (свойства замыкания). *Операция замыкания обладает свойствами*:

1) $[F] \supset F$;

2) $[[F]] = [F]$;

3) если $F_1 \subset F_2$, то $[F_1] \subset [F_2]$;

4) $[F_1 \cup F_2] \supset [F_1] \cup [F_2]$.

Доказательство. Элементарно. ■

Пусть $F \subset P_2$. Если выполняется равенство $F = [F]$, то F называется *замкнутым классом* или *классом Поста.*

Простейшим примером замкнутого класса является P_2. Нетрудно доказать следующее утверждение.

Теорема 5. Пересечение конечного числа замкнутых классов является замкнутым классом.

Доказательство. Так как $F_1 \cap F_2 \subset F_1$ и $F_1 \cap F_2 \subset F_2$, то $[F_1 \cap F_2] \subset F_1$ и $[F_1 \cap F_2] \subset F_2$, в силу свойства 3) и замкнутости F_1 и F_2. Следовательно,

$[F_1 \cap F_2] \subset F_1 \cap F_2$. Пользуясь свойством 1), заключаем отсюда, что $[F_1 \cap F_2] = F_1 \cap F_2$. ■

В терминах замыкания и замкнутого класса можно дать эквивалентное определение полноты: F — полная система, если $[F] = P_2$.

Задачи.

1. Сведением к заведомо полным системам в P_2 показать, что множество A является полной системой в P_2:

1) $A = \{x \downarrow y\}$;
2) $A = \{x \to y, \overline{x \oplus y \oplus z}\}$;
3) $A = \{xy \oplus z, (x \sim y) \oplus z\}$;
4) $A = \{x \to y, f = (01011110)\}$.

2. Является ли множество A замкнутым классом:

1) $A = \{0, 1\}$; 2) $A = \{x\}$; 3) $A = \{1, x\}$;
4) $A = \{0, x_1 \vee x_2 \vee \ldots \vee x_n,\ n \geq 1\}$;
5) $A = \{x_1 \oplus x_2 \oplus \ldots \oplus x_n,\ n \geq 1\}$.

3. Показать, что $f \in [A]$, выразив f формулой над множеством A:

1) $f = \overline{x}$, $A = \{0, x \to y\}$;
2) $f = x$, $A = \{x \oplus y\}$;
3) $f = x \oplus y \oplus z$, $A = \{x \sim y\}$;
4) $f = x \vee y$, $A = \{\overline{x} \vee \overline{y}\}$;
5) $f = xy$, $A = \{xy \oplus y\}$.

1.6. Полиномы Жегалкина

Монотонной конъюнкцией от переменных $x_1, \ldots, x_n$ называется формула 1, а также любая формула вида

$$x_{i_1} \cdot x_{i_2} \cdot \ldots \cdot x_{i_s}, \tag{1}$$

где $s \geq 1$, $1 \leq i_k \leq n$ для всех $k = 1, \ldots, s$, причём все переменные различны. В силу коммутативности конъюнкции порядок переменных в (1) не имеет значения.

Полиномом Жегалкина над $x_1, \ldots, x_n$ называется формула 0, а также любая формула вида

$$\bigoplus_{j=1}^{m} K_j = K_1 \oplus K_2 \oplus \ldots \oplus K_m, \tag{2}$$

где $m \geq 1$ и все K_j — различные монотонные конъюнкции от переменных $x_1, \ldots, x_n$. Так как операция $\oplus$ коммутативна, то порядок слагаемых в (2) не имеет значения.

Теорема 1 (теорема Жегалкина). *Любую булеву функцию $f(x_1, \ldots, x_n)$ можно единственным образом представить в виде полинома Жегалкина над $x_1, \ldots, x_n$.*

Доказательство. *Существование.* В силу теоремы 5.3 система $\{1, x \cdot y, x \oplus y\}$ полна. Следовательно, всякую булеву функцию $f(x_1, \ldots, x_n)$ можно реализовать формулой над $\{1, x \cdot y, x \oplus y\}$.

а) Пользуясь дистрибутивностью, раскрываем все скобки в этой реализации и получаем, что

$$f(x_1, \ldots, x_n) = K'_1 \oplus K'_2 \oplus \ldots \oplus K'_m,$$

где любая K'_j — конъюнкция переменных и единиц.

б) Пользуясь коммутативностью и соотношениями

$$x \cdot x = x, \quad 1 \cdot 1 = 1, \quad A \cdot 1 = A,$$

преобразуем все полученные конъюнкции в монотонные.

в) Пользуясь соотношениями

$$A \oplus A = 0, \quad A \oplus 0 = A,$$

преобразуем полученную сумму в полином Жегалкина. Существование доказано.

Единственность. Найдём число различных всевозможных монотонных конъюнкций от n переменных. Ясно, что оно количеству различных подмножеств множества $\{1, \ldots, n\}$. Монотонной конъюнкции $x_{i_1} \cdot x_{i_2} \cdot \ldots \cdot x_{i_s}$, например, соответствует подмножество $\{i_1, \ldots i_s\} \subset \{1, \ldots, n\}$, а 1 соответствует пустое множество $\varnothing$. Из элементарной комбинаторики известно, что это число равно 2^n.

Далее, полином Жегалкина однозначно определяется входящими в него монотонными конъюнкциями (различными). Пустому множеству конъюнкций соответствует нулевой полином Жегалкина. Таким образом, количество полиномов Жегалкина равно числу различных подмножеств множества монотонных конъюнкций, т. е. 2^{2^n}.

Мы получили, что число различных полиномов Жегалкина совпадает с числом всех булевых функций. Из доказанного выше, отображение из множества полиномов Жегалкина во множество булевых функций сюръективно. Следовательно, это отображение биективно. Единственность доказана. ■

Нетрудно видеть, что произвольный полиномов Жегалкина $P(\widetilde{x}^n)$ можно записать в виде

$$P(\widetilde{x}^n) = a_0 \oplus \bigoplus_{i_1 \ldots i_s} a_{i_1 \ldots i_s} \cdot x_{i_1} \cdot x_{i_2} \cdot \ldots \cdot x_{i_s}, \tag{3}$$

где суммирование производится по всем непустым подмножествам $\{i_1, \ldots i_s\} \subset \{1, \ldots, n\}$, а коэффициенты a_0, $a_{i_1 \ldots i_s}$ принимают значения 0 или 1.

Введём специальную нумерацию монотонных конъюнкций от переменных $x_1, \ldots, x_n$. Монотонной конъюнкции K сопоставим вектор $\widetilde{\sigma}(K) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\} \in B^n$, в котором $\sigma_i = 1$ тогда и только тогда, когда x_i входит в K. *Номером монотонной конъюнкции* называется число $\nu(\widetilde{\sigma}(K)) = \sum_{i=1}^{n} \sigma_i \cdot 2^{n-i}$. Константа 1 в этой нумерации будет иметь номер 0. Используя введённую нумерацию, (3) можно записать в виде

$$P(\widetilde{x}^n) = \beta_0 \cdot 1 \oplus \beta_1 \cdot K_1 \oplus \ldots \oplus \beta_{2^n-1} \cdot K_{2^n-1}. \tag{4}$$

Опишем метод построения полинома Жегалкина. Пусть $P(\widetilde{x}^n)$ — искомый полином, реализующий заданную функцию $f(\widetilde{x}^n)$. Представим его в виде (4) с неизвестными коэффициентами β_i. для каждого $\widetilde{\alpha} \in B^n$ составляем уравнение $P(\widetilde{\alpha}) = f(\widetilde{\alpha})$. В результате получим систему из 2^n уравнений с 2^n неизвестными. Эта система всегда имеет единственное решение. Решив её, находим коэффициенты полинома $P(\widetilde{x}^n)$. Описанный метод называется *методом неопределённых коэффициентов*.

Пример 1. Методом неопределённых коэффициентов построим полином Жегалкина для функции $f(x, y) = x \vee y$. Пусть

$$P(x, y) = \beta_0 \oplus \beta_1 \cdot x \oplus \beta_2 \cdot y \oplus \beta_3 \cdot xy.$$

Выписываем систему уравнений для коэффициентов β_0, β_1, β_2, β_3.

$$\begin{cases} f(0,0) = 0 = \beta_0 \oplus \beta_1 \cdot 0 \oplus \beta_2 \cdot 0 \oplus \beta_3 \cdot 0, \\ f(0,1) = 1 = \beta_0 \oplus \beta_1 \cdot 0 \oplus \beta_2 \cdot 1 \oplus \beta_3 \cdot 0, \\ f(1,0) = 1 = \beta_0 \oplus \beta_1 \cdot 1 \oplus \beta_2 \cdot 0 \oplus \beta_3 \cdot 0, \\ f(1,1) = 1 = \beta_0 \oplus \beta_1 \cdot 1 \oplus \beta_2 \cdot 1 \oplus \beta_3 \cdot 1. \end{cases}$$

Эта система эквивалентна следующей

$$\begin{cases} \beta_0 = 0, \\ \beta_0 \oplus \beta_2 = 1, \\ \beta_0 \oplus \beta_1 = 1, \\ \beta_0 \oplus \beta_1 \oplus \beta_2 \oplus \beta_3 = 1. \end{cases}$$

Получаем $\beta_0 = 0$, $\beta_0 = \beta_1 = \beta_2 = \beta_3 = 0$. В результате

$$x \vee y = x \oplus y \oplus xy.$$

Задачи.

1. Методом неопределённых коэффициентов найти полиномы Жегалкина для следующих функций:

1) $f(\widetilde{x}^3) = (01101001)$;
2) $f(\widetilde{x}^3) = (10001110)$;
3) $f(\widetilde{x}^3) = (00000111)$.

2. Методом неопределённых коэффициентов найти полиномы Жегалкина для следующих функций:

1) $f(\widetilde{x}^2) = x_1 \,|\, x_2$;
2) $f(\widetilde{x}^3) = x_1(x_2 \vee x_3)$;
3) $f(\widetilde{x}^3) = x_1 \to (x_2 \to x_3)$.

2. Замкнутые классы и критерий полноты

2.1. Принцип двойственности. Класс самодвойственных функций

Функция $g(x_1, \ldots, x_n)$ называется *двойственной* к функции $f(x_1, \ldots, x_n)$, если

$$g(x_1, \ldots, x_n) = \overline{f}(\overline{x}_1, \ldots, \overline{x}_n). \tag{1}$$

Функция, двойственная к функции $f(x_1, \ldots, x_n)$, обозначается через $f^*(x_1, \ldots, x_n)$.

Из определения (1) и тождества $\overline{\overline{x}} = x$ следует, что

$$f^{**}(x_1, \ldots, x_n) = f(x_1, \ldots, x_n). \tag{2}$$

Таким образом, двойственные друг к другу функции образуют пары, некоторые из которых приведены в таблице 1.

f	f^*
0	1
x	x
$\overline{x}$	$\overline{x}$
$e_i^n(x_1, \ldots, x_n)$	$e_i^n(x_1, \ldots, x_n)$
$x \wedge y$	$x \vee y$
$x \oplus y$	$x \oplus y \oplus 1 = \overline{x \oplus y}$
$x \to y$	$\overline{x \vee \overline{y}} = \overline{x} \wedge y = \overline{y \to x}$
$x \,\|\, y$	$\overline{x \wedge y} = \overline{x} \vee \overline{y}$

Таблица 1.

Обозначим через $x_1, \ldots, x_n$ все различные символы переменных, встречающихся в множествах

$$(x_{11}, \ldots, x_{1p_1}), \ldots, (x_{m1}, \ldots, x_{mp_m}).$$

Теорема 1. *Если*

$$g(x_1, \ldots, x_n) = f(f_1(x_{11}, \ldots, x_{1p_1}), \ldots, f_m(x_{m1}, \ldots, x_{mp_m})), \tag{3}$$

то

$$g^*(x_1, \ldots, x_n) = f^*(f_1^*(x_{11}, \ldots, x_{1p_1}), \ldots, f_m^*(x_{m1}, \ldots, x_{mp_m})),$$

Доказательство. Из определения двойственной функции имеем

$$g^*(x_1, \ldots, x_n) = \overline{f}(f_1(\overline{x}_{11}, \ldots, \overline{x}_{1p_1}), \ldots, f_m(\overline{x}_{m1}, \ldots, \overline{x}_{mp_m})).$$

В правой части этого равенства каждую формулу $f_i(\overline{x}_{i1}, \ldots, \overline{x}_{ip_i})$, $i = 1, \ldots, m$, заменим эквивалентной формулой $\overline{\overline{f}}_i(\overline{x}_{i1}, \ldots, \overline{x}_{ip_i})$. Тогда

$$g^*(x_1, \ldots, x_n) = \overline{f}(\overline{\overline{f}}_1(\overline{x}_{11}, \ldots, \overline{x}_{1p_1}), \ldots, \overline{\overline{f}}_m(\overline{x}_{m1}, \ldots, \overline{x}_{mp_m})).$$

Функция $\overline{f}_i(\overline{x}_{i1}, \ldots, \overline{x}_{ip_i})$ по определению есть функция $f_i^*(x_{i1}, \ldots, x_{ip_i})$. Следовательно

$$g^*(x_1, \ldots, x_n) = \overline{f}(\overline{f}_1^*(x_{11}, \ldots, x_{1p_1}), \ldots, \overline{f}_m^*(x_{m1}, \ldots, x_{mp_m})).$$

Из определения двойственной функции получаем, что $\overline{f}(\overline{f}_1^*, \ldots, \overline{f}_m^*)$ есть $f^*(f_1^*, \ldots, f_m^*)$. Окончательно приходим к равенству

$$g^*(x_1, \ldots, x_n) = f^*(f_1^*(x_{11}, \ldots, x_{1p_1}), \ldots, f_m^*(x_{m1}, \ldots, x_{mp_m})).$$

Теорема доказана. ■

Из теоремы вытекает

Принцип двойственности. *Если формула $\mathcal{F} = C[f_1, \ldots, f_s]$ реализует функцию $f(x_1, \ldots, x_n)$, то формула $C[f_1^*, \ldots, f_s^*]$, т. е. формула, полученная из $\mathcal{F}$ заменой функций f_1, …, f_s на f_1^*, …, f_s^*, реализует функцию $f^*(x_1, \ldots, x_n)$.*

Эта формула называется *формулой, двойственной к $\mathcal{F}$*, и обозначается через $\mathcal{F}^*$. Таким образом,

$$\mathcal{F}^* = C[f_1^*, \ldots, f_s^*].$$

Булева функция $f(x_1, \ldots, x_n)$ называется *самодвойственной*, если

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

Обозначим через S класс всех самодвойственных функций.

Пример 1. Из таблицы 1 видно, что Функции x, $\overline{x}$, $e_i^n(x_1, \ldots, x_n)$ являются самодвойственными, т. е. принадлежат классу S, а функции 0, $x_1 \wedge x_2$, $x_1 \vee x_2$ не принадлежат классу S.

Пример 2. Покажем, что функция $m(x, y, z) = xy \vee xz \vee yz$ принадлежат классу S, Имеем

$$m^*(x, y, z) = (x \vee y)(x \vee z)(y \vee z) = xy \vee xz \vee yz = m(x, y, z).$$

Для самодвойственной функции справедливо тождество

$$\overline{f}(\overline{x}_1, \ldots, \overline{x}_n) = f(x_1, \ldots, x_n). \tag{4}$$

Следовательно, на противоположных наборах $(\alpha_1, \ldots, \alpha_n)$ и $(\overline{\alpha}_1, \ldots, \overline{\alpha}_n)$ самодвойственная функция принимает противоположные значения. Таким образом, самодвойственная функция полностью определяется своими значениями на первой половине строк (см. табл. 1.2.1). Поэтому число самодвойственных функций, зависящих от переменных $x_1, \ldots, x_n$, равно $2^{2^{n-1}} = \sqrt{2^{2^n}}$.

Пусть функция f представлена вектором $\widetilde{\alpha}_f = (\alpha_0, \alpha_1, \ldots, \alpha_{2m+1})$, $m = 2^{n-1} - 1$. Если f — самодвойственная, то из (4) следует равенство

$$\widetilde{\alpha}_f = (\alpha_0, \alpha_1, \ldots, \alpha_m, \overline{\alpha}_m, \ldots, \overline{\alpha}_1, \overline{\alpha}_0). \tag{5}$$

Теорема 2. *Класс S — замкнутый.*

Доказательство. Так как класс S содержит тождественную функцию, то достаточно показать, что функция

$$\Phi = f(f_1, \ldots, f_m)$$

является самодвойственной, если функции $f_1, \ldots, f_m$ самодвойственны. Имеем

$$\Phi^* = f^*(f_1^*, \ldots, f_m^*) = f(f_1, \ldots, f_m) = \Phi,$$

т. е. $\Phi \in S$. ■

Лемма (лемма о несамодвойственной функции). *Если $f(x_1, \ldots, x_n) \notin S$, то из неё путём подстановки функций x и $\overline{x}$ можно получить несамодвойственную функцию одного переменного, т. е. константу.*

Доказательство. Так как $f \notin S$, то найдётся набор $(\alpha_1, \ldots, \alpha_n)$ такой, что

$$f(\overline{\alpha}_1, \ldots, \overline{\alpha}_n) = f(\alpha_1, \ldots, \alpha_n).$$

Обозначим $\varphi_i(x) = x^{\alpha_i}$, $i = 1, \ldots, n$. Положим

$$\varphi(x) = f(\varphi_1(x), \ldots, \varphi_n(x)).$$

Имеем

$$\varphi(0) = f(\varphi_1(0), \ldots, \varphi_n(0)) = f(0^{\alpha_1}, \ldots, 0^{\alpha_n}) = f(\overline{\alpha}_1, \ldots, \overline{\alpha}_n) =$$
$$= f(\alpha_1, \ldots, \alpha_n) = f(1^{\alpha_1}, \ldots, 1^{\alpha_n}) = f(\varphi_1(1), \ldots, \varphi_n(1)) = \varphi(1).$$

Лемма доказана. ■

Задачи.

1. Проверить таблицу 1.

2. Является ли функция g двойственной к функции f, если:

1) $f = x \oplus y$, $g = x \sim y$;
2) $f = x \to y$, $g = y \to x$;
3) $f = x \,|\, y$, $g = x \downarrow y$;
4) $f = (\overline{x} \to \overline{y}) \to (y \to x)$, $g = (x \to y) \wedge (\overline{y} \to \overline{x})$.

3. Выяснить, является ли самодвойственной функция f, заданная вектором:

1) $\widetilde{\alpha}_f = (10110100)$; 2) $\widetilde{\alpha}_f = (01100110)$;
3) $\widetilde{\alpha}_f = (1100\,1001\,0110\,1100)$; 4) $\widetilde{\alpha}_f = (1110\,0111\,0001\,1000)$;
5) $\widetilde{\alpha}_f = (1001\,0110\,1001\,0110)$; 6) $\widetilde{\alpha}_f = (1010\,0101\,0101\,1010)$.

2.2. Классы, сохраняющие константы

Обозначим через T_0 класс всех булевых функций $f(x_1, \ldots, x_n)$, сохраняющих константу 0, т. е. удовлетворяющих равенству

$$f(0, \ldots, 0) = 0.$$

Пример 1. Функции 0, x, $x_1 \wedge x_2$, $x_1 \vee x_2$, $x_1 \oplus x_2$ принадлежат классу T_0, а функции 1, $\overline{x}$, $x_1 \to x_2$, $x_1 | x_2$ не принадлежат классу T_0.

Найдём число функций в классе T_0, зависящих от n переменных. Таблица для функции f из T_0 в первой строке содержит значение 0. Следовательно, функций столько, сколько существует булевых векторов длины $2^n - 1$, т. е. $2^{2^n-1} = \dfrac{1}{2}\,2^{2^n}$.

Теорема 1. *Класс T_0 — замкнутый.*

Доказательство. Рассмотрим индуктивное определение формулы. Рассмотрим выражение вида

$$\Phi = f(A_1, \ldots, A_n),$$

где $f(x_1,\dots,x_n)\in T_0$ и каждое A_i, $i=1,\dots,n$, является либо переменной либо функцией из T_0. Так как тождественная функция принадлежит T_0, то можно считать, что любая A_i есть функция из T_0. Тогда

$$\Phi(0,\dots,0)=f(A_1(0,\dots,0),\dots,A_n(0,\dots,0))=f(0,\dots,0)=0.$$

Следовательно $\Phi\in T_0$ и класс T_0 — замкнутый. ■

Обозначим через T_1 класс всех булевых функций $f(x_1,\dots,x_n)$, сохраняющих константу 1, т. е. удовлетворяющих равенству

$$f(1,\dots,1)=1.$$

Пример 2. Функции 1, x, $x_1\wedge x_2$, $x_1\vee x_2$, $x_1\to x_2$ принадлежат классу T_1, а функции 0, $\overline{x}$, $x_1\oplus x_2$, $x_1|\,x_2$, не принадлежат классу T_1.

Легко проверяется, что класс T_1 двойствен классу T_0, т. е. класс T_1 состоит из функций двойственных функциям из T_0. Таким образом $T_0^*=T_1$ и $T_1^*=T_0$.

Класс T_1 содержит 2^{2^n-1} функций и для него справедлива теорема, аналогичная теореме 1.

Теорема 2. *Класс T_1 — замкнутый.*

Доказательство. Рассмотрим индуктивное определение формулы. Рассмотрим выражение вида

$$\Phi=f(A_1,\dots,A_n),$$

где $f(x_1,\dots,x_n)\in T_1$ и каждое A_i, $i=1,\dots,n$, является либо переменной либо функцией из T_1. Так как тождественная функция принадлежит T_1, то можно считать, что любая A_i есть функция из T_1. Тогда

$$\Phi(1,\dots,1)=f(A_1(1,\dots,1),\dots,A_n(1,\dots,1))=f(1,\dots,1)=1.$$

Следовательно $\Phi\in T_1$ и класс T_1 — замкнутый. ■

Задачи.

1. Выяснить, каким из множеств $T_0\cup T_1$, $T_1\setminus T_0$ принадлежат перечисленные ниже функции:

1) $((x\vee y)\to(x\,|\,yz))\downarrow((y\sim x)\to x)$;
2) $(xy\to z)\,|\,((x\to y)\downarrow(z\oplus\overline{x}y))$;
3) $(x\to y)\wedge(y\downarrow z)\vee(z\to y)$;
4) $\widetilde{\alpha}_f=(10010110)$; 5) $\widetilde{\alpha}_f=(11011001)$.

2. Доказать, что:

1) $T_0 = [\{x \wedge y, x \oplus y\}] = [\{x \vee y, x \oplus y\}]$;
2) $T_1 = [\{x \wedge y, x \sim y\}] = [\{x \vee y, x \sim y\}]$;
2) $T_0 \cap T_1 = [\{x \wedge y, x \oplus y \oplus z\}]$.

2.3. Класс монотонных функций

Булева функция $f(x_1, \ldots, x_n)$ называется *монотонной*, если для любых двух наборов $\widetilde{\alpha}^n$ и $\widetilde{\beta}^n$ таких, что $\widetilde{\alpha}^n \preccurlyeq \widetilde{\beta}^n$, справедливо неравенство

$$f(\widetilde{\alpha}^n) \leq f(\widetilde{\beta}^n)$$

Обозначим через M класс всех монотонных функций.

Пример 1. Функции 0, 1, x, $x_1 \wedge x_2$, $x_1 \vee x_2$ принадлежат классу M, а функции $\overline{x}$, $x_1 | x_2$, $x_1 \downarrow x_2$, $x_1 \oplus x_2$, $x_1 \to x_2$, $x_1 \sim x_2$ не принадлежат классу M.

Теорема 1. *Класс M — замкнутый.*

Доказательство. Поскольку тождественная функция принадлежит классу M, то достаточно показать, что

$$\Phi = f(f_1, \ldots, f_m),$$

является монотонной, если где f, f_1, $\ldots$ f_m монотонны. Пусть

$$\widetilde{x} = (x_1, \ldots, x_n),\ \widetilde{x}_1 = (x_{11}, \ldots, x_{1p_1}), \ldots,\ \widetilde{x}_m = (x_{m1}, \ldots, x_{mp_m}),$$

— наборы переменных функций Φ, f_1, $\ldots$, f_m, причём множество переменных функции Φ состоит из тех и только тех переменных, которые встречаются у функций f_1, $\ldots$, f_m.

Пусть $\widetilde{\alpha}$ и $\widetilde{\beta}$ — наборы длины n значений $\widetilde{x}$, причём $\widetilde{\alpha} \preccurlyeq \widetilde{\beta}$. Эти наборы определяют наборы $\widetilde{\alpha}_1$, $\widetilde{\beta}_1$, $\ldots$, $\widetilde{\alpha}_m$, $\widetilde{\beta}_m$ значений переменных $\widetilde{x}_1$, $\ldots$, $\widetilde{x}_m$ такие, что $\widetilde{\alpha}_1 \preccurlyeq \widetilde{\beta}_1$, $\ldots$, $\widetilde{\alpha}_m \preccurlyeq \widetilde{\beta}_m$.

В силу монотонности функций f_1, $\ldots$, f_m

$$f_1(\widetilde{\alpha}_1) \preccurlyeq f_1(\widetilde{\beta}_1), \ldots, f_m(\widetilde{\alpha}_m) \preccurlyeq f_m(\widetilde{\beta}_m).$$

Поэтому

$$(f_1(\widetilde{\alpha}_1), \ldots, f_m(\widetilde{\alpha}_m)) \preccurlyeq (f_1(\widetilde{\beta}_1), \ldots, f_m(\widetilde{\beta}_m)),$$

и в силу монотонности f имеем

$$f(f_1(\widetilde{\alpha}_1), \ldots, f_m(\widetilde{\alpha}_m)) \leq f(f_1(\widetilde{\beta}_1), \ldots, f_m(\widetilde{\beta}_m)).$$

В результате

$$\Phi(\widetilde{\alpha}) = f(f_1(\widetilde{\alpha}_1), \ldots, f_m(\widetilde{\alpha}_m)) \leq f(f_1(\widetilde{\beta}_1), \ldots, f_m(\widetilde{\beta}_m)) = \Phi(\widetilde{\beta}).$$

Следовательно $\Phi \in M$ и класс M — замкнутый. ■

Наборы $\widetilde{\alpha}^n$, $\widetilde{\beta}^n$ называются *соседними* (по i-й координате), если $\widetilde{\alpha}^n = (\alpha_1, \ldots, \alpha_{i-1}, \alpha_i, \alpha_{i+1}, \ldots, \alpha_n)$, $\widetilde{\beta}^n = (\alpha_1, \ldots, \alpha_{i-1}, \overline{\alpha}_i, \alpha_{i+1}, \ldots, \alpha_n)$.

Лемма (о не монотонной функции). *Если $f(x_1, \ldots, x_n) \notin M$, то из неё путём подстановки констант 0, 1 и функции x можно получить функцию $\overline{x}$.*

Доказательство. Сначала покажем, что найдутся соседние наборы $\widetilde{\alpha}$ и $\widetilde{\beta}$ такие, что $\widetilde{\alpha} \preccurlyeq \widetilde{\beta}$ и

$$f(\widetilde{\alpha}) > f(\widetilde{\beta}).$$

Так как $f \notin M$, то существуют наборы $\widetilde{\alpha}_1$ и $\widetilde{\beta}_1$ такие, что $\widetilde{\alpha}_1 \preccurlyeq \widetilde{\beta}_1$ и $f(\widetilde{\alpha}_1) > f(\widetilde{\beta}_1)$. Если наборы $\widetilde{\alpha}_1$ и $\widetilde{\beta}_1$ — соседние, то эти наборы искомые. Если $\widetilde{\alpha}_1$ и $\widetilde{\beta}_1$ не являются соседними, то набор $\widetilde{\beta}_1$ отличается от набора $\widetilde{\alpha}_1$ в t координатах, где $t > 1$. Эти t координат в наборе $\widetilde{\alpha}_1$ имеют значение 0, а в наборе $\widetilde{\beta}_1$ имеют значение 1. Следовательно, между $\widetilde{\alpha}_1$ и $\widetilde{\beta}_1$ можно вставить $t-1$ наборов $\widetilde{\alpha}_2$, $\widetilde{\alpha}_3$, …, $\widetilde{\alpha}_t$ таких, что

$$\widetilde{\alpha}_2 \preccurlyeq \widetilde{\alpha}_3 \preccurlyeq \ldots, \preccurlyeq \widetilde{\alpha}_t \preccurlyeq \widetilde{\beta}_1.$$

Очевидно, что наборы, стоящие в этой цепочке рядом, будут соседними. Так как $f(\widetilde{\alpha}_1) > f(\widetilde{\beta}_1)$, то по крайней мере на одной из этих пар соседних наборов — обозначим их через $\widetilde{\alpha}$ и $\widetilde{\beta}$ ($\widetilde{\alpha} \preccurlyeq \widetilde{\beta}$) — будет $f(\widetilde{\alpha}) > f(\widetilde{\beta})$.

Пусть данные наборы будут соседними по i-й координате. Следовательно

$$\widetilde{\alpha} = (\alpha_1, \ldots, \alpha_{i-1}, 0, \alpha_{i+1}, \ldots, \alpha_n),$$
$$\widetilde{\beta} = (\alpha_1, \ldots, \alpha_{i-1}, 1, \alpha_{i+1}, \ldots, \alpha_n).$$

Рассмотрим функцию

$$\varphi(x) = f(\alpha_1, \ldots, \alpha_{i-1}, x, \alpha_{i+1}, \ldots, \alpha_n).$$

Тогда

$$\varphi(0) = f(\alpha_1, \ldots, \alpha_{i-1}, 0, \alpha_{i+1}, \ldots, \alpha_n) = f(\widetilde{\alpha}) > f(\widetilde{\beta}) = f(\alpha_1, \ldots, \alpha_{i-1}, 1, \alpha_{i+1}, \ldots, \alpha_n) =$$

Это неравенство означает, что $\varphi(0) = 1$ и $\varphi(1) = 0$, т. е. $\varphi(x) = \overline{x}$. Лемма доказана. ■

Задачи.

1. Какие из перечисленных ниже функций являются монотонными?

1) $x \to (x \to y)$;

2) $x \to (y \to x)$;

3) $xy(x \oplus y)$;

4) $xy \oplus yz \oplus xz \oplus z$.

2. По вектору значений $\widetilde{\alpha}_f$ выяснить, является ли функция f монотонной:

1) $\widetilde{\alpha}_f = (00110111)$; 2) $\widetilde{\alpha}_f = (01100111)$;

3) $\widetilde{\alpha}_f = (00010101\,01010111)$;

4) $\widetilde{\alpha}_f = (00000000\,10111111)$.

2.4. Класс линейных функций

Булева функция $f(x_1, \ldots, x_n)$ называется *линейной*, если

$$f(x_1, \ldots, x_n) = a_0 \oplus a_1 x_1 \ldots \oplus a_n x_n,$$

где константы a_0, $\ldots$, a_n равны 0 или 1. Класс всех линейных функций обознается через L.

Пример 1. Функции 0, 1, x, $\overline{x} = x \oplus 1$, $x_1 \oplus x_2$, $x_1 \sim x_2$ принадлежат классу L, а функции $x_1 \wedge x_2$, $x_1 \vee x_2$, $x_1 \to x_2$, $x_1 | x_2$, $x_1 \downarrow x_2$ не принадлежат классу L.

Теорема 1. *Класс L — замкнутый.*

Доказательство. Если не учитывать слагаемых с коэффициентами $a_i = 0$, то всякую линейную функцию можно представить в виде

$$a_0 \oplus x_{i_1} \oplus x_{i_2} \oplus \ldots \oplus x_{i_k}.$$

Если теперь вместо каждого x_{i_j} подставить линейное выражение или просто переменную, которая также является линейным выражением, то получится снова линейное выражение. Следовательно класс L — замкнутый. ■

Лемма (лемма о нелинейной функции). *Если $f(x_1, \ldots, x_n) \notin L$, то из неё путём подстановки констант 0, 1 и функций x, $\overline{x}$ можно получить функцию $x_1 \wedge x_2$ или функцию $\overline{x_1 \wedge x_2}$.*

Доказательство. Пусть $f(x_1, \ldots, x_n) \notin L$. Возьмём полином Жегалкина для f:

$$f(x_1, \ldots, x_n) = \bigoplus_{(i_1, \ldots, i_s)} a_{i_1, \ldots, i_s} x_{i_1} \ldots x_{i_s}.$$

В силу нелинейности полинома в нём найдётся слагаемое, содержащее не менее двух множителей. Не ограничивая общности будем считать, что среди этих множителей присутствуют x_1 и x_2. Тогда полином Жегалкина можно представить в виде:

$$f(x_1,\dots,x_n) = x_1x_2P_1(x_3,\dots,x_n) \oplus x_1P_2(x_3,\dots,x_n) \oplus \\ \oplus\, x_2P_3(x_3,\dots,x_n) \oplus P_4(x_3,\dots,x_n),$$

где P_1, P_2, P_3, P_4 — некоторые полиномы, причём в полиноме $P_1(x_3,\dots,x_n)$ есть ненулевые коэффициенты.

Так как функция 0 представляется полиномом 0, то из теоремы о единственности полинома Жегалкина вытекает, что функция, задаваемая полиномом $P_1(x_3,\dots,x_n)$, не равна тождественно 0. Следовательно. найдутся $\alpha_3,\dots,\alpha_n \in E_2$ такие, что $P_1(\alpha_3,\dots,\alpha_n) = 1$.

Рассмотрим вспомогательную функцию

$$\varphi(x_1,x_2) = f(x_1,x_2,\alpha_3,\dots,\alpha_n) = x_1x_2 \oplus \alpha x_1 \oplus \beta x_2 \oplus \gamma,$$

где α, β, γ — некоторые константы из E_2.

$$\begin{aligned}\varphi(x_1\oplus\beta, x_2\oplus\alpha) &= (x_1\oplus\beta)(x_2\oplus\alpha)\oplus\alpha(x_1\oplus\beta)\oplus\beta(x_2\oplus\alpha)\oplus\gamma = \\ &= (x_1x_2\oplus x_1\alpha\oplus\beta x_2\oplus\beta\alpha)\oplus(\alpha x_1\oplus\alpha\beta)\oplus(\beta x_2\oplus\beta\alpha)\oplus\gamma = \\ &= x_1x_2\oplus\alpha\beta\oplus\gamma,\end{aligned}$$

В результате получаем

$$\varphi(x_1\oplus\beta, x_2\oplus\alpha) = x_1x_2\oplus(\alpha\beta\oplus\gamma) = \begin{cases} x_1x_2, & \alpha\beta\oplus\gamma = 0, \\ \overline{x_1x_2}, & \alpha\beta\oplus\gamma = 1. \end{cases}$$

Лемма доказана. ■

Задачи.

1. Разлагая функцию f в полином Жегалкина, выяснить является ли она линейной.

1) $f(\widetilde{x}^3) = (x_1x_2 \vee \overline{x_1x_2}) \oplus x_3$;
2) $f(\widetilde{x}^2) = x_1x_2(x_1 \oplus x_2)$;
3) $f(\widetilde{x}^4) = \overline{x}_1x_2 \vee \overline{x}_2x_3 \vee \overline{x}_3x_4 \vee \overline{x}_4x_1$;
4) $f(\widetilde{x}^3) = (x_1 \to x_2)(x_2 \to x_1) \sim x_3$.

2. Выяснить, является ли функция f линейной.

1) $\widetilde{\alpha}_f) = (1010\,1010\,0110\,1000)$;

2) $\widetilde{\alpha}_f) = (1001\,0110\,1001\,0110)$;
3) $\widetilde{\alpha}_f) = (1001\,0110\,0110\,1001)$;
4) $\widetilde{\alpha}_f) = (0110\,1001\,1010\,0101)$.

2.5. Теорема Поста о полноте.

Теорема 1 (о функциональной полноте). *Система булевых функций A является полной в P_2 тогда и только тогда, когда она не содержится целиком ни в одном из пяти замкнутых классов T_0, T_1, S, M и L.*

Доказательство. *Необходимость.* Пусть A — полная система, т. е. $[A] = P_2$. Предположим, что A содержится в одном из классов T_0, T_1, S, M, L. Обозначим его через N. Тогда в силу свойств замыкания и замкнутости N получаем

$$P_2 = [A] \subseteq [N] = N.$$

Значит $N = P_2$. Полученное противоречие доказывает необходимость.

Достаточность. Пусть A целиком не содержится ни в одном из пяти указанных классов. Тогда в A существуют функции f_0, f_1, f_S, f_M, f_L, удовлетворяющие условиям:

$$f_0 \notin T_0,\ f_1 \notin T_1,\ f_S \notin S,\ f_M \notin M,\ f_L \notin L.$$

Можно считать, что все эти функции зависят от одних и тех же переменных $x_1, \ldots, x_n$.

Так как система функций $\{\overline{x}, x \wedge y\}$ является полной, то достаточно из функций f_0, f_1, f_S, f_M, f_L получить отрицание и конъюнкцию.

Сначала построим из функций f_0, f_1, f_S константы 0 и 1. Рассмотрим функцию $f_0 \notin T_0$. Возможны два случая:

1. $f_0(1, \ldots, 1) = 1$. Пусть $\varphi(x) = f_0(x, \ldots, x)$. Так как

$$\varphi(0) = f_0(0, \ldots, 0) = 1, \quad \varphi(1) = f_0(1, \ldots, 1) = 1,$$

то функция $\varphi(x)$ есть константа 1. Функция $\psi(x) = f_1(\varphi(x), \ldots, \varphi(x))$ есть есть константа 0 в силу $f_1(1, \ldots, 1) = 0$.

2. $f_0(1, \ldots, 1) = 0$. Пусть $\varphi(x) = f_0(x, \ldots, x)$. Так как

$$\varphi(0) = f_0(0, \ldots, 0) = 1, \quad \varphi(1) = f_0(1, \ldots, 1) = 0,$$

то $\varphi(x) = \overline{x}$. Имея $\overline{x}$, то в силу леммы о несамодвойственной функции, из функции f_S ($f_S \notin S$) мы можем получить константу. Используя $\overline{x}$, получим вторую константу. Итак, в обоих случаях получены константы 0 и 1.

Имея константы 0 и 1 и применяя к функции $f_M \notin M$ лемму о немонотонной функции получим функцию $\overline{x}$.

На основе леммы о нелинейной функции можно получить из функции f_L ($f_L \notin L$) подстановкой констант и функции $\overline{x}$ конъюнкцию либо отрицание конъюнкции. Так как у нас есть функция $\overline{x}$, то мы в любом случае можем получить конъюнкцию. ■

Следствие. *Всякий замкнутый класс A функций из P_2, такой, что $A \neq P_2$, содержится по крайней мере в одном из классов T_0, T_1, S, M, L.*

Система булевых функций $B \subseteq P_2$, называется *базисом* в P_2, если

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

Теорема 2. *Максимальное число функций в базисе P_2 равно* 4.

Доказательство. Докажем, что из любой полной системы можно выделить полную подсистему, содержащую не более 4 функций. Пусть A — полная система. Тогда по теореме Поста в ней существуют пять функций $f_0 \notin T_0$, $f_1 \notin T_1$, $f_S \notin S$, $f_L \notin L$, $f_M \notin M$. Из этой же теоремы следует, что система $\{f_0, f_1, f_S, f_L, f_M\}$ полна.

Рассмотрим функцию $f_0 \notin T_0$. Возможны два случая.

1. $f_0(1, \ldots, 1) = 1$. Тогда $f_0 \notin S$, и по теореме Поста система $\{f_0, f_1, f_L, f_M\}$ полна.

2. $f_0(1, \ldots, 1) = 0$. Тогда $f_0 \notin T_1$, $f_0 \notin M$ и по теореме Поста система $\{f_0, f_S, f_L\}$ полна.

Следовательно, система, содержащая более 4 функций, не может быть базисом.

Рассмотрим систему функций

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

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

$$\{0, 1, x \wedge y\,\} \subseteq M; \qquad \{0, 1, x \oplus y \oplus z\,\} \subseteq L;$$
$$\{0, x \wedge y, x \oplus y \oplus z\,\} \subseteq T_0; \quad \{1, x \wedge y, x \oplus y \oplus z\,\} \subseteq T_1.$$

Теорема доказана. ■

Класс функций $A \subseteq P_2$ называется *предполным* (или *максимальным*), если

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

Теорема 3. *В P_2 существуют только пять предполных классов, а именно: T_0, T_1, S, M, L.*

Доказательство.

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

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

б) Докажем, что все пять рассматриваемых класса являются предполными. Пусть R один из классов T_0, T_1, S, M, L. Тогда $[R] = R \neq P_2$ и пункт 1) выполнен.

Пусть $f \notin R$. Тогда система $R \cup \{f\}$ не содержится ни в одном из пяти классов. По теореме Поста она является полной и выполнен пункт 2). В результате R — предполный класс.

в) Докажем, что нет других предполных классов. Пусть A — предполный класс. Тогда $[A] \neq P_2$. По теореме Поста существует класс $R \in \{T_0, T_1, S, M, L\}$ такой, что $A \subseteq R$. Если $A \neq R$, то существует $f \in R \setminus A$. Тогда $A \cup \{f\} \subseteq R$ и система $A \cup \{f\}$ не полна, что противоречит пункту 2). Полученное противоречие завершает доказательство. ■

Задачи.

1. Выяснить, полна ли система функций:

1) $\{xy, x \vee y, x \oplus y, xy \vee yz \vee zx\}$;

2) $\{xy, x \vee y, x \oplus y \oplus z \oplus 1\}$;

3) $\{x \to y, x \to \overline{y}z\}$;

4) $\{x\overline{y}, \overline{x} \sim yz\}$.

2. Выяснить, полна ли система функций, заданных векторами своих значений:

1) $\{f_1 = (0110), f_2 = (1100\,0011), f_3 = (1001\,0110)\}$;
2) $\{f_1 = (0111), f_2 = (0101\,1010), f_3 = (0111\,1110)\}$;
3) $\{f_1 = (0101), f_2 = (1110\,1000), f_3 = (0110\,1001)\}$;
4) $\{f_1 = (11), f_2 = (0111), f_3 = (0011\,0111)\}$.

Указатель обозначений

E_2 — множество $\{0, 1\}$
E_2^n — n-я декартова степень множества E_2
L — класс всех линейных функций
M — класс всех монотонных функций
P_2 — множество всех булевых функций
$P_2^{(n)}$ — множество всех n-местных булевых функций
S — класс всех самодвойственных функций
T_0 — класс всех функций, сохраняющих константу 0
T_1 — класс всех функций, сохраняющих константу 1

Список литературы

1. Алексеев В.Б. **Лекции по дискретной математике:** Учеб. пособие. — М.: ИНФРА-М, 2017. — 90 с.

2. Гаврилов Г.П., Сапоженко А.А. **Задачи и упражнения по дискретной математике:** Учеб. пособие. — 3-е изд., перераб. — М.: ФИЗМАТЛИТ, 2004. — 416 с.

3. Марченков С.С. **Основы теории булевых функций.** — М.: ФИЗМАТЛИТ, 2014. — 136 с.

4. Яблонский С.В. **Введение в дискретную математику:** Учеб. пособие для вузов. — 4-е изд., стер. — М.: Высшая школа, 2003. — 384 с.

5. Яблонский С.В., Гаврилов Г.П., Кудрявцев В.Б. **Функции алгебры логики и классы Поста.** — М.: Наука, 1966. — 120 с.

Содержание

УНИВЕРСИТЕТ ИТМО

Миссия университета – открывать возможности для гармоничного развития конкурентоспособной личности и вдохновлять на решение глобальных задач.

ФАКУЛЬТЕТ ПРОГРАММНОЙ ИНЖЕНЕРИИ И КОМПЬЮТЕРНОЙ ТЕХНИКИ

Факультет программной инженерии и компьютерной техники специализируется на подготовке специалистов по разработке компьютерных систем и новейших технологий программирования. Вектор развития факультета определяется прогнозом потребностей компьютерной и программной индустрии через 10-20 лет. Мы готовим специалистов грядущей постинформационной эпохи – эпохи виртуальной реальности, киберфизических систем и интернета вещей.

На факультете умеют и учат создавать компьютеры. Здесь старейшая в России научная и инженерная школа проектирования ЭВМ. И в настоящее время все ведущие сотрудники кафедры – действующие ученые, инженеры и руководители в отрасли компьютерных технологий.

Студентов научат устройству и разработке вычислительных систем от микропроцессоров до компьютеров и смартфонов, от контроллеров устройств интернета вещей до систем управления роботами, от компьютерных кластеров до центров обработки данных.

Здесь создают новые технологии программирования. В основе научных исследований и преподавания лежит перспективная концепция «программной инженерии» – промышленной разработки и поддержки программных систем в рамках единой формализованной системы методологий и технологий.

Студенты приобретают знания и опыт в программировании информационных систем будущего: «облачных» вычислений, искусственного интеллекта, основанного на онтологиях и базах знаний, систем поиска и обработки больших данных (data mining, big data) и интернета вещей.

Выпускники кафедры могут использовать информационные и мультимедиа-технологии в творческой деятельности, в области театрального искусства, киноискусства и телевидения, а также в исследовательской, проектной и практической деятельности, в области средств массовой информации, рекламы, бизнес-коммуникаций, медиа-индустрии.

На факультете осуществляется мультидисциплинарная подготовка методам обработки информации и технологиям программирования. Выпускник кафедры – программист будущего, умеющий применять новейшие нейротехнологии для разработки приложений в области машинного обучения, систем искусственного интеллекта, обработки несистематизированных данных окружающей реальности.

Наши выпускники получают конкурентоспособное образование, способны быстро адаптироваться под новые условия, готовы совершенствовать свою квалификацию и ожидаемы ведущими отечественными и зарубежными предприятиями и фирмами: РЖД, Яндекс, Promt, Luxoft, Газпром, Сбербанк, Intel, Microsoft, Oracle, IBM, AMD, Deutsche Bank – далеко не полный перечень организаций, куда каждый год трудоустраиваются все новые и новые выпускники факультета, и где ценят наше качество образования.

Кудашов Вячеслав Николаевич

Булевы функции

Учебно-методическое пособие

В авторской редакции
Редакционно-издательский отдел Университета ИТМО
Зав. РИО Н.Ф. Гусарова
Подписано к печати
Заказ №
Тираж
Отпечатано на ризографе

Редакционно-издательский отдел
Университета ИТМО
197101, Санкт-Петербург, Кронверкский пр., 49