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. *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 $h(x) \equiv f(x \oplus \alpha_1, \dots, x \oplus \alpha_n)$
$h(0) = f(\alpha_1, \dots, \alpha_n) = c,\ c = const$
$h(1) = f(\bar{\alpha}_1, \dots, \bar{\alpha}_n) = c$
$h(x) = c \Rightarrow \bar{c} = \bar{h}(x) \Rightarrow 0, 1 \in [\{\bar{x}, f\}]$ ⊠