Дискретная математика и математическая логика

Конспект по 2 семестру специальностей «экономическая кибернетика» и «компьютерная безопасность»

(лектор В. И. Бенедиктович)

Оглавление

Глава 1

Булевы функции

Замкнутые классы булевых функций

Пусть $A \subseteq P$
• **Замыканием** A называется множество функций из P_2, которые можно выразить в виде формул над A и обозначается $[A]$.

Свойства замыкания:

1. $A \subseteq [A]$
2. $A \subseteq B \Rightarrow [A] \subseteq [B]$
3. $\big[[A]\big] = [A]$
4. $[A] \cup [B] \subseteq [A \cup B]$

• A - **полная система** булевой функции, если $[A] = P_2$.
• Система буевых функций A **замкнутая**, если $[A] = A$.

Пример. $A = \{1, x_1 \oplus x_2\}$ не замкнута, так как $1 \oplus 1 = 0 \notin A$

Пусть A - замкнутый неполный класс системы булевых функций. Тогда если $A \subseteq B$, то B - неполная система.

♦ $B \subseteq A \Rightarrow [B] \subseteq [A] \neq P_2 \Rightarrow [B] \neq P_2 \Rightarrow B$ - неполная система. ⊠

Примеры замкнутых классов булевых функций

I) Класс $T_0 = \{f(x_1, \ldots, x_n) | f(0, \ldots, 0) = 0\}$

Например:
$0,\ x,\ x_1 \cdot x_2,\ x_1 \vee x_2,\ x_1 \oplus x_2 \in T_0$
$1,\ \bar{x},\ x_1 \Rightarrow x_2,\ x_1 | x_2,\ x_1 \downarrow x_2,\ x_1 \Leftrightarrow x_2 \notin T_0$

Мощность класса: $2^n - 1$ ненулевых строк $\Rightarrow |T_0| = 2^2 - 1 = \frac{1}{2} 2^{2^n}$

Теорема. *Класс T_0 замкнут.*

♦ Поскольку $x \in T_0$, то достаточно показать, что если $f_1, f_2, \dots, f_n \in T_0$, то $f(f_1, \dots, f_n) \in T_0$. Действительно, $f(f_1(0, \dots, 0), \dots, f_n(0, \dots, 0)) = f(0, \dots, 0) = 0$ ⊠

II) Класс $T_1 = \{f(x_1, \dots, x_n) \in P_2 | f(1, \dots, 1) = 1\}$

Например:
$1, x, x_1 \cdot x_2, x_1 \vee x_2, x_1 \Rightarrow x_2, x_1 \Leftrightarrow x_2 \in T_1$
$0, \bar{x}, x_1 | x_2, x_1 \downarrow x_2, x_1 \oplus x_2 \notin T_1$

Теорема. *Класс Класс T_1 замкнут.*

♦ Доказательство аналогично доказательству предыдущей теоремы ⊠

III) Класс M монотонных функций.

Введём **частичный булевый порядок** на E_2^n: $\bar{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_n)$, $\bar{\beta} = (\beta_1, \beta_2, \dots, \beta_n) \in E_2^n$
Говорят, что $\bar{\alpha} \leqslant \bar{\beta} \Leftrightarrow \alpha_i \leqslant \beta_i$ для $\forall i$

• Функция $f(x_1, \dots, x_n)$ называется **монотонной**, если $\forall \bar{\alpha}, \bar{\beta} : \bar{\alpha} \leqslant \bar{\beta} \Rightarrow f(\bar{\alpha}) \leqslant f(\bar{\beta})$
Множество всех монотонных функций обозначают M.

Например:
$0, 1, x, x_1 \cdot x_2, x_1 \vee x_2 \in M$
$0, \bar{x}, x_1 \Rightarrow x_2 \notin M$

Теорема. *Класс M замкнут.*

♦ Достаточно показать, что если $f_1, f_2, \dots, f_m \in M$, то $f(f_1, \dots, f_m) \in M = \Phi$
Пусть $\bar{\alpha} \leqslant \bar{\beta}$, тогда $f_1(\bar{\alpha}) \leqslant f_1(\bar{\beta}), \dots, f_m(\bar{\alpha}) \leqslant f_m(\bar{\beta}) \Rightarrow (f_1(\bar{\alpha}), \dots, f_m(\bar{\alpha})) \leqslant (f_1(\bar{\beta}), \dots, f_m(\bar{\alpha})) \Rightarrow f(f_1(\bar{\alpha}), \dots, f_m(\bar{\alpha})) \leqslant f(f_1(\bar{\beta}), \dots, f_m(\bar{\alpha}))$, то есть $\Phi(\bar{\alpha}) \leqslant \Phi(\bar{\beta})$ ⊠

Лемма. *О немонотонной функции*
Если $f(x_1, \dots, x_n)$ - немонотонная функция, то $\bar{x} \in [\{0, 1, f\}]$

♦ Пусть $f(x_1, \dots, x_n)$ - немонотонная функция, то есть $\exists \bar{\alpha} < \bar{\beta} \Rightarrow f(\bar{\alpha}) = 1, f(\bar{\beta}) = 0 (1 > 0)$.
$\bar{\alpha} < \bar{\beta}$ означает, что $\exists 1 \leqslant i_1 < i_2 < \dots < i_k \leqslant n$:
$\gamma_0 = \bar{\alpha} = (\alpha_1, \dots, \alpha_{i_1-1}, 0, \alpha_{i_1+1}, \dots, \alpha_{i_2-1}, 0, \alpha_{i_2+1}, \dots, \alpha_{i_k-1}, 0, \alpha_{i_k+1}, \dots, \alpha_n)$
$\gamma_1 = (\alpha_1, \dots, \alpha_{i_1-1}, 1, \alpha_{i_1+1}, \dots, \alpha_{i_2-1}, 0, \alpha_{i_2+1}, \dots, \alpha_{i_k-1}, 0, \alpha_{i_k+1}, \dots, \alpha_n)$
$\gamma_2 = (\alpha_2, \dots, \alpha_{i_1-1}, 1, \alpha_{i_1+1}, \dots, \alpha_{i_2-1}, 1, \alpha_{i_2+1}, \dots, \alpha_{i_k-1}, 0, \alpha_{i_k+1}, \dots, \alpha_n)$
$\dots$
$\gamma_k = \bar{\beta} = (\alpha_1, \dots, \alpha_{i_1-1}, 1, \alpha_{i_1+1}, \dots, \alpha_{i_2-1}, 1, \alpha_{i_2+1}, \dots, \alpha_{i_k-1}, 1, \alpha_{i_k+1}, \dots, \alpha_n)$
$\gamma_0 < \gamma_1 < \gamma_2 < \gamma_3 < \dots < \gamma_k = \bar{\beta}$
Так как $f(\gamma_0) = 1, f(\gamma_k) = 0, f(\gamma_e) = 1, f(\gamma_{e+1}) = 0$, то $\exists l : 0 \leqslant l \leqslant k-1$, то есть $\alpha_e = 0, \beta_e = 1, \forall i \neq l, \alpha_i = \beta_i$
Построим функцию $h(x) = f(\alpha_1, \dots, \alpha_{e-1}, x, \alpha_{e+1}, \dots, \alpha_n)$

$$\begin{cases} h(0) = f(\bar{\alpha}) = 1 \\ h(1) = f(\bar{\beta}) = 0 \end{cases} \Rightarrow h(x) \equiv \bar{x}$$ ⊠

IV) Класс S самодвойственных функций.

• Функция $f^*(x_1,\dots,x_n)=\bar{f}(\bar{x}_1,\dots,\bar{x}_n)$ называется двойственной для функции $f(x_1,\dots,x_n)$
• Функция $f(x_1,\dots,x_n)$ называется самодвойственной, если $f(x_1,\dots,x_n)=f^*(x_1,\dots,x_n)$
Другими словами:

$$\bar{f}(x_1,\dots,x_n)=f(\bar{x}_1,\dots,\bar{x}_n) \tag{1}$$

• Наборы $\bar{\alpha}=(\alpha_1,\dots,\alpha_n)$ и $\bar{\beta}=(\bar{\alpha}_1,\dots,\bar{\alpha}_n)$ называются противоположными наборами.

Например:
$x,\bar{x}\in S$
$x_1\cdot x_2\notin S$, то есть $(x_1\cdot x_2)^*=\overline{\overline{x_1}\cdot\overline{x_2}}=x_1\vee x_2\neq x_1\cdot x_2$

Теорема. *6* *Класс S замкнут.*

♦ Достаточно показать, что $f_1,f_2,\dots,f_n\in S$, то $\Phi=f(f_1,\dots,f_n)\in S$
$\Phi^*(x_1,\dots,x_n)=\bar{\Phi}(\bar{x}_1,\dots,\bar{x}_n)=\bar{f}(f_1(\bar{x}_1,\dots,\bar{x}_n),\dots,f_n(\bar{x}_1,\dots,\bar{x}_n))\overset{(1)}{=}$
$\overset{(1)}{=}\bar{f}(\bar{f}_1(x_1,\dots,x_n),\dots,\bar{f}_n(x_1,\dots,x_n))=f(f_1(x_1,\dots,x_n),\dots,f_n(x_1,\dots,x_n))=\Phi(x_1,\dots,x_n)$
⊠

Лемма. *О несамодвойственной функции.*
Если $f(x_1,\dots,x_n)$ - несамодвойственная функция, то $0,1\in[\{\bar{x},f\}]$

♦ Пусть $f(x_1,\dots,x_n)$ - несамодвойственная функция. Тогда $\exists\bar{\alpha}=(\alpha_1,\dots,\alpha_n), f(\bar{\alpha})=f(\bar{\alpha}_1,\dots,\bar{\alpha}_n)=f(\alpha_1,\dots,\alpha_n)$.
Заменим α_i на $x\oplus\alpha_i$: $\begin{cases} x, \text{если } \alpha_i=0,\\ \bar{x}, \text{если } \alpha_i=1;\end{cases}$
Получим функцию $h(x)\equiv f(x\oplus\alpha_1,\dots,x\oplus\alpha_n)$
$h(0)=f(\alpha_1,\dots,\alpha_n)=c,\ c=const$
$h(1)=f(\bar{\alpha}_1,\dots,\bar{\alpha}_n)=c$
$h(x)=c\Rightarrow\bar{c}=\bar{h}(x)\Rightarrow 0,1\in[\{\bar{x},f\}]$ ⊠

Полином Жегалкина

• Полином Жегалкина — функция вида $\sum\limits_{\{i_1,\dots,i_k\}\in\{1,2,\dots,n\}} a_{i_1,\dots,a_k}\cdot x_{i_1}\cdot\ldots\cdot x_{i_k}\oplus a$, где a — свободный член.

Пример: $x_1x_2x_3\oplus x_1x_2\oplus x_1x_3\oplus x_1\oplus 1$

Полные системы булевых функций

Теорема. *7* *Система функций $A=x_1\vee x_2, x_1\cdot x_2,\bar{x}$ является полной. (Базис Буля)*

♦ $f(x_1,\dots,x_n)\in P_2$. Если булевая функция отлична от нуля, то по следствию из 2 теоремы Шеннона функция f выражается в виде совершенной дизъюнктивной нормальной формы, в которую входят дизъюнкция, конъюнкция, отрицание, тем самым она принадлежит замыканию класса. Если $f=0$, то $f=x_1\cdot\bar{x}_1$. ⊠

Теорема. *8 (о сведении)*
Если система A — полная и любая функция из A может быть выражена формулой над некоторой системой функций B, то B — полная система.

♦ $[A]=P_2, A\subseteq[B]\Rightarrow P_2=[A]\subseteq\big[[B]\big]=[B]\subseteq P_2\Rightarrow[B]=P_2$. То есть B - полная система.
⊠

Теорема. *9*
Сдедующие системы являются полными:

1. $A_1 = \{x_1 \vee x_2,\ \bar{x}\}$
2. $A_2 = \{x_1 \cdot x_2,\ \bar{x}\}$
3. $A_3 = \{x_1 | x_2\}$
4. $A_4 = \{x_1 \cdot x_2,\ x_1 \oplus x_2,\ 1\}$

♦

1. По теореме 7 система $\{x_1 \vee x_2,\ \bar{x}\}$ — полная. По закону де Моргана: $x_1 \cdot x_2 = \overline{\overline{x_1} \vee \overline{x_2}} \Rightarrow x_1 \cdot x_2 \in [A_1]$. По теореме 8 следует$[A_1] = P_2$.
2. По закону де Моргана $x_1 \vee x_2 = \overline{\overline{x_1} \cdot \overline{x_2}} \Rightarrow x_1 \vee x_2 \in [A_2]$. По теореме 8$[A_2] = P_2$.
3. Можем представить отрицание в виде штриха Шеффера: $\bar{x} = x|x. x_1 \cdot x_2 = \overline{x_1|x_2} = (x_1|x_2)|(x_1|x_2) \Rightarrow \bar{x},\ \ x_1 \cdot x_2 \in [A_3]$. По теореме 8 и доказательству п.2 $A_3 = P_2$.
4. $\bar{x} = x \oplus 1 \Rightarrow \bar{x} = [A_4]$. По теореме 8 и доказательству п.2 следует, что $[A_4] = P_2$.

⊠

Теорема. 10 *(теорема Жегалкина)*
Любую булевую функцию $f(x_1, \dots, x_n)$ можно представить единственным образом в виде полинома Жегалкина $G_f(x_1, \dots, x_n)$.

♦ 1) Докажем существование:
В силу теоремы 9 и доказательства п.4 система $\{x_1 \cdot x_2,\ x_1 \oplus x_2,\ 1\}$ полная $\Rightarrow$ любая булевая функция $f(x_1, \dots, x_n)$ может быть реализована над этой системой. После раскрытия скобок используют дистрибутивность конъюнкции относительно сложения по mod 2 ($\oplus$) и приведения подобных получаем полином Жегалкина.

2) Докажем единственность:
Подсчитаем количество полиномов Жегалкина от переменных $x_1, \dots, x_n$. Каждое слагаемое в полиноме Жегалкина имеет вид конъюнкции переменных $x_{i_1}, \dots, x_{i_k}$ или существует свободный член 1. Каждая такая конъюнкция определяется подмножеством индексов во множестве индексов $i = \overline{1, n}$ ($\{i_1, \dots, i_k\} \subset \{1, \dots, n\}$). Значит, множество всевозможных слагаемых в полиноме равно количеству подмножеств в n-элементном множестве, то есть 2^n.
Чтобы составить полином Жегалкина нужно выбрать подмножество из множества всевозможных слагаемых. Число полиномов Жегалкина равно 2^{2^n}, что равно количеству булевых функций от n переменных. А так как любая булевая функция имеет полином Жегалкин, представляющий её, то существует единственный полином представляющий булевую функцию. ⊠

В силу этой функции полином Жегалкина представляет собой булевую функцию G_f. $G_f(x_1, \dots, x_n)$ — алгебраически нормальная формула (АНФ) булевой функции.

Булевая функция $f(x_1, \dots, x_n)$ существенно зависит от x_i (не является фиктивной переменной) и содержится в каком-либо слагаемом $G_f(x_1, \dots, x_n)$.

Пример: $x_1 \vee x_2$

Методы приведения к виду полинома Жегалкина

1. Метод неопределенных коэффициентов
$x_1 \vee x_2 = a \cdot x_1x_2 + b \cdot x_1 + c \cdot x_2 + d$; нам необхожимо найти a, b, c, d. Подставим $(0,0), (0,1), (1,0), (1,1)$:

$(0,0)$	$d = 0$
$(0,1)$	$1 = c + d \Rightarrow c = 1$
$(1,0)$	$1 = b + d \Rightarrow b = 1$
$(1,1)$	$1 = a + b + c + d \Rightarrow a = 1$ (по mod 2)

Следовательно, $x_1 \vee x_2 = x_1x_2 \oplus x_1 \oplus x_2$.
В общем случае для определения неизвестных коэффициентов при $a_{i_1,\dots,i_k}x_{i_1}, \dots, x_{i_k}$ составляется уравнение $G_f(a_1, \dots, a_i) = f(a_1, \dots, a_n)$, из чего следует, что всего 2^n уравнений, 2^n неизвестных коэффициентов и в силу теоремы 10 имеет единственное решение.

2. Метод эквивалентных преобразований
С помощью следующих тождеств: $\bar{A} = A \oplus 1$, $A \vee B = \overline{\overline{A} \cdot \overline{B}} = (A \oplus 1) \cdot (B \oplus 1) \oplus 1 = AB \oplus A \oplus B$, $A \cdot A = A$, $A \cdot 1 = A$, $A \oplus A = 0$, $A \oplus 0 = A$, приводим формулу к эквивалентной над системой этих трёх функций $x_1 \cdot x_2, x_1 \oplus x_2, \bar{x}$ и запишем в виде $x_1 \vee x_2 = x_1 \cdot x_2 \oplus x_1 \oplus x_2$.

3. Метод треугольника Паскаля
Используется, когда функция задана вектором значений. Метод позволяет преобразовать таблицу истинности в полином Жегалкина путем построения вспомогательной треугольной таблицы в соответствии со следующими правилами:

   (a) Строится таблица истинности, в которой строки идут в лексикографическом порядке возрастания двоичных кодов (от 0 до 1): $00\dots00$, $00\dots01$, $00\dots10$, $00\dots11$, $\dots$, $11\dots11$;

   (b) Строится вспомогательная треугольная таблица, в которой первый столбец совпадает со столбцом значений функции из таблицы истинности;

   (c) Ячейка в каждом последующем столбце таблицы получается путем суммирования по mod 2 двух ячеек: стоящей в той же строке и в строке ниже предыдущего столбца;

   (d) Столбцы вспомогательной треугольной таблицы нумеруются двоичными кодами в том же порядке, что и строки таблицы истинности;

   (e) Каждому двоичному коду ставится в соответствие один из членов полинома Жегалкина в зависимости от позиций кода, в которых стоят единицы;

   (f) Если в верхней строке любого столбца стоит 1, то соответствующий член входит в полином Жегалкина.

x_1	x_2	$x_1 \vee x_2$
0	0	0
0	1	1
1	0	1
1	1	1

00	01	10	11
1	x_1	x_2	$x_1 \cdot x_2$
0	1	1	1
1	0	0	
1	0		
1			

Из треугольника Паскаля результат: $x_1 \vee x_2 = x_1 \cdot x_2 \oplus x_1 \oplus x_2$

V) Класс L линейных функций.

• Булевая функция $f(x_1, \dots, x_n)$ **линейная**, если она может быть задана в виде полинома Жегалкина степени $\leqslant 1$.

$$f(x_1, \dots, x_n) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n$$

где $a_i \in E_2 = \{0, 1\}, \quad i = \overline{0, n}$

Множество всех линейных функций обозначают L.

Например: $0,\ 1,\ x,\ \bar{x} = x \oplus 1,\ x_1 \oplus x_2,\ x_1 \Leftrightarrow x_2 = x_1 \oplus x_2 \oplus 1\ \in L$
$x_1 \cdot x_2,\ x_1 \vee x_2 = x_1 \cdot x_2 \oplus x_1 \oplus x_2,\ x_1 \Rightarrow x2,\ x_1 | x_2, x_1 \downarrow x_2 \notin L$

Теорема. 11
Класс L замкнут.

♦ $L = [\{1,\ x,\ x_1 \oplus x_2\}]$ – замыкание замыкания = замыканию $\Rightarrow L$ замкнут. ⊠

Лемма. 3 *(о нелинейной функции)*
Если булевая функция нелинейная, то $x_1 \cdot x_2 \in [\{0,\ 1,\ \bar{x},\ f\}]$.

♦ Пусть $f = (x_1, \dots, x_n)$ – нелинейная, тогда по теореме 10 f может быть представлена в виде полинома Жегалкина со степенью $\leqslant 1$. Тогда в представление $G_f(x_1, \dots, x_n)$ входит произведение $x_1 \cdot x_2 \Rightarrow$ полином Жегалкина можно представить в следующем виде:
$G_f(x_1, \dots, x_n) = x_1 \cdot x_2 \cdot p_0(x_3, x_4, \dots, x_n) \oplus x_1 \cdot p_1(x_3, x_4, \dots, x_n) \oplus x_2 \cdot p_2(x_3, x_4, \dots, x_n) \oplus p_3(x_3, x_4, \dots, x_n), \quad p_0(x_3, x_4, \dots, x_n) \not\equiv 0.$
$\exists a_3, a_4, \dots, a_n \in E_2 : \quad p_0(a_3, \dots, a_n) = 1$

Пусть $p_1(x_3, x_4, \dots, x_n) = b_1$,
$p_2(x_3, x_4, \dots, x_n) = b_2$,
$p_3(x_3, x_4, \dots, x_n) = b_3$

$G_f(x_1, x_2, a_3, \dots, a_n) = x_1 \cdot x_2 \oplus b_1 \cdot x_1 \oplus b_2 \cdot x_2 \oplus b_3$

Сделаем подстановки:
x_1 заменим на $x_1 \oplus b_2 \quad \begin{cases} x_1, \text{если} b_2 = 0, \\ \bar{x}_1, \text{если} b_2 = 1; \end{cases}$,
а x_2 заменим на $x_2 \oplus b_1 \quad \begin{cases} x_2, \text{если} b_1 = 0, \\ \bar{x}_2, \text{если} b_1 = 1; \end{cases}$.

В результате:
$G_f(x_1 \oplus b_2, x_2 \oplus b_1, a_3, \dots, a_n) = (x_1 \oplus b_2)(x_2 \oplus b_1) \oplus b_1(x_1 \oplus b_2) \oplus b_2(x_2 \oplus b_1) \oplus b_3 = x_1 \cdot x_2 \oplus$

$b_1 \cdot b_2 \oplus b_3, \quad b_1 \cdot b_2 \oplus b_3 = c$

$$x_1 \cdot x_2 = G_f(x_1 \oplus b_2, x_2 \oplus b_1, a_3, \dots, a_n) \oplus c = \begin{cases} G_f, \text{если} c = 0, \\ \bar{G}_f, \text{если} c = 1; \end{cases} \quad \Rightarrow x_1 \cdot x_2 \in [\{0,\ 1,\ \bar{x},\ f\}]. \boxtimes$$

Заметим, что классы $T_0,\ T_1,\ S,\ M,\ L$ попарно различны:

	T_0	T_1	S	M	L
0	+	-	-	+	+
1	-	+	-	+	+
$\bar{x}$	-	-	+	-	+

Теорема. 12 *(Критерий полноты Поста)*
Чтобы система функций A была полной необходимо и достаточно, чтобы она целиком не содержалась ни в одном из классов $T_0,\ T_1,\ S,\ M,\ L$. (То есть $f_0,\ f_1,\ f_s,\ f_m,\ f_l \in A$ и $f_0 \notin T_0,\ f_1 \notin T_1,\ f_m \notin M,\ f_s \notin S,\ f_l \notin L$.)

⧫ Необходимость: A -полная и пусть $A \subseteq X$, где X - один из классов $T_0,\ T_1,\ S,\ M,\ L$. Тогда замыкание $[A] \subseteq [X] \notin P_2 \Rightarrow A$ – неполная, из чего следует противоречие.
Достаточность: Так как $f_0,\ f_1,\ f_s,\ f_m,\ f_l \in A$ и $f_0 \notin T_0,\ f_1 \notin T_1,\ f_m \notin M,\ f_s \notin S,\ f_l \notin L \Leftrightarrow f_0(0, \dots, 0) = 1$. Рассмотрим два случая:

a) $\quad f_0(1, \dots, 1) = 1 \Rightarrow f_0(x, \dots, x) \equiv 1 \in [A]$.
С другой стороны, $f_1(1, \dots, 1) = 0 \Rightarrow f_1(f_0(x, \dots, x), \dots, f_0(x, \dots, x_n)) \equiv 0 \in A$. Так как $0,\ 1 \in [A]$ и $f_m \in [A]$, то по лемме 1 о немонотонной функции $\bar{x} \in [0,\ 1,\ f_m] \in [A]$.

b) $\quad f_0(1, \dots, 1) = 0 \Rightarrow f_0(x, \dots, x) \equiv \bar{x}$. По лемме 2 о не самодвойственной функции: $0,\ 1 \in [\bar{x},\ f_s] \subseteq [A] \Rightarrow$ замыканию класса A принадлежат константы и отрицание и по лемме 3 о нелинейной функции $x_1 \cdot x_2 \in [0,\ 1,\ \bar{x},\ f_l] \equiv [A]$.
Таким образом, $\bar{x},\ x_1 \cdot x_2 \in [f_0,\ f_1,\ f_s,\ f_m,\ f_l] \subseteq [A]$. По теореме 9 о сведении A — полная система. ⊠

Замечание: *по теореме Поста можно проверить полноту любой системы из множества булевых функций* $A = \{f_1, \dots, f_t\}$. Строим таблицу, где строки соответствуют функциям, а столбцы - классам.

	T_0	T_1	S	M	L
f_1			+		
f_i			+	-	
f_t			+		

На пересечении строки f_i и столбца записываем: «+», если функция f_i принадлежит классу, записанному в данном столбце, и «-», если f_i не принадлежит классу, записанному в данном столбце.

По теореме Поста, система A является полной тогда и только тогда, когда в любом столбце найдётся хотя бы один минус, и неполной, если есть хотя бы один стобец, полностью состоящий из плюсов («+»).

Пример:

	T_0	T_1	S	M	L
$\bar{x}$	-	-	-	+	+
$x \Rightarrow y$	-	+	-	-	-

$\Rightarrow$ система полная.

Минимизация булевых функций

Элементарная конъюнкция — выражение вида $K = x_{i_1}^{\sigma_1}, \dots, x_{i_r}^{\sigma_r}$, где r — ранг конъюнкции, $i_k \in \{1, \dots, n\}$, $\sigma_i \in \{0, 1\}$, $i_j \neq i_k$ при $j \neq k$.

$$x_{i_j}^{\sigma_j} = \begin{cases} x_{i_j}, \ \sigma_j = 1, \\ \bar{x}_{i_j}, \ \sigma_j = 0 \end{cases} \quad \text{— литералы.}$$

Утверждение: const = 1 - элементарная конъюнкция, $r = 0$.

• Полная элементарная конъюнкция — элементарная конъюнкция, в которой каждая переменная $f_1, \dots, f_n$ входит в нее не более 1 раза вместе с отрицанием.

• Дизъюнктивная нормальная форма (ДНФ) — $R = \forall_{i=1}^{s} K_i$, где $K_i \neq K_j$ при $i \neq j$, K_i - элементарные коньюнкции.

• Совершенная ДНФ (СДНФ) — ДНФ, состоящая из различных полных элементарных конъюнкций.

Булевая функция может быть представлена в виде ДНФ не единственным образом.

СДНФ и СКНФ обеспечивают единственность представления любой булевой функции, но они неудобны при технической реализации булевой функции, поэтому их преобразуют в наиболее простые формы, более рациональные с точки зрения их реализации.
Вводят индекс простоты, характеризующий сложность ДНФ. В качестве индекса используют количество переменных и их отрицаний, их литералов.

• Минимальная ДНФ — ДНФ, содержащая наименьшее количество литералов среди всех ДНФ, реализующих данную булевую функцию.

Замечание:
Число различных элементарных конъюнкций от n переменных равно 3^n, так как любая переменная может входить в конъюнкцию, не входить в конъюнкцию или входить с отрицанием, следовательно количество ДНФ равно 2^{3^n}.

• Импликанта булевой функции $f(x_1, \dots, x_n)$ — булевая функция $g(x_1, \dots, x_n)$, если для любого набора $\bar{\alpha} \in E_2^n$ из $g(\bar{\alpha}) = 1$, следует, что $f(\bar{\alpha}) = 1$ или $g \vee f \equiv f$.
f — имплицента булевой функции $g(x_1, \dots, x_n)$.

Замечание:
Всякая элементарная конъюнкция, входящая в булевую функцию является её импликантой.
Конъюнкция любого числа импликант также импликанта болевой функции.

• Импликанта от $f(x_1, \dots, x_n)$, являющаяся элементарной конъюнкцией, называется простой, если никакая её часть не является булевой функцией f.

• Сокращенная ДНФ — ДНФ, реализующая f и состоящая из всех простых импликант.

• Тупиковая сокращенная ДНФ — сокращенная ДНФ, если отбрасывание любых элементов конъюнкции или литерала приводит ее к неэквивалентной ДНФ.

• Кратчайшая ДНФ — ДНФ, содержащая минимальное количество импликант.

Замечание:
Булевая функция может иметь несколько тупиковых ДНФ.

• Минимальная ДНФ — тупиковая ДНФ f, содержащая наименьшее количество литералов.

Замечание:
Булевая функция может иметь несколько минимальных и кратчайших ДНФ; существует тупиковая ДНФ, не являющаяся кратчайшей, и существует кратчайшая ДНФ, не являющаяся минимальной.

Утверждение:
Минимальная ДНФ булевой функции $f(x_1, \dots, x_n)$ получается из сокращенной ДНФ путем удаления некоторых элементарных конъюнкций.

⧫ Покажем, что все импликанты, составляющие минимальную ДНФ, являются простыми.
От противного:
Пусть $R = k_1 \vee k$, где k_1 -не простая конъюнкция, k - дизъюнкция остальных конъюнкций, которые входят в разложение булевой функции.
Так как k_1 - не простая конъюнкция, то её можно представить в виде произведение других конъюнкций: $k_1 = k_1' \cdot k_2''$, где k_1' - импликанта f, то есть $k_1' \vee f = f$. Тогда $f = (k_1 \vee k) \vee k_1' = (k_1' \cdot k_2'' \vee k) \vee k_1' = k_1' k_2'' \vee k k_1' = k_1' \vee k$, что меньше, чем $k_1' \cdot k_2''$ $\Rightarrow R$ не минимальная, получили противоречие. ⊠
Этапы минимизации булевой функции:

1. Построение СДНФ;
2. Получение сокращенной ДНФ;
3. Нахождение всех тупиковых ДНФ;
4. Выбор из тупиковых ДНФ минимальных;

Теорема. 1 *(Квайна)*
Если в произвольной ДНФ булевой функции произвести всевозможные обобщенные склеивания, а затем выполнить все поглощения, то получится сокращенная ДНФ.

I) Метод Блейка-Порецкого:

1. Построение СДНФ;
2. По теореме Квайна, производим все обобщённые склеивания, пока возможно, по правилу:
   $x k_1 \vee \bar{x} k_2 = x k_1 \vee \bar{x} k_2 \vee k_1 k_2$
3. По теореме Квайна производим всевозможные поглопоглощения по правилу:
   $k_1 \vee k_1 k_2 = k_1$

4. удаляем лишние конъюнкции по правилу обобщённого склеивания:
   $xk_1 \vee \bar{x}k_2 \vee k_1k_2 = xk_1 \vee \bar{x}k_2$

Пример:
$\omega(f) = (11011011)$

x	y	z	$f(x, y, z)$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	1

1. $f(x, y, z) = \bar{x}\bar{y}\bar{z} \vee \bar{x}\bar{y}z \vee \bar{x}yz \vee x\bar{y}\bar{z} \vee xy\bar{z} \vee xyz$

2. $\bar{x}\bar{y}\bar{z} \vee \bar{x}\bar{y}z = \bar{x}\bar{y}\bar{z} \vee \bar{x}\bar{y}z \vee \bar{x}\bar{y}$
   $\bar{x}\bar{y}z \vee \bar{x}yz = \bar{x}\bar{y}z \vee \bar{x}yz \vee \bar{x}z$
   $\bar{x}\bar{y}\bar{z} \vee x\bar{y}\bar{z} = \bar{x}\bar{y}\bar{z} \vee x\bar{y}\bar{z} \vee \bar{y}\bar{z}$
   $xy\bar{z} \vee xyz = xy\bar{z} \vee xyz \vee xy$
   $\bar{x}\bar{y}\bar{z} \vee \bar{x}\bar{y}z \vee \bar{x}yz \vee x\bar{y}\bar{z} \vee xy\bar{z} \vee xyz \vee \bar{x}\bar{y} \vee \bar{x}z\bar{y}\bar{z} \vee xy$

3. Поглощаем:
   $\bar{x}\bar{y}z \vee \bar{x}\bar{y}z \vee \bar{x}\bar{y} = \bar{x}\bar{y}$
   $x\bar{y}\bar{z} \vee \bar{y}\bar{z} = \bar{y}\bar{z}$
   $\bar{x}yz \vee \bar{x}z = \bar{x}z$
   $xyz \vee xyz \vee xy = xy$
   $f(x, y, z) = \bar{x}\bar{y} \vee \bar{x}z \vee \bar{y}\bar{z} \vee xy$

4. Склеиваем:
   $f(x, y, z) = \bar{x}z \vee \bar{y}\bar{z} \vee xy$

II) Метод Квайна:
2 операции:

а) попарное неполное склеивание:
$kx \vee k\bar{x} = kx \vee k\bar{x} \vee k$

б) элементарное поглощение:
$kx^{\sigma} \vee k = k$

Теорема. 2 *(Квайна)*
Исходя из СДНФ, если произвести всевозможные операции а) и б), то получим сокращенную ДНФ

Алгоритм Квайна:

1. По таблице истинности стротм СДНФ;

2. Выполняем всевозможные операции неполного попарного склеивания для элементарных конъюнкций длины n

3. Выполняем всевозможные операции элементарного поглощения для элементарных конъюнкций длины $n-1$

4. В результате получится множество элементарных конъюнкций, состоящее из 2 подмножеств: элементарных конъюнкций длины n и элементарных конъюнкций длины $n-1$

5. Если множество элементарных конъюнкций длины $n-1$ не пусто, то заново выполняем операции а) и б)

6. Завершается алгоритм, когда подмножество элементарных конъюнкций не будет либо пустым, либо нельзя будет выполнить ни одной операции. С результате получим сокращённую ДНФ

Переход от СДНФ к сокращенной ДНФ происходит с помощью импликантной матрицы Квайна. В этой матрице полные элементарные конъюнкции СДНФ записываются в заголовке столбцов, а простые импликанты сокращенных ДНФ в заголовках строк. На пересечении ставится «+», если импликант в строке входит в конъюнкцию k_j.
Минимальные ДНФ строятся по этой матрице:
Вначале строится тупиковая ДНФ, в которой выбирается минимальное число простых импликант сокращенной ДНФ, дизъюнкция которых накроет плюсами все столбцы импликантной матрицы, т.е. каждый столбец содержит «+», стоящий на пересечении со строкой, соответствующей одной из выбранных импликант.
Далее из тупиковых ДНФ выбирается минимальная ДНФ, имеющая наименьшее число вхождений переменных из всех построенных тупиковых из матрицы.

Замечание:
Для столбцов, имеющих только один «+», соответствующие им простые импликанты сокращенной ДНФ являются базисными, дизъюнкции которых составляют ядро булевой функции, которое обязательно входит в минимальную ДНФ.

Пример:

1. $f(x,y,z) = \bar{x}\bar{y}\bar{z} \vee \bar{x}\bar{y}z \vee \bar{x}yz \vee x\bar{y}\bar{z} \vee xy\bar{z} \vee xyz$

2. Попарное неполное склеивание:
$\bar{x}\bar{y}\bar{z} \vee \bar{x}\bar{y}z \vee \bar{x}yz \vee x\bar{y}\bar{z} \vee xy\bar{z} \vee xyz \vee \bar{x}\bar{y} \vee \bar{y}\bar{z} \vee \bar{x}z \vee yz \vee x\bar{z} \vee xy$

3. Сокращённая ДНФ:
$f(x,y,z) = \bar{x}\bar{y} \vee \bar{y}\bar{z} \vee \bar{x}z \vee yz \vee x\bar{z} \vee xy$

	$\bar{x}\bar{y}\bar{z}$	$\bar{x}\bar{y}z$	$\bar{x}yz$	$x\bar{y}\bar{z}$	$xy\bar{z}$	xyz	
$\bar{x}\bar{y}$	$\oplus$	$\oplus$					V
$\bar{y}\bar{z}$	$\pm$			$\pm$			W
$\bar{x}z$		$\pm$	$\pm$				W
yz			$\oplus$			$\oplus$	V
$x\bar{z}$				$\oplus$	$\oplus$		V
xy					$\pm$	$\pm$	W

Тупиковые ДНФ:
$\bar{x}\bar{y} \vee yz \vee x\bar{z}$ и
$y\bar{z} \vee \bar{x}z \vee xy$

Глава 2

Теория графов

Основные понятия

• **Граф** - следующая упорядоченная пара: $G = (V, E)$, где V - непустое множество, состоящая из вершин графа, а $E \subseteq V^{(2)}$, где $V^{(2)}$ - все двухэлементные подмножества из V.

$V^{(2)} = \{\{v, w\} | v, w \in V\}$

• Граф **конечный**, если множество вершин конечно$|V| = n$.

Если $|E| = n$, то граф G обозначается $G(n, m)$

$n = |V|$ - порядок графа G.
$m = |E|$ - размер графа G.
Если $n = 1$, то граф тривиальный.
• Граф **простой**, если он не имеет петель - $\{v, w\}$ и не имеет кратных ребер, то есть несколько пар $\{v, w\}$.

Вершины v и w **смежные**, обозначают $v\tilde{w}$, если ребро $\{v, w\} \in E$.

Ребро $e = \{v, w\} = vw$ инцидентно вершинам v и w, а эти вершины v, w называют концами e.

Два ребра называют смежными, если существует $v \in V$, которой они инцидентны или существует их общий конец.

Пусть есть $v \in V(G)$. тогда множество всех вершин u таких, что $u\tilde{v}$, $\quad N_G(v) = \{u \in V(G) | u\tilde{v}\}$ называют окружением вершины v.

$N_G(v) \cup \{v\} = N_G[v] = N[v]$ — замкнутое окружение вершины v.

• **Степень вершины** $v \quad deg_G(v) = |N_G(v)|$ равна числу рёбер, выходящих из данной вершины.

Если $V' \subseteq V(G)$, то окружение множества вершин V' - множество $N_G(V') = \bigcup\limits_{v \in V'} N_G(v)$

• Вершина, которая смежна с любой вершиной из V называется **доминирующей**, то есть $v \in V;\ \forall u \in V \setminus \{v\},\ v \sim u$

Если $v \in V$, такая что для любой $u \in V \setminus \{v\}$ $v \sim u$, то v - доминирующая.

• **Доминирующее множество** - множество U, такое что для любого $v \in V(G) \setminus \{u\}$ существует $u \in U$, такое что $v \sim u$.

• **Число доминирования** $\gamma(G)$ - мощность наименьшего доминирующего множества.

• Если $\deg(v) = 0$, то v - **изолированная**.

• Если $\deg(v) = 1$, то v - **висячая** или **лист**.

Минимальная степень вершин - $\delta(G) \geq 0$.

Максимальная степень вершин - $\Delta(G) \leq n - 1$.

• Список степеней, упорядоченный по возрастанию - **степенная последовательность** $\delta = d_1 \leq d_2 \leq \cdots \leq d_n \leq \Delta$.

Регулярный/однородный граф степени k (k-регулярный) - граф, такой что $\deg(v) = k$, $v \in V$. При $k = 3$ граф кубический.

• **Псевдограф** — граф, который может содержать петли и кратные ребра, кратные петли.

• Мультиграф — граф, который может содержать кратные ребра.

• Если EV^2 (составлено из упорядоченных двоек/пар), то граф **G—ориентированный** (орграф), а его ребра — дуги.

Если v — начало дуги (v, w), то дуга исходит из v.
Если w — конец дуги (v, w), то дуга заходит в w.

• Количество заходящих дуг — **полустепень захода** $deg - w$.

• Количество исходящих дуг — **полустепень исхода** $deg + v$.
Если в E существует состоящие из более чем двух вершин $e\{v,\ w,\ u\}$, то G —**гиперграф**.

Для любого(мульти/псевдо) графа справедлива лемма:

Лемма. *Лемма о рукопожатиях:*
$deg(v_1) + deg(v_2) + \ldots + deg(v_n) = 2m, \quad \forall i, \quad v_i \in V.$

⧫ Это следует из того, что вклад каждого ребра в левую часть такой же, что и петли в правую часть равенства, равный двум. ⊠

Следствие:
Количество вершин нечетных степеней четно.

On — пустой граф — граф, состоящий из n изолированных вершин (нет ребер).

Kn — полный граф — граф, где все вершины попарно смежны: $m = C_n^2$.

Pn —цепь на n вершинах — граф, у которого 2 листа, а остальные вершины имеют степень 2. Длина (см. далее) равна $n-1$.

Cn —цикл на n вершинах — связный (см. далее) граф, у которого все вершины имеют степень 2. $G' = (V', E')$ — подграф графа G, если $V' \subseteq V, \quad E \subseteq E'$.

• **Собственный подграф** — граф G', где $V'V$ и/или EE'.

Если $V'V(G)$, то **порожденный (индуцированный) подграф** множества вершин $V'G[V'] = def(V', E')$, где $E' = vu \in E(G)|v, u \in V'$.
$W \subseteq V(G) \Rightarrow G[V \setminus W] = defG - W$
$F \subseteq E(G) \Rightarrow G + F = (V, E(G) \cup F) \Rightarrow G - F = (V, E(G) \setminus F)$
$V = \{v\} \Rightarrow G - \{v\}$ аналогично $G - v$
$F = \{e\} \Rightarrow G + \{e\}$ аналогично $G + e$
$\Rightarrow G - \{e\}$ аналогично $G - e$

Независимое множество вершин $W \subseteq V(G) — W$, такое что $G[W]$ - пустой.
Мощность максимального W — число независимостей $\alpha(G)$.
Клика $W \subseteq V(G) — W$, такое что $G[W]$ - полный.
Мощность максимального W — кликовое число $w(G)$.
• **Остов (субграф)** — подграф $G' = (V', E')$, такой что $V' = V(G)$.

Пусть $G = (V, E)$ — произвольный подграф.
Реберный граф — $L(G)$, такой что:
1) вершины L — ребра G
2) 2 вершины ij и kl принадлежащие $E(G)$ — смежные, если в G ij и kl — смежные.
$deg(ij)$ в $L(G) = deg(i)$ в $G + deg(j)$ в $G\breve{}2$.
Замечание: порядок $|L(G)| = m$, если $G(n, m)$.

Утверждение: размер $L(G) = m_L = \frac{1}{2} \cdot \sum\limits_{i=1}^{n} d_i^2 - m$.

♦ Вершина i в G имеет степень d_i, то в $L(G)$ она образует $C_{d_i}^2$ ребер, каждая пара ребер—вершина в$L(G) \Rightarrow m_L = \sum\limits_{i=1}^{n} C_{d_i}^2 = \frac{1}{2} \cdot \sum\limits_{i=1}^{n} d_i(d_i - 1)$=[по дистрибутивности и лемме о рукопожатиях] $=\frac{1}{2} \cdot \sum\limits_{i=1}^{n} d_i^2 - m$. ⊠

Следствие:$\sum\limits_{i=1}^{n} d_i^2 = \sum\limits_{ij \in E(G)} (d_i + d_j)$ — первый индекс Загреба
♦ $2m_L = \sum\limits_{ij \in E(G)} d_ij = \sum\limits_{ij \in E(G)} (d_i + d_j - 2) = \sum\limits_{ij \in E(G)} (d_i + d_j) - 2m;$

$2(m_L + m) = \sum\limits_{ij \in E(G)} (d_i + d_j)$ и $2(m_L + m) = \sum\limits_{i=1}^{2} d_i^2$. ⊠

• **Помеченный граф** — 1) граф, вершинам или ребрам которого присвоены какие-либо метки (числа, буквы); 2)граф порядка n, если его вершинам присвоить попарно различные номера от 1 до n.

Теорема. 1
Количество помеченных графов порядка $n = 2^{C_n^2}$.

♦ По определению количество ребер в полном графе порядка n равно числу всевозможных пар вершин равное $C_n^2 \Rightarrow$ количество всех графов с фиксированным множеством вершин равное числу всех подмножеств множества всевозможных пар вершин $= 2^{C_n^2}$. ⊠