МИНИСТЕРСТВО НАУКИ И ОБРАЗОВАНИЯ РФ
ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Рагимханов В. Р.

ДИСКРЕТНАЯ МАТЕМАТИКА
Часть IV
Булевы функции

Махачкала
Издательство ДГУ
2019

Издается по решению РИС ДГУ

Рагимханов В. Р. Дискретная математика. Часть IV. Булевы функции. — Махачкала, Издательство ДГУ, 2019. — 102 с.

В пособии изложены основные сведения о булевых функциях — важнейшем классе дискретных функций. В ней излагаются различные формы представления булевых функций, доказываются ключевые теоремы о системах булевых функций. Каждый параграф заканчивается упражнениями, способствующих закреплению материала.

Рецензенты: Раджабов К. Я. — декан факультета «Прикладная информатика (в экономике)» ДГИНХ, кандидат физико-математических наук;

Галяев В. С. — заведующий кафедрой «Информационные технологии» ДГИНХ, кандидат физико-математических наук.

Оглавление

1. Булев куб $\mathbb{B}^n$

1.1. Обозначения и напоминания

Здесь мы приводим обозначения и некоторые свойства алгебры $\mathbb{B}^n$, которые полезно вспомнить в связи с дальнейшим изложением.

- ✓ $\mathbf{n}$ — n-элементное множество $\{1, 2, \ldots, n\}$.
- ✓ $\mathbf{n}_<$ — n-элементная цепь $\{1 < 2 < \ldots < n\}$.
- ✓ $\mathscr{B}(\mathbf{n})$ — множество всех подмножеств множества $\mathbf{n}$.
- ✓ На двухэлементной булевой алгебре $\mathbb{B} = \{\mathbf{0}, \mathbf{1}\}$ определен и фиксирован естественный порядок: $\mathbf{0} < \mathbf{1}$.
- ✓ Для $\alpha \in \mathbb{B}$ полагаем
$$|\alpha| = \begin{cases} 0, & \text{если } \alpha = \mathbf{0}; \\ 1, & \text{если } \alpha = \mathbf{1}. \end{cases}$$
Вместо $|\alpha|$ мы будем писать просто α, если из контекста ясно, что подразумевается под α : число или булев элемент.
- ✓ Через $\tilde{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ обозначаем элементы $\mathbb{B}^n$.

✓ Для $\tilde{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ обозначим через $||\tilde{\alpha}||$ количество ненулевых его компонент:

$$||\tilde{\alpha}|| \stackrel{\text{def}}{:=} \sum_{i=1}^{n} \alpha_i.$$

✓ (**отображение ν**). Для $\tilde{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ определим его номер $\nu(\tilde{\alpha})$

$$\nu(\tilde{\alpha}) = \alpha_1 2^{n-1} + \alpha_2 2^{n-2} + \ldots + \alpha_{n-1} 2 + \alpha_n,$$
$$(\text{точнее} \quad \nu(\tilde{\alpha}) = |\alpha_1| 2^{n-1} + |\alpha_2| 2^{n-2} + \ldots + |\alpha_{n-1}| 2 + |\alpha_n|).$$

Из определения ясно, что на $\tilde{\alpha}$ можно смотреть как на булевый вариант двоичного представления числа $\nu(\tilde{\alpha})$. Таким образом, если для целого неотрицательного k имеем двоичное разложение

$$k = \alpha_1 2^{n-1} + \alpha_2 2^{n-2} + \ldots + \alpha_{n-1} 2 + \alpha_n,$$

то

$$\nu(\alpha_1, \alpha_2, \ldots, \alpha_n) = k \quad \text{и} \quad \nu^{-1}(k) = (\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Здесь ν^{-1} — отображение, обратное для отображения ν, ставящее в соответствие каждому целому неотрицательному k его булев двоичный код $(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Из сказанного выше получаем справедливость следующего предложения.

Предложение 1.1. *Отображение*

$$\nu + 1\colon \mathbb{B}^n \to \mathbf{2^n},$$

которое каждому $\tilde{\alpha} \in \mathbb{B}^n$ *ставит в соответствие число* $\nu(\tilde{\alpha}) + 1$, *является биективным отображением* $\mathbb{B}^n$ *на* $\mathbf{2^n} = \{1, 2, \dots, 2^n\}$.

✓ (**отображение** μ). Для $\tilde{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_n)$ определим подмножество $\mu(\tilde{\alpha})$ множества $\mathbf{n} = \{1, 2, \dots, n\}$:

$$\mu(\tilde{\alpha}) = \{i \in \mathbf{n} \,|\, \alpha_i = \mathbf{1}\}.$$

Отображение $\mu\colon \tilde{\alpha} \mapsto \mu(\tilde{\alpha})$ является, очевидно, биективным отображением из $\mathbb{B}^n$ на множество $\mathscr{B}(\mathbf{n})$ всех подмножеств множества $\mathbf{n}$. Обратным для отображения μ будет отображение μ^{-1}, которое каждому множеству $A \subseteq \{1, 2, \dots, n\}$ ставит в соответствие n-мерный набор

$$\mu^{-1}(A) = (\alpha_1, \alpha_2, \dots, \alpha_n), \quad \text{где} \quad \alpha_i = \begin{cases} \mathbf{1}, & \text{если } i \in A; \\ \mathbf{0}, & \text{если } i \notin A. \end{cases}$$

Итак, справедливо следующее предложение.

Предложение 1.2. *Отображение*

$$\mu\colon \mathbb{B}^n \to \mathscr{B}(\boldsymbol{n})$$

является биективным отображением.

1.2. $\mathbb{B}^n$ как упорядоченное множество

В этом разделе мы определим на $\mathbb{B}^n$ два отношения порядка: лексикографический порядок и порядок произведения; установим некоторые утверждения об этих отношениях порядка и их взаимосвязи.

1.2.1. Лексикографический порядок на $\mathbb{B}^n$.

Считая, что $\mathbf{0} < \mathbf{1}$, для n-мерных наборов $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ и $\tilde{\beta} = (\beta_1, \ldots, \beta_n)$ из $\mathbb{B}^n$, полагаем:

$$
\checkmark\ (\alpha_1, \ldots, \alpha_n) < (\beta_1, \ldots, \beta_n), \quad
\begin{array}{ll}
\text{если} & \alpha_1 < \beta_1, \\
\text{или} & \alpha_1 = \beta_1, \ \text{и } \alpha_2 < \beta_2, \\
\text{или} & \alpha_1 = \beta_1, \alpha_2 = \beta_2 \text{ и } \alpha_3 < \beta_3, \\
\ldots & \ldots\ldots\ldots\ldots\ldots\ldots \\
\text{или} & \alpha_1 = \beta_1, \ldots, \alpha_{n-1} = \beta_{n-1} \text{ и } \alpha_n < \beta_n.
\end{array}
$$

✓ $\tilde{\alpha} \leqslant \tilde{\beta}$ означает, как всегда, что $\tilde{\alpha} < \tilde{\beta}$ или $\tilde{\alpha} = \tilde{\beta}$.

Относительно введенного лексикографического порядка $\mathbb{B}^n$ является линейно упорядоченным множеством, или, по-другому, цепью ($\equiv$ любые два элемента $\tilde{\alpha}$ и $\tilde{\beta}$ из $\mathbb{B}^n$ являются $\leqslant$-сравнимыми). Так, например,

$$\mathbb{B}^2\colon (\mathbf{0}, \mathbf{0}) < (\mathbf{0}, \mathbf{1}) < (\mathbf{1}, \mathbf{0}) < (\mathbf{1}, \mathbf{1});$$
$$\mathbb{B}^3\colon (\mathbf{0}, \mathbf{0}, \mathbf{0}) < (\mathbf{0}, \mathbf{0}, \mathbf{1}) < (\mathbf{0}, \mathbf{1}, \mathbf{0}) < (\mathbf{0}, \mathbf{1}, \mathbf{1}) < (\mathbf{1}, \mathbf{0}, \mathbf{0}) < \ldots < (\mathbf{1}, \mathbf{1}, \mathbf{1}).$$

Линейный лексикографический порядок на $\mathbb{B}^n$ позволяет каждому элементу $\tilde{\alpha}$ из $\mathbb{B}^n$ приписать свой порядковый номер относительно этого упорядочения. Определенная в предыдущем пункте функция номер $\nu\colon \tilde{\alpha} \mapsto \nu(\tilde{\alpha})$ как раз и осуществляет такую нумерацию (начиная с нуля):

$$\mathbb{B}^2\colon\ \underbrace{(\mathbf{0},\mathbf{0})}_{\text{0-й номер}} < \underbrace{(\mathbf{0},\mathbf{1})}_{\text{1-й номер}} < \underbrace{(\mathbf{1},\mathbf{0})}_{\text{2-й номер}} < \underbrace{(\mathbf{1},\mathbf{1})}_{\text{3-й номер}};$$

$$\mathbb{B}^3\colon\ \underbrace{(\mathbf{0},\mathbf{0},\mathbf{0})}_{\text{0-й номер}} < \underbrace{(\mathbf{0},\mathbf{0},\mathbf{1})}_{\text{1-й номер}} < \underbrace{(\mathbf{0},\mathbf{1},\mathbf{0})}_{\text{2-й номер}} < \underbrace{(\mathbf{0},\mathbf{1},\mathbf{1})}_{\text{3-й номер}} < \underbrace{(\mathbf{1},\mathbf{0},\mathbf{0})}_{\text{4-й номер}} < \ldots < \underbrace{(\mathbf{1},\mathbf{1},\mathbf{1})}_{\text{7-й номер}}.$$

Лексикографический порядок на $\mathbb{B}^n$ тесно связан с двоичной арифметикой. Так, из способа сравнения двух чисел, записанных в двоичной системе счисления, и равенства $\nu(\alpha_1,\ldots,\alpha_n) = \alpha_1 2^{n-1} + \alpha_2 2^{n-2} + \ldots + \alpha_{n-1}2 + \alpha_n$ непосредственно следует справедливость следующего предложения.

Предложение 1.3. *Для любых наборов $\tilde{\alpha} = (\alpha_1,\ldots,\alpha_n)$ и $\tilde{\beta} = (\beta_1,\ldots,\beta_n)$ из $\mathbb{B}^n$ справедливы следующие утверждения.*

1. $\tilde{\alpha} \leqslant \tilde{\beta} \iff \nu(\tilde{\alpha}) \leqslant \nu(\tilde{\beta})$.

2. *Если* $\tilde{\alpha} \wedge \tilde{\beta} = \mathbf{0}$, *то* $\nu(\tilde{\alpha} \vee \tilde{\beta}) = \nu(\tilde{\alpha}) + \nu(\tilde{\beta})$.

Т. к. $(\mathbb{B}^n, \leqslant)$ — конечное линейно упорядоченное множество, то оно изоморфно стандартной цепи $\mathbf{m}_< = \{1 < 2 < 3 < \cdots < m\}$, где m равно количеству элементов

$\mathbb{B}^n$, т. е. $m = 2^n$. Упомянутый изоморфизм осуществляет отображение $\tilde{\alpha} \mapsto \nu(\tilde{\alpha})+1$, уже встречавшееся нам в предыдущем разделе. Таким образом, установлена следующая теорема.

Теорема 1.1. *Отображение $\nu + 1$ устанавливает изоморфизм линейно упорядоченных множеств $(\mathbb{B}^n, \leqslant)$ и $\mathbf{2}^{\mathbf{n}}_{<} = \{1 < 2 < 3 < \cdots < 2^n\}$:*

$$(\mathbb{B}^n, \leqslant) \cong \mathbf{2}^{\mathbf{n}}_{<}.$$

1.2.2. Порядок произведения на $\mathbb{B}^n$.

Считая, что $\mathbf{0} < \mathbf{1}$, для n-мерных наборов $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ и $\tilde{\beta} = (\beta_1, \ldots, \beta_n)$ из $\mathbb{B}^n$ полагаем:

✓ $(\alpha_1, \ldots, \alpha_n) \preccurlyeq (\beta_1, \ldots, \beta_n)$, если $\alpha_1 \leqslant \beta_1, \alpha_2 \leqslant \beta_2, \ldots, \alpha_n \leqslant \beta_n$.

Отметим, что определенное отношение порядка $\preccurlyeq$ не является линейным отношением порядка на $\mathbb{B}^n$; так, например,

$$(\mathbf{0}, \mathbf{1}) \not\preccurlyeq (\mathbf{1}, \mathbf{0}) \text{ и } (\mathbf{1}, \mathbf{0}) \not\preccurlyeq (\mathbf{0}, \mathbf{1}) \text{ в } \mathbb{B}^2.$$

В то время как с лексикографическим порядком $\mathbb{B}^n$ изоморфно стандартному линейно упорядоченному множеству $\mathbf{2}^{\mathbf{n}}_{<}$, упорядоченное множество $(\mathbb{B}^n, \preccurlyeq)$ изоморфно другому стандартному упорядоченному множеству $\mathscr{B}(\mathbf{n})$. Этот факт мы зафиксируем в теореме 1.2, вытекающей из предложения 1.2 и следующего предложения.

Предложение 1.4. *Для любых наборов* $\tilde\alpha = (\alpha_1, \dots, \alpha_n)$ *и* $\tilde\beta = (\beta_1, \dots, \beta_n)$ *из* $\mathbb{B}^n$ *справедлива следующая эквивалентность*

$$\tilde\alpha \preccurlyeq \tilde\beta \iff \mu(\tilde\alpha) \subseteq \mu(\tilde\beta).$$

◀Пусть $\tilde\alpha = (\alpha_1, \dots, \alpha_n), \tilde\beta = (\beta_1, \dots, \beta_n) \in \mathbb{B}^n$ и $A = \mu(\tilde\alpha), B = \mu(\tilde\beta) \subseteq \{1, 2, \dots, n\}$. Пусть $\tilde\alpha \preccurlyeq \tilde\beta$; тогда $A \subseteq B$. Действительно, если $k \in A$, то по определению $\mu(\tilde\alpha)$ получаем, что $\alpha_k = \mathbf{1}$. А т. к. $\tilde\alpha \preccurlyeq \tilde\beta$, то $\alpha_k \leqslant \beta_k$ и, значит, $\beta_k = \mathbf{1}$. Это означает, что $k \in B$, т. е. $A \subseteq B$.

Обратно, пусть $A \subseteq B$, тогда $\tilde\alpha \preccurlyeq \tilde\beta$. Действительно, т. к. $A \subseteq B$, то справедлива импликация:

$$\text{если} \quad k \in A, \quad \text{то} \quad k \in B.$$

Но это означает, что справедлива импликация:

$$\text{если} \quad \alpha_k = \mathbf{1}, \quad \text{то} \quad \beta_k = \mathbf{1}.$$

Отсюда получаем, что для любого $k = 1, 2, \dots, n$, $\alpha_k \leqslant \beta_k$, т. е. $\tilde\alpha \preccurlyeq \tilde\beta$. ▶

Теорема 1.2. *Отображение*

$$\mu\colon \mathbb{B}^n \to \mathscr{B}(\boldsymbol{n})$$

устанавливает изоморфизм упорядоченных множеств $(\mathbb{B}^n, \preccurlyeq)$ *и* $\mathscr{B}(\boldsymbol{n})$*:*

$$(\mathbb{B}^n, \preccurlyeq) \cong \mathscr{B}(\boldsymbol{n}).$$

Пользуясь указанным изоморфизмом и известными нам фактами о $\mathscr{B}(\mathbf{n})$ (или непосредственно из определений), получаем следующие результаты об упорядоченном множестве $(\mathbb{B}^n, \preccurlyeq)$.

✓ $(\mathbb{B}^n, \preccurlyeq)$ — конечная решетка с наименьшим элементом $\tilde{\mathbf{0}} = (\mathbf{0}, \ldots, \mathbf{0})$ и наибольшим элементом $\tilde{\mathbf{1}} = (\mathbf{1}, \ldots, \mathbf{1})$.

При этом

$$\begin{gathered}\sup\{\tilde{\alpha}, \tilde{\beta}\} = \tilde{\alpha} \vee \tilde{\beta},\\ \inf\{\tilde{\alpha}, \tilde{\beta}\} = \tilde{\alpha} \wedge \tilde{\beta},\\ \neg(\alpha_1, \ldots, \alpha_n) = (\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_n),\end{gathered}$$

где в левых частях равенств стоят «порядковые» операции супремума, инфимума и дополнения, а в левых частях — знакомые нам булевы операции суммы, произведения и дополнения. Таким образом, именно порядок произведения $\preccurlyeq$ на $\mathbb{B}^n$ является естественным порядком на булевой алгебре $(\mathbb{B}^n, \vee, \wedge, \bar{\ }, \mathbf{0}, \mathbf{1})$.

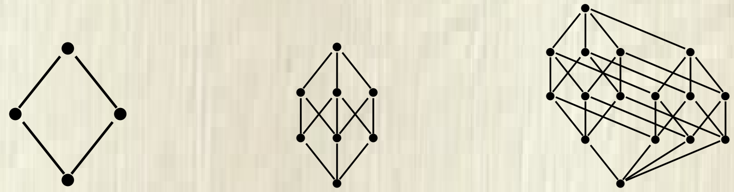
✓ *Отношение покрытия* $\tilde{\alpha} \prec\!\cdot\, \tilde{\beta}$: элемент $\tilde{\beta}$ *покрывает* $\tilde{\alpha}$ тогда и только тогда, когда $\tilde{\alpha}$ и $\tilde{\beta}$ отличаются лишь в одной компоненте, причем эта компонента в $\tilde{\alpha}$ равна $\mathbf{0}$, а в $\tilde{\beta}$ равна $\mathbf{1}$:

$$\tilde{\alpha} \prec\!\cdot\, \tilde{\beta} \iff \begin{array}{l}\tilde{\alpha} = (\sigma_1, \ldots, \sigma_{k-1}, \mathbf{0}, \sigma_k, \ldots, \sigma_n),\\ \tilde{\beta} = (\sigma_1, \ldots, \sigma_{k-1}, \mathbf{1}, \sigma_k, \ldots, \sigma_n)\end{array} \quad \text{для некоторого} \quad k.$$

— **(Напоминание)** Пусть $(P, \leqslant)$ — упорядоченное множество и $x, y \in P$. Говорим, что y *покрывает* x и пишем $x \lessdot y$, если из $x < z \leqslant y$ следует $z = y$, иначе говоря:

$$x \lessdot y \iff x < y \quad \text{и} \quad [x, y] = \{x, y\}.$$

✓ *Диаграммы Хассе.* На следующих рисунках приведены диаграммы Хассе для $\mathbb{B}^2, \mathbb{B}^3$ и $\mathbb{B}^4$.



✓ $\rho(\tilde{\alpha})$ — ранговая функция решетки $(\mathbb{B}^n, \preccurlyeq)$ дается формулой:

$$\rho(\tilde{\alpha}) = \sum_{i=1}^{n} \alpha_i \qquad (= \text{числу ненулевых компонент } \tilde{\alpha}).$$

✓ *Длина* $l(\mathbb{B}^n)$ решетки $(\mathbb{B}^n, \preccurlyeq)$ равна n:

$$l(\mathbb{B}^n) = n.$$

— **(Напоминание)** *Длина* $l(P)$ упорядоченного множества $(P, \leqslant)$ равна k, где k — натуральное число, если существует цепь в P, состоящая из $k+1$ элементов, и все цепи в P содержат $\leqslant k+1$ элементов.

— Пример цепи в $(\mathbb{B}^4, \preccurlyeq)$ длины $l(\mathbb{B}^4) = 4$:

$$(\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{0}) \prec (\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1}) \prec (\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1}) \prec (\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1}) \prec (\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1}).$$

— Количество цепей в $(\mathbb{B}^n, \preccurlyeq)$ максимально возможной длины $l(\mathbb{B}^n) = n$ равно $n!$

✓ *Ширина* $s(\mathbb{B}^n)$ (или *число Шпернера*) решетки $(\mathbb{B}^n, \preccurlyeq)$ равна $\binom{n}{\lfloor n/2 \rfloor}$:

$$s(\mathbb{B}^n) = \binom{n}{\lfloor n/2 \rfloor}.$$

— **(Напоминание)** *Число Шпернера* $s(P)$ или *ширина* упорядоченного множества $(P, \leqslant)$ равно k, где k — натуральное число, если существует антицепь в P, состоящая из k элементов, и все антицепи в P содержат $\leqslant k$ элементов.

— Пример антицепи в $(\mathbb{B}^4, \preccurlyeq)$ длины $s(\mathbb{B}^4) = \binom{4}{\lfloor 4/2 \rfloor} = 6$:

$$(\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1}),(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1}),(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0}),(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1}),(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0}),(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0}).$$

— Антицепями, содержащими $s(\mathbb{B}^n)$ элементов в $\mathbb{B}^n$ являются только два средних уровня рангов $\lfloor n/2 \rfloor$ и $\lceil n/2 \rceil$ (которые совпадают при четном n).

✓ *Число Дилуорса* $d(\mathbb{B}^n)$ решетки $(\mathbb{B}^n, \preccurlyeq)$ равно $\binom{n}{\lfloor n/2 \rfloor}$:

$$d(\mathbb{B}^n) = \binom{n}{\lfloor n/2 \rfloor}.$$

— **(Напоминание)** *Число Дилуорса* $d(P)$ упорядоченного множества P равно k, где k — натуральное число, если P можно разбить на k блоков-цепей из P и любое другое разбиение P на блоки-цепи содержит $\geqslant k$ блоков.

— **(Напоминание)** *Теорема Дилуорса.* Пусть P — конечное упорядоченное множество. Наименьшее число непересекающихся цепей, на которые может быть разложено множество P, равно наибольшей мощности антицепи в P:

$$d(P) = s(P).$$

— Пример разбиения решетки $(\mathbb{B}^4, \preccurlyeq)$ на $d(\mathbb{B}^n) = \binom{4}{\lfloor 4/2 \rfloor} = 6$ блоков-цепей:

$$\mathbb{B}^4 = C_1 \,\Big|\, C_2 \,\Big|\, C_3 \,\Big|\, C_4 \,\Big|\, C_5 \,\Big|\, C_6,$$

где

$$\begin{aligned}
C_1 &: (0,0,0,0) \prec (0,0,0,1) \prec (0,0,1,1) \prec (0,1,1,1) \prec (1,1,1,1),\\
C_2 &: (0,1,0,0) \prec (0,1,1,0) \prec (0,1,1,1),\\
C_3 &: (0,0,1,0) \prec (1,0,1,0) \prec (1,0,1,1),\\
C_4 &: (0,0,0,1) \prec (1,0,0,1) \prec (1,1,0,1),\\
C_5 &: (0,1,0,1),\\
C_6 &: (0,0,1,1).
\end{aligned}$$

✓ $l(\tilde{\alpha}, \tilde{\beta}) \overset{\text{def}}{:=} l([\tilde{\alpha}, \tilde{\beta}])$ — длина максимальной цепи интервала $[\tilde{\alpha}, \tilde{\beta}]$ равна $\rho(\tilde{\beta}) - \rho(\tilde{\alpha})$ и равна числу координат, в которых различаются $\tilde{\alpha}$ и $\tilde{\beta}$:

$$l(\tilde{\alpha}, \tilde{\beta}) = \rho(\tilde{\beta}) - \rho(\tilde{\alpha}).$$

На $\mathbb{B}^n$ нами определены два порядка:

1) линейный порядок: $\tilde{\alpha} \leqslant \tilde{\beta}$ означает, что $\nu(\tilde{\alpha}) \leqslant \nu(\tilde{\beta})$ (лексикографический порядок);

2) частичный порядок: $\tilde{\alpha} \preccurlyeq \tilde{\beta}$ означает, что $\alpha_i \leqslant \beta_i$, $i = \overline{1, n}$ (порядок произведения).

Иногда нам бывает нужно знать соотношения между этими порядками. В следующей лемме приведены некоторые из таких соотношений.

Лемма 1.1. *Справедливы следующие утверждения.*

1. *Если $\tilde{\alpha} \preccurlyeq \tilde{\beta}$, то $\tilde{\alpha} \leqslant \tilde{\beta}$. Иными словами, отношение $\leqslant$ является полным (линейным) продолжением частичного порядка $\preccurlyeq$.*

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

$$\begin{cases} \tilde{\alpha} \prec\cdot\, \tilde{\beta}, \\ \alpha_k = \mathbf{0}, \beta_k = \mathbf{1} \end{cases} \Longleftrightarrow \begin{cases} \nu(\tilde{\beta}) = \nu(\tilde{\alpha}) + 2^{n-k}, \\ \left\lfloor \frac{\nu(\tilde{\beta})}{2^{n-k+1}} \right\rfloor = \left\lfloor \frac{\nu(\tilde{\alpha})}{2^{n-k+1}} \right\rfloor. \end{cases}$$

3. *Пусть $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ — произвольный n-мерный набор. Тогда число n-мерных наборов, покрывающих $\tilde{\alpha}$ (относительно частичного порядка $\preccurlyeq$) равно числу нулевых компонент этого набора. Кроме того, если $\alpha_{i_1}, \ldots, \alpha_{i_k}$ —*

это равные нулю компоненты $\tilde{\alpha}$, то номера векторов в прямом коде, покрывающих $\tilde{\alpha}$, равны

$$\nu(\tilde{\alpha}) + 2^{n-i_1}, \nu(\tilde{\alpha}) + 2^{n-i_2}, \ldots, \nu(\tilde{\alpha}) + 2^{n-i_k}.$$

◀ 1. Следует из цепочки рассуждений:

$$\tilde{\alpha} \preccurlyeq \tilde{\beta} \Longrightarrow \alpha_1 \leqslant \beta_1, \ldots, \alpha_n \leqslant \beta_n \Longrightarrow$$
$$\Longrightarrow \alpha_1 2^{n-1} + \alpha_2 2^{n-2} + \cdots + \alpha_n \leqslant \beta_1 2^{n-1} + \beta_2 2^{n-2} + \cdots + \beta_n \Longrightarrow$$
$$\Longrightarrow \nu(\tilde{\alpha}) \leqslant \nu(\tilde{\beta}) \Longrightarrow \tilde{\alpha} \leqslant \tilde{\beta}.$$

2. Пусть $\tilde{\alpha} \prec\cdot\, \tilde{\beta}$ и

$$\tilde{\alpha} = (\alpha_1, \ldots, \alpha_{k-1}, \mathbf{0}, \alpha_{k+1}, \ldots, \alpha_n) \quad \text{и} \quad \tilde{\beta} = (\beta_1, \ldots, \beta_{k-1}, \mathbf{1}, \beta_{k+1}, \ldots, \beta_n)$$

Тогда ясно, что $\nu(\tilde{\beta}) = \nu(\tilde{\alpha}) + 2^{n-k}$. Далее

$$\nu(\tilde{\alpha}) = \underbrace{(\alpha_1 2^{n-1} + \cdots + \alpha_{k-1} 2^{n-k+1})}_{s} + \underbrace{(\alpha_{k+1} 2^{n-k-1} + \cdots + \alpha_n)}_{t} = s + t,$$

причем s делится на 2^{n-k+1} и $0 \leqslant t < 2^{n-k}$. Значит

$$\frac{\nu(\tilde{\alpha})}{2^{n-k+1}} = \underbrace{\frac{s}{2^{n-k+1}}}_{m} + \underbrace{\frac{t}{2^{n-k+1}}}_{\varepsilon} = m + \varepsilon,$$

где m — целое, а $0 \leqslant \varepsilon < 1/2$. Отсюда

$$\left\lfloor \frac{\nu(\tilde\beta)}{2^{n-k+1}} \right\rfloor = \left\lfloor \frac{\nu(\tilde\alpha) + 2^{n-k}}{2^{n-k+1}} \right\rfloor = \left\lfloor m + \varepsilon + \frac{1}{2} \right\rfloor = \left\lfloor \frac{\nu(\tilde\alpha)}{2^{n-k+1}} \right\rfloor.$$

Обратно, пусть $\tilde\alpha = (\alpha_1, \ldots, \alpha_n)$ и $\tilde\beta = (\beta_1, \ldots, \beta_n)$. Тогда

$$\begin{aligned} \nu(\tilde\alpha) =& \alpha_1 2^{n-1} + \cdots + \alpha_{k-1} 2^{n-k+1} + \alpha_k 2^{n-k} + \alpha_{k+1} 2^{n-k-1} + \cdots + \alpha_n \\ \nu(\tilde\beta) =& \beta_1 2^{n-1} + \cdots + \beta_{k-1} 2^{n-k+1} + \beta_k 2^{n-k} + \beta_{k+1} 2^{n-k-1} + \cdots + \beta_n. \end{aligned} \tag{\dagger}$$

Распишем равенство $\nu(\tilde\beta) = \nu(\tilde\alpha) + 2^{n-k}$:

$$\begin{gathered} \beta_1 2^{n-1} + \cdots + \beta_{k-1} 2^{n-k+1} + \beta_k 2^{n-k} + \beta_{k+1} 2^{n-k-1} + \cdots + \beta_n = \\ = \alpha_1 2^{n-1} + \cdots + \alpha_{k-1} 2^{n-k+1} + (\alpha_k + 1) 2^{n-k} + \alpha_{k+1} 2^{n-k-1} + \cdots + \alpha_n \end{gathered}$$

Откуда, ввиду однозначности двоичного разложения,

$$\alpha_{k+1} = \beta_{k+1}, \alpha_{k+2} = \beta_{k+2}, \ldots, \alpha_n = \beta_n.$$

Далее, из $\dagger$ имеем

$$\begin{aligned} \frac{\nu(\tilde\alpha)}{2^{n-k+1}} &= (\alpha_1 2^{k-2} + \cdots + \alpha_{k-1}) + \varepsilon_1, \\ \frac{\nu(\tilde\beta)}{2^{n-k+1}} &= (\beta_1 2^{k-2} + \cdots + \beta_{k-1}) + \varepsilon_2, \end{aligned}$$

где числа, выделенные скобками — целые числа (целые части соответствующих чисел), а $\varepsilon_1, \varepsilon_2$ — числа из интервала $[0, 1)$ (дробные части соответствующих чисел). Из этих равенств, а также из условия $\left\lfloor \frac{\nu(\tilde\beta)}{2^{n-k+1}} \right\rfloor = \left\lfloor \frac{\nu(\tilde\alpha)}{2^{n-k+1}} \right\rfloor$ имеем

$$\alpha_1 2^{k-2} + \alpha_2 2^{k-3} + \cdots + \alpha_{k-1} = \beta_1 2^{k-2} + \beta_2 2^{k-3} + \cdots + \beta_{k-1}.$$

Откуда

$$\alpha_1 = \beta_1, \alpha_2 = \beta_2, \ldots, \alpha_{k-1} = \beta_{k-1}.$$

Таким образом, мы показали, что $\tilde\alpha$ и $\tilde\beta$ могут отличаться лишь k-ой компонентой. А так как $\nu(\tilde\beta) = \nu(\tilde\alpha) + 2^{n-k}$, то $\tilde\alpha \prec\!\cdot\, \tilde\beta$ и значит $\alpha_k = \mathbf{0}, \beta_k = \mathbf{1}$.

3. Следует из доказанного в этой лемме утверждения 2 и того, что элемент $\tilde\beta$ покрывает $\tilde\alpha$ тогда и только тогда, когда $\tilde\alpha$ и $\tilde\beta$ отличаются лишь в одной компоненте, причем эта компонента в $\tilde\alpha$ равна $\mathbf{0}$, а в $\tilde\beta$ равна $\mathbf{1}$. ►

2. Булевы функции

2.1. Напоминания и обозначения

Для удобства читателя напомним некоторые понятия и обозначения.

✓ $\mathbb{B} = \{\mathbf{0}, \mathbf{1}\}$ — двухэлементная («минимальная») булева алгебра.

✓ $\vee, \wedge$ и $\bar{\ }$ — (основные) булевы операции на $\mathbb{B}$. Вместо $a \wedge b$ будем часто писать ab или $a \cdot b$, а вместо $\bar a$ будем также применять запись $\neg a$.

✓ Исходя из основных булевых операций, мы определяем производные (от них) операции $-, \oplus, \rightarrow, \leftrightarrow, |, \downarrow, \stackrel{*}{-}, \stackrel{*}{\rightarrow}$ следующим образом:

$$a - b :\stackrel{\text{def}}{=} a \wedge \bar{b}, \qquad a \,|\, b :\stackrel{\text{def}}{=} \bar{a} \vee \bar{b},$$
$$a \oplus b :\stackrel{\text{def}}{=} a\bar{b} \vee \bar{a}b, \qquad a \downarrow b :\stackrel{\text{def}}{=} \bar{a} \wedge \bar{b},$$
$$a \rightarrow b :\stackrel{\text{def}}{=} \bar{a} \vee b, \qquad a \stackrel{*}{-} b :\stackrel{\text{def}}{=} \bar{a} \vee b,$$
$$a \leftrightarrow b :\stackrel{\text{def}}{=} (\bar{a} \vee b) \cdot (\bar{b} \vee a), \qquad a \stackrel{*}{\rightarrow} b :\stackrel{\text{def}}{=} a \vee \bar{b}.$$

✓ *Булево выражение* над множеством переменных $\{x_1, \ldots, x_n\}$ — это выражение, построенное из переменных $x_1, \ldots, x_n$ с помощью основных булевых операций. Точнее, булевы выражения над множеством переменных $\{x_1, \ldots, x_n\}$ определяются следующим рекурсивным определением:

1) всякая переменная x_i из $\{x_1, \ldots, x_n\}$ является булевым выражением над $\{x_1, \ldots, x_n\}$,

2) элементы **0** и **1** являются булевыми выражениями над $\{x_1, \ldots, x_n\}$,

3) если A — булево выражение над $\{x_1, \ldots, x_n\}$, то $\bar{A}$ также является булевым выражением над $\{x_1, \ldots, x_n\}$,

4) если A, B — булевы выражения над $\{x_1, \ldots, x_n\}$, то

$$(A \vee B), \ (A \wedge B)$$

также являются булевыми выражениями над $\{x_1, \ldots, x_n\}$,

5) только такие выражения являются булевыми выражениями над $\{x_1, \ldots, x_n\}$, если только эти выражения получаются из 1), 2), 3) и 4).

✓ *Обобщенное булево* выражение над множеством переменных $\{x_1, \ldots, x_n\}$ — это выражение построенное из $x_1, \ldots, x_n$ с помощью основных и производных булевых операций. Точнее:

1) всякая переменная x_i из $\{x_1, \ldots, x_n\}$ является обобщенным булевым выражением над $\{x_1, \ldots, x_n\}$,

2) элементы **0** и **1** являются обобщенными булевыми выражениями над $\{x_1, \ldots, x_n\}$,

3) если A — обобщенное булево выражение над $\{x_1, \ldots, x_n\}$, то $\bar{A}$ также является обобщенным булевым выражением над $\{x_1, \ldots, x_n\}$,

4) если A, B — обобщенные булевы выражения над множеством $\{x_1, \ldots, x_n\}$, то

$$(A \vee B), (A \wedge B), (A - B),\ (A \oplus B), (A \to B), (A \leftrightarrow B),$$
$$(A \,|\, B), (A \downarrow B), (A \overset{*}{-} B),\ (A \overset{*}{\to} B)$$

также являются обобщенными булевыми выражениями над множеством переменных $\{x_1, \ldots, x_n\}$,

5) только такие выражения являются обобщенными булевыми выражениями над $\{x_1, \dots, x_n\}$, если только эти выражения получаются из $1), 2), 3)$ и 4).

Определение 2.1. *Булевой функцией (n переменных)* называется функция

$$f(x_1, \dots, x_n) \colon \mathbb{B}^n \to \mathbb{B}.$$

Обозначения:

$$\mathbb{BF}(n) \overset{\text{def}}{:=} \mathbb{Map}(\mathbb{B}^n, \mathbb{B}), \qquad \mathbb{BF} \overset{\text{def}}{:=} \bigcup_{n=1}^{\infty} \mathbb{BF}(n).$$

Итак, $\mathbb{BF}(n)$ — это множество всех булевых функций n переменных, а $\mathbb{BF}$ обозначает множество всех булевых функций (различного числа переменных).

Функции «проектирования на i-ю координату»

$$p_i^n(x_1, \dots, x_n) \overset{\text{def}}{:=} x_i$$

будем, как обычно, обозначать просто через x_i, $1 \leqslant i \leqslant n$. (Как видим, это обозначение совпадает с обозначением булевой переменной. Такой «конфликт обозначений» почти всегда безобиден.)

2.2. Способы задания булевых функций

Говоря о способах задания булевых функций, отметим следующие.

Из имеющихся с помощью булевых операций. Область значений всякой булевой функции — булева алгебра $\mathbb{B}$. Будучи булевой алгеброй в $\mathbb{B}$ определены булевы операции $\vee, \wedge, \bar{\ }$ и производные от них операции $-, \oplus, \to, \leftrightarrow, |, \downarrow, \overset{*}{-}, \overset{*}{\to}$. Это позволяет строить новые функции из уже имеющихся в наличии. Так, если даны две функции $f, g \in \mathbb{BF}(n)$, то можно ввести в рассмотрение и функции

$$\bar{f}\colon (x_1, \ldots, x_n) \mapsto \overline{f(x_1, \ldots, x_n)},$$
$$f \circ g\colon (x_1, \ldots, x_n) \mapsto f(x_1, \ldots, x_n) \circ g(x_1, \ldots, x_n),$$

где «$\circ$» — любая из 10-ти бинарных операций

$$\vee, \wedge, -, \oplus, \to, \leftrightarrow, |, \downarrow, \overset{*}{-}, \overset{*}{\to}.$$

С помощью булевых выражений. Каждое булево выражение или обобщенное булево выражение над множеством переменных $\{x_1, \ldots, x_n\}$ естественным образом задает некоторую булеву функцию. Так, булево выражение $((x_1 \vee x_3) \wedge (x_2 \vee \bar{x}_3))$ задает булеву функцию $f(x_1, x_2, x_3) = ((x_1 \vee x_3) \wedge (x_2 \vee \bar{x}_3))$, а, к примеру, следующие функции заданы с помощью обобщенных булевых выражений.

$$
\begin{aligned}
f(x_1,x_2,x_3) &= (\overline{(x_1 \to x_2)} \oplus ((x_2 \,|\, x_1) \leftrightarrow x_3)),\\
g(x_1,x_2,x_3) &= ((x_1 \oplus x_2) \to (x_2 \to x_1)),\\
h(x_1,x_2,x_3) &= ((x_1 \,|\, x_2) \downarrow (x_2 \oplus x_3)).
\end{aligned}
$$

Замечательным фактом является то, что, как мы увидим ниже, *всякая булева функция задается некоторым булевым выражением.* Причем (даже представляющих интерес) булевых выражений или обобщенных булевых выражений, задающих одну и ту же функцию, может быть несколько.

Табличный способ. Ввиду того что область определения $\mathbb{B}^n$ булевой функции есть конечное множество (состоит из 2^n элементов), то булеву функцию можно задавать с помощью таблицы:

x_1	x_2	$\ldots$	x_n	$f(x_1,\ldots,x_n)$
$\mathbf{0}$	$\mathbf{0}$	$\ldots$	$\mathbf{0}$	α_0
$\mathbf{0}$	$\mathbf{0}$	$\ldots$	$\mathbf{1}$	α_1
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$\mathbf{1}$	$\mathbf{1}$	$\ldots$	$\mathbf{1}$	α_{2^n-1}

(2.1)

Из табличного задания булевых функций легко видеть, что общее число булевых функций n переменных $x_1,\ldots,x_n$ равно 2^{2^n}:

$$\big|\,\mathbb{BF}(n)\big| = 2^{2^n}.$$

Действительно, согласно табличному способу, чтобы задать булеву функцию $f(x_1, \ldots, x_n)$, нужно сделать 2^n шагов, записывая значения **0** или **1** в столбце для значений функции в каждую из 2^n строк. Поскольку для каждого из 2^n шагов существует два выбора **0** или **1**, то по правилу произведения получаем, что $\left|\mathbb{BF}(n)\right| = 2^{2^n}$.

Например, все четыре возможные функции одной переменной имеют следующее табличное представление:

x	$f(x) = x$	$f(x) = \bar{x}$	$f(x) = \mathbf{0}$	$f(x) = \mathbf{1}$
0	**0**	**1**	**0**	**1**
1	**1**	**0**	**0**	**1**

.

Приведем также табличное задание основных и производных булевых операций:

Сайт ДГУ
Тиульный лист
Оглавление
страница 25 из 158
Назад
Полный экран
Закрыть
Выход

x	y	дизъюнкция $x \vee y$	конъюнкция $x \wedge y$	импликация $x \to y$	сумма по модулю 2 $x \oplus y$	эквиваленция $x \leftrightarrow y$
0	0	0	0	1	0	1
0	1	1	0	1	1	0
1	0	1	0	0	1	0
1	1	1	1	1	0	1

x	y	штрих Шеффера $x \mid y$	стрелка Пирса $x \downarrow y$	разность $x - y$	коимпликация $x \overset{*}{\rightarrow} y$	коразность $x \overset{*}{-} y$
0	**0**	**1**	**1**	**0**	**0**	**1**
0	**1**	**1**	**0**	**0**	**1**	**0**
1	**0**	**1**	**0**	**1**	**0**	**1**
1	**1**	**0**	**0**	**0**	**0**	**1**

Нужно отметить также многообразие обозначений и названий для приведенных функций (операций). Это связано с тем, что эти операции достаточно интенсивно используются в различных областях знания, главные из которых — это математическая логика, теория множеств, алгебра и техника. Специфика этих наук не могла не отразиться как на названиях некоторых операций, так и на их обозначениях. Мы не будем приводить все альтернативные названия и обозначения этих операций, а только фиксируем варианты их прочтения, которыми будем практически пользоваться:

$\bar{x}$, $\neg x$ — «не x», «отрицание x», «дополнение x»;

$x \vee y$ — «дизъюнкция x и y», «x или y», «сумма x и y»;

$x \wedge y$ — «конъюнкция x и y», «x и y », «произведение x и y»;

$x \to y$ — «x имплицирует y», «если x, то y», «x влечет y»;

$x \oplus y$ — «сумма по модулю 2 x и y», «либо x, либо y» (*исключающее или*);

$x \leftrightarrow y$ — «x эквивалентно y», «x тогда и только тогда, когда y»;

$x \,|\, y$ — «x штрих Шеффера y», «не x или не y»;

$x \downarrow y$ — «x стрелка Пирса y», «не x и не y»;

$x - y$ — «x разность y»;

$x \overset{*}{\to} y$ — «x коимплицирует y»;

$x \overset{*}{-} y$ — «x коразность y».

Таблица Вейча. Для представления функции $f\colon \mathbb{B}^n \to \mathbb{B}$ в виде таблицы Вейча задается разбиение множества переменных $\{x_1, \ldots, x_n\}$ функции на два блока:

$$\{x_1, \ldots, x_n\} = \{x_1, \ldots, x_k\} \Big| \{x_{k+1}, \ldots, x_n\},$$

что соответствует представлению области определения $\mathbb{B}^n$ функции f в виде декартова произведения

$$\mathbb{B}^n = \mathbb{B}^k \times \mathbb{B}^{n-k}.$$

Функция $f(x_1, \dots, x_n)$ тогда задается в виде двумерной таблицы, в которой строки «нумеруются» элементами из $\mathbb{B}^k$ (значениями переменных $x_1, \dots, x_k$), а столбцы «нумеруются» элементами из $\mathbb{B}^{n-k}$ (значениями переменных $x_{k+1}, \dots, x_n$); при этом на пересечении строки с «номером» $\alpha_1, \dots, \alpha_k$ и столбца с «номером» $\alpha_{k+1}, \dots, \alpha_n$ записывается значение функции f на наборе $(\alpha_1, \dots, \alpha_k, \alpha_{k+1}, \dots, \alpha_n)$:

$$
\begin{array}{cccc|cccccc|c}
 & & & & \mathbf{0} & \mathbf{0} & \dots & \alpha_{k+1} & \dots & \mathbf{1} & x_{k+1} \\
 & & & & \mathbf{0} & \mathbf{0} & \dots & \alpha_{k+2} & \dots & \mathbf{1} & x_{k+2} \\
 & & & & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
 & & & & \mathbf{0} & \mathbf{1} & \dots & \alpha_n & \dots & \mathbf{1} & x_n \\
x_1 & x_2 & \dots & x_k & & & & & & & \\
\hline
\mathbf{0} & \mathbf{0} & \dots & \mathbf{0} & & & & \vdots & & & \\
\mathbf{0} & \mathbf{0} & \dots & \mathbf{1} & & & & \vdots & & & \\
\dots & \dots & \dots & \dots & & & & \vdots & & & \\
\alpha_1 & \alpha_2 & \dots & \alpha_k & \cdots & \cdots & \cdots & \boxed{f(\alpha_1, \dots, \alpha_n)} & & & \\
\dots & \dots & \dots & \dots & & & & & & & \\
\mathbf{1} & \mathbf{1} & \dots & \mathbf{1} & & & & & & &
\end{array}
$$

Часто случается так, что нас по определенным причинам интересует какая-то группа переменных $x_{s_1}, \dots, x_{s_k}$, $(1 \leqslant s_1 < \dots < s_k \leqslant n)$ функции f. В связи с этим можно предложить небольшое обобщение приведенного способа задания булевой функции, который также будем называть таблицей Вейча функции $f(x_1, \dots, x_n)$. Для этого разобьем множество переменных $x_1, \dots, x_n$ на блок переменных, которые нас интересуют, и остальные переменные:

$$\{x_1,\ldots,x_n\} = \{x_{s_1}, x_{s_2},\ldots,x_{s_k}\}\Big|\{x_{r_1}, x_{r_2},\ldots,x_{r_{n-k}}\}.$$

Таблицей Вейча функции $f(x_1,\ldots,x_n)$, соответствующей этому разбиению, называется двумерная таблица, строки которой «нумеруются» значениями переменных $x_{s_1}, x_{s_2},\ldots,x_{s_k}$,а столбцы — значениями переменных $x_{r_1}, x_{r_2},\ldots,x_{r_{n-k}}$; на пересечении строки с «номером» $\alpha_{s_1},\alpha_{s_2},\ldots,\alpha_{s_k}$ и столбца с «номером» $\alpha_{r_1},\alpha_{r_2},\ldots,\alpha_{r_{n-k}}$ стоит значение функции f на наборе $(\alpha_1,\ldots,\alpha_n)$.

Задание булевой функции в виде слова. Как мы знаем, такой способ задания функции обоснован только при условии, если область определения функции линейно упорядочена. Договоримся, что когда речь идет о словесном задании булевой функции n переменных, n-мерный единичный булев куб $\mathbb{B}^n$ (область определения булевой функции $f\colon \mathbb{B}^n \to \mathbb{B}$) линейно упорядочен посредством лексикографического порядка:

$$(\mathbf{0},\ldots,\mathbf{0},\mathbf{0}) < (\mathbf{0},\ldots,\mathbf{0},\mathbf{1}) < (\mathbf{0},\ldots,\mathbf{1},\mathbf{0}) < \ldots < (\mathbf{1},\ldots,\mathbf{1},\mathbf{1}).$$

Кстати, в табличной записи (2.1) строки аргументов мы расположили именно в таком лексикографическом порядке. После такой договоренности словесная форма записи функции (2.1) имеет вид

$$f = [\![\alpha_0\alpha_1\ldots\alpha_{2^n-1}]\!].$$

Приведем словесное задание основных и производных булевых операций ($x = x_1, y = x_2$):

$$\begin{aligned} x \vee y &= [\![\mathbf{0111}]\!], & x \to y &= [\![\mathbf{1101}]\!], \\ x \wedge y &= [\![\mathbf{0001}]\!], & x \leftrightarrow y &= [\![\mathbf{1001}]\!], \\ x - y &= [\![\mathbf{0010}]\!], & x \,|\, y &= [\![\mathbf{1110}]\!], \\ x \oplus y &= [\![\mathbf{0110}]\!], & x \downarrow y &= [\![\mathbf{1000}]\!]. \end{aligned}$$

С помощью характеристического множества. Так как булева функция $f(x_1, \ldots, x_n) \colon \mathbb{B}^n \to \mathbb{B}$ может принимать только два значения ($\mathbf{0}$ или $\mathbf{1}$), то любую булеву функцию можно задать с помощью указания множества значений наборов из $\mathbb{B}^n$, на которых она принимает значение $\mathbf{1}$ (на остальных наборах из $\mathbb{B}^n$ эта функция принимает значение $\mathbf{0}$). Это мотивирует следующее определение: *характеристическим множеством* булевой функции $f(x_1, \ldots, x_n) \colon \mathbb{B}^n \to \mathbb{B}$ называется множество

$$N_f \overset{\mathrm{def}}{:=} \{(\alpha_1, \ldots, \alpha_n) \in \mathbb{B}^n \mid f(\alpha_1, \ldots, \alpha_n) = \mathbf{1}\}.$$

Впрочем, в некоторых случаях может быть удобнее задать его дополнение

$$\overline{N}_f \overset{\mathrm{def}}{:=} \mathbb{B}^n \setminus N_f = \{(\alpha_1, \ldots, \alpha_n) \in \mathbb{B}^n \mid f(\alpha_1, \ldots, \alpha_n) = \mathbf{0}\}$$

(множества N_f и $\overline{N}_f$, конечно же, однозначно определяют друг друга).

Приведем задание основных и производных булевых операций с помощью характеристического множества:

$$\begin{aligned} N_{x\vee y} &= \{(\mathbf{0},\mathbf{1}),(\mathbf{1},\mathbf{0}),(\mathbf{1},\mathbf{1})\}, & N_{x\to y} &= \{(\mathbf{0},\mathbf{0}),(\mathbf{0},\mathbf{1}),(\mathbf{1},\mathbf{1})\},\\ N_{x\wedge y} &= \{(\mathbf{1},\mathbf{1})\}, & N_{x\leftrightarrow y} &= \{(\mathbf{0},\mathbf{0}),(\mathbf{1},\mathbf{1})\},\\ N_{x-y} &= \{(\mathbf{1},\mathbf{0})\}, & N_{x\,|\,y} &= \{(\mathbf{0},\mathbf{0})\},\\ N_{x\oplus y} &= \{(\mathbf{0},\mathbf{1}),(\mathbf{1},\mathbf{0})\}, & N_{x\downarrow y} &= \{(\mathbf{0},\mathbf{0}),(\mathbf{0},\mathbf{1}),(\mathbf{1},\mathbf{0})\}. \end{aligned}$$

Пример 1. Рассмотрим функцию трех переменных

$$m(x_1,x_2,x_3)\colon \mathbb{B}^3\to\mathbb{B},$$

заданную следующим образом: она равна $\mathbf{1}$, если значения хотя бы двух ее аргументов равны $\mathbf{1}$, и равна $\mathbf{0}$ в противном случае. Эту функцию называют *функцией голосования (трех)* или *функцией баллотировки (тремя)*. Такое название связано со следующей ее интерпретацией: представьте себе, что идет голосование какого-то вопроса, в котором принимают участие три человека; при этом голос «за» обозначим через $\mathbf{1}$, а голос «против» — через $\mathbf{0}$; тогда вопрос решится положительно только в том случае, когда не менее двух человек решат его положительно.

Ниже мы приводим различные способы задания этой булевой функции.

С помощью булевых выражений:

$$m(x_1,x_2,x_3)=x_1x_2\vee x_2x_3\vee x_3x_1$$

или

$$m(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_3x_1.$$

Табличный способ:

x_1	x_2	x_3	$m(x_1, x_2, x_3)$
0	**0**	**0**	**0**
0	**0**	**1**	**0**
0	**1**	**0**	**0**
0	**1**	**1**	**1**
1	**0**	**0**	**0**
1	**0**	**1**	**1**
1	**1**	**0**	**1**
1	**1**	**1**	**1**

Таблица Вейча:

Таблица Вейча $m(x_1,x_2,x_3)$, *соответствующая разбиению* $\{x_1\}|\{x_2,x_3\}$

	0	**0**	**1**	**1**	x_2
	0	**1**	**0**	**1**	x_3
x_1					
0	**0**	**0**	**0**	**1**	
1	**0**	**1**	**1**	**1**	

Таблица Вейча $m(x_1,x_2,x_3)$, *соответствующая разбиению* $\{x_2\}|\{x_1,x_3\}$

	0	**0**	**1**	**1**	x_1
	0	**1**	**0**	**1**	x_3
x_2					
0	**0**	**0**	**0**	**1**	
1	**0**	**1**	**1**	**1**	

Таблица Вейча $m(x_1,x_2,x_3)$, *соответствующая разбиению* $\{x_3\}|\{x_1,x_2\}$

	0	**0**	**1**	**1**	x_1
	0	**1**	**0**	**1**	x_2
x_3					
0	**0**	**0**	**0**	**1**	
1	**0**	**1**	**1**	**1**	

Словесное задание:
$$m(x_1, x_2, x_3) = [\![\mathbf{00010111}]\!]$$
С помощью характеристического множества:
$$N_m = \{(\mathbf{0}, \mathbf{1}, \mathbf{1}), (\mathbf{1}, \mathbf{0}, \mathbf{1}), (\mathbf{1}, \mathbf{1}, \mathbf{0}), (\mathbf{1}, \mathbf{1}, \mathbf{1})\}$$

В случае небольшого числа переменных путем построения их таблиц очень легко устанавливать равенство или неравенство двух булевых функций. Если Вы таким образом докажите следующие равенства, то это позволит Вам уверенно пользоваться ими без всяких ссылок на общую теорию булевых алгебр (в которой эти равенства принимались нами как аксиомы, определения или доказывались нами на основе аксиом и определений). Эти равенства мы будем называть *основными булевыми равенствами (тождествами, законами, правилами)*, и мы ими постоянно будем пользоваться, часто без специальных оговорок.

(1) *Коммутативные законы:*
$$x \star y = y \star x,$$
где $\star$ — любая из операций $\vee, \wedge, \oplus, \leftrightarrow, \downarrow, |$. (Конечно, при этом в обе части равенства нужно подставлять один и тот же символ операции.)

(2) *Ассоциативные законы:*
$$x \star (y \star z) = (x \star y) \star z,$$

где $\star$ — любая из операций $\vee, \wedge, \oplus, \leftrightarrow$.

(3) *Дистрибутивные законы:*

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z),$$
$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z),$$
$$x \wedge (y \oplus z) = (x \wedge y) \oplus (x \wedge z).$$

(4) *Законы Де Моргана:*

$$\overline{x \vee y} = \bar{x} \wedge \bar{y},$$
$$\overline{x \wedge y} = \bar{x} \vee \bar{y}.$$

(5) *Законы поглощения:*

$$x \vee (x \wedge y) = x,$$
$$x \wedge (x \vee y) = x.$$

(6) *Закон двойного отрицания:*

$$\bar{\bar{x}} = x.$$

(7) *Правила получения нуля:*

$$x \wedge \bar{x} = x \wedge \mathbf{0} = x \oplus x = x \leftrightarrow \bar{x} = \mathbf{0}.$$

(8) *Правила получения единицы:*

$$x \vee \bar{x} = x \vee \mathbf{1} = x \leftrightarrow x = x \oplus \bar{x} = x \to x = \mathbf{1}.$$

(9) *Правила тождества:*

$$x \vee x = x \wedge x = x \wedge \mathbf{1} = x \vee \mathbf{0} = x \oplus \mathbf{0} = x \leftrightarrow \mathbf{1} = x.$$

(10) *Правила отрицания:*

$$x \oplus \mathbf{1} = x \leftrightarrow \mathbf{0} = x \to \mathbf{0} = x \,|\, x = x \downarrow x = \bar{x}.$$

При записи обобщенных булевых выражений порядок выполнения операций, как обычно, определяется скобками. Если количество операций в выражении равно n, то количество скобок равно $2n$; при большом n такое выражение очень трудно воспринимается, а при записи очень легко забыть о какой-нибудь скобке. Для уменьшения числа скобок обычно принимаются соглашения. Мы примем самые распространенные соглашения:

1) внешние скобки обычно опускаются;

2) в следующем списке операций

$$\neg,\ \wedge,\ \vee$$

в первую очередь (при прочих равных условиях) выполняется та, которая стоит раньше (левее);

3) остальные бинарные операции будем считать имеющими равный приоритет, но меньший, чем дизъюнкция (их порядок выполнения регламентируется скобками).

Кроме того, напомним, что, если «$\circ$» — ассоциативная операция (в нашем случае «$\circ$» — какая-нибудь из операций $\wedge, \vee, \oplus, \leftrightarrow$), то произвольная расстановка скобок в выражении

$$A_1 \circ A_2 \circ \cdots \circ A_n$$

дает один и тот же результат; поэтому в таком выражении скобки вообще можно опустить.

2.3. Существенные и фиктивные переменные булевых функций

Для вещественной функции двух вещественных переменных $f(x, y)\colon \mathbb{R}^2 \to \mathbb{R}$, равной $f(x, y) = x^2 + y - y$, значения переменной y никак не влияют на значения функции:

$$f(x, a) = f(x, b) \quad \text{для любых} \quad a, b \in \mathbb{R}.$$

Такая же ситуация может наблюдаться и для булевых функций. Так, например, для функции $f(x, y)\colon \mathbb{B}^2 \to \mathbb{B}$, равной $f(x, y) = x \oplus (y \wedge \bar{y})$, значения переменной y

никак не влияют на значения функции:

$$f(x,\alpha) = f(x,\beta) \quad \text{для любых } \alpha,\beta \in \mathbb{B}, \text{ т. е. } \ f(x,\mathbf{0}) = f(x,\mathbf{1}).$$

Такого типа переменные можно (и будем) называть несущественными или фиктивными переменными.

Определение 2.2. Переменная x_k называется *фиктивной* или *несущественной* переменной для булевой функции $f(x_1,\ldots,x_n)$, если

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

Если переменная x_k не является фиктивной переменной для функции $f(x_1,\ldots,x_n)$, то эта переменная называется *существенной* переменной этой функции.

В связи с введением понятия фиктивной переменной возникает вопрос о равенстве двух булевых функций. Мы принимаем следующее определение.

Определение 2.3. Две булевы функции f и g называются *равными*, если они имеют *одни и те же существенные* переменные и на любых двух наборах, различающихся, быть может, только значениями несущественных переменных, значения этих функций f и g совпадают.

Таким образом, можно сказать, что две булевы функции равны, если одну из них можно получить из другой путем добавления и изъятия конечного числа фиктивных переменных.

Обозначим через $\mathbb{BF}^c(n)$ все булевы функции $f(x_1,\ldots,x_n)$, которые зависят от всех своих переменных $x_1,\ldots,x_n$ существенно.

Лемма 2.1. *Справедливы следующие утверждения.*

1. *Число $N(s_1,s_2,\ldots,s_k)$ булевых функций $f(x_1,\ldots,x_n)$ из $\mathbb{BF}(n)$, у которых переменные $x_{s_1},x_{s_2},\ldots,x_{s_k}$ являются фиктивными, дается формулой*

$$N(s_1,s_2,\ldots,s_k)=2^{2^{n-k}}.$$

2. *Число булевых функций $f(x_1,\ldots,x_n)$ из $\mathbb{BF}(n)$, существенно зависящих от всех своих n переменных, дается формулой*

$$\left|\mathbb{BF}^c(n)\right|=\sum_{k=0}^{n}(-1)^k\binom{n}{k}2^{2^{n-k}}.$$

◀ 1. Переменные $x_{s_1},\ldots,x_{s_k}$ являются фиктивными для $f(x_1,\ldots,x_n)$, если каждая из этих переменных является фиктивной для этой функции, т. е. если равны значения функции $f(x_1,\ldots,x_n)$ на любых двух наборах $(\alpha_1,\ldots,\alpha_n)\in\mathbb{B}^n$ и $(\beta_1,\ldots,\beta_n)\in\mathbb{B}^n$, различающихся, быть может, компонентами $s_1,\ldots,s_k$. Отсюда получаем, что для функции $f(x_1,\ldots,x_n)$ переменные $x_{s_1},\ldots,x_{s_k}$ являются фиктивными тогда и только тогда, когда в таблице Вейча этой функции, соответствующей разбиению

$$\{x_1,\ldots,x_n\}=\{x_{s_1},x_{s_2},\ldots,x_{s_k}\}\Big|\{x_{r_1},x_{r_2},\ldots,x_{r_{n-k}}\},$$

все строки равны:

$$
\begin{array}{cccc|cccc|l}
 & & & & \mathbf{0} & \mathbf{0} & \dots & \mathbf{1} & x_{r_1} \\
 & & & & \mathbf{0} & \mathbf{0} & \dots & \mathbf{1} & x_{r_2} \\
 & & & & \dots & \dots & \dots & \dots & \dots \\
 & & & & \mathbf{0} & \mathbf{1} & \dots & \mathbf{1} & x_{r_{n-k}} \\
x_{s_1} & x_{s_2} & \dots & x_{s_k} & & & & & \\
\hline
\mathbf{0} & \mathbf{0} & \dots & \mathbf{0} & \alpha_1 & \alpha_2 & \dots & \alpha_{2^{n-k}} & \\
\mathbf{0} & \mathbf{0} & \dots & \mathbf{1} & \alpha_1 & \alpha_2 & \dots & \alpha_{2^{n-k}} & \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \\
\mathbf{1} & \mathbf{1} & \dots & \mathbf{1} & \alpha_1 & \alpha_2 & \dots & \alpha_{2^{n-k}} &
\end{array}
$$

Число таких таблиц, как легко видеть, равно $2^{2^{n-k}}$.

2. Обозначим через $N(s_1, \dots, s_k)$ число булевых функций $f(x_1, \dots, x_n)$, у которых переменные $x_{s_1}, \dots, x_{s_k}$ являются фиктивными. Далее, у булевой функции $f(x_1, \dots, x_n)$ все переменные являются существенными, если ни одна из ее переменных не является фиктивной. Отсюда, согласно формуле включений и исключений, справедлива формула

$$|\mathbb{BF}^{\,c}(n)| = S_0 - S_1 + S_2 - \dots + (-1)^n S_n,$$

где

$$S_k = \sum_{1 \leqslant s_1 < s_2 < \dots < s_k \leqslant n} N(s_1, s_2, \dots, s_k).$$

В утверждении 1 нашей леммы показано, что $N(s_1, s_2, \dots, s_k) = 2^{2^{n-k}}$. Отсюда

$$S_k = \sum_{1 \leqslant s_1 < \dots < s_k \leqslant n} N(s_1, \dots, s_k) =$$

$$= \sum_{1 \leqslant s_1 < \dots < s_k \leqslant n} 2^{2^{n-k}} = 2^{2^{n-k}} \sum_{1 \leqslant s_1 < \dots < s_k \leqslant n} 1 = 2^{2^{n-k}} \binom{n}{k}.$$

Значит,

$$|\mathbb{BF}^c(n)| = \sum_{k=0}^{n} (-1)^k \binom{n}{k} 2^{2^{n-k}}.$$

Лемма доказана. ▶

В частности, получаем, что количество булевых функций двух переменных, существенно зависящих от обеих своих переменных, равно

$$\binom{2}{0} 2^{2^{2-0}} - \binom{2}{1} 2^{2^{2-1}} + \binom{2}{2} 2^{2^{2-2}} = 16 - 8 + 2 = 10.$$

Именно эти функции и приведены в таблице на стр. 25.

Замечание 2.1. Можно сказать, что с увеличением n «почти все» булевы функции $f(x_1, \ldots, x_n)$ зависят существенно от всех своих n переменных. Точнее, справедливо равенство:

$$\lim_{n\to\infty} \frac{|\mathbb{BF}^c(n)|}{|\mathbb{BF}(n)|} = 1.$$

Предложение 2.1. *Пусть $f(x_1, \ldots, x_n) = [\![\alpha_0 \alpha_1 \ldots \alpha_{2^n-1}]\!]$. Переменная x_k является фиктивной переменной этой булевой функции тогда и только тогда, когда*

$$\alpha_i = \alpha_{i+2^{n-k}} \quad \textit{при} \quad \left\lfloor \frac{i}{2^{n-k+1}} \right\rfloor = \left\lfloor \frac{i + 2^{n-k}}{2^{n-k+1}} \right\rfloor.$$

◀ Пусть x_k — фиктивная переменная и

$$\begin{aligned}
&\tilde{\sigma}_0 = (\sigma_1, \ldots, \sigma_{k-1}, \mathbf{0}, \sigma_{k+1}, \ldots, \sigma_n),\\
&\tilde{\sigma}_1 = (\sigma_1, \ldots, \sigma_{k-1}, \mathbf{1}, \sigma_{k+1}, \ldots, \sigma_n),\\
&\nu(\tilde{\sigma}_0) = i \quad \text{— номер вектора } \tilde{\sigma}_0 \text{ в прямом коде.}
\end{aligned}$$

Тогда $f(\tilde{\sigma}_0) = \alpha_i$, $f(\tilde{\sigma}_1) = \alpha_{i+2^{n-k}}$ и по лемме 1.1 $\nu(\tilde{\sigma}_1) = \nu(\tilde{\sigma}_0) + 2^{n-k}$ и $\left\lfloor \frac{i}{2^{n-k+1}} \right\rfloor = \left\lfloor \frac{i+2^{n-k}}{2^{n-k+1}} \right\rfloor$. Так как x_k — фиктивная переменная для $f(x_1, \ldots, x_n)$, то $f(\tilde{\sigma}_0) = f(\tilde{\sigma}_1)$, т. е.

$$\alpha_i = \alpha_{i+2^{n-k}} \quad \text{при} \quad \left\lfloor \frac{i}{2^{n-k+1}} \right\rfloor = \left\lfloor \frac{i+2^{n-k}}{2^{n-k+1}} \right\rfloor.$$

Обратно, пусть $\alpha_i = \alpha_{i+2^{n-k}}$ при $\left\lfloor \frac{i}{2^{n-k+1}} \right\rfloor = \left\lfloor \frac{i+2^{n-k}}{2^{n-k+1}} \right\rfloor$. Покажем, что x_k —фиктивная переменная. Возьмем произвольно два вектора $\tilde{\sigma}_0$ и $\tilde{\sigma}_1$, различающиеся лишь k-й компонентой. Тогда по лемме 1.1 $\nu(\tilde{\sigma}_1) = \nu(\tilde{\sigma}_0) + 2^{n-k}$ и $\left\lfloor \frac{\nu(\tilde{\sigma}_1)}{2^{n-k+1}} \right\rfloor = \left\lfloor \frac{\nu(\tilde{\sigma}_0)}{2^{n-k+1}} \right\rfloor$; положим $i = \nu(\tilde{\sigma}_0)$. Тогда по условию $\alpha_i = \alpha_{i+2^{n-k}}$, т. е. $f(\tilde{\sigma}_0) = f(\tilde{\sigma}_1)$, что и доказывает фиктивность переменной x_k. ▶

Основываясь на доказанном утверждении, можно предложить следующий метод решения вопроса о фиктивности переменной булевой функции, если эта функция задана в виде слова. Пусть задана булева функция $f = [\![\alpha_0 \alpha_1 \ldots \alpha_{2^n-1}]\!]$, зависящая от n переменных. Для того чтобы выяснить, является ли переменная x_k фиктивной или существенной разобьем данное слово $[\![\alpha_0 \alpha_1 \ldots \alpha_{2^n-1}]\!]$ на 2^{k-1} равных блока

$$[\![\alpha_0 \ldots \alpha_{2^{n-k+1}-1} \,\big|\, \alpha_{2^{n-k+1}} \ldots \alpha_{2\cdot 2^{n-k+1}-1} \,\big|\, \ldots \,\big|\, \alpha_{(2^{k-1}-1)\cdot 2^{n-k+1}} \ldots \alpha_{2^n-1}]\!]$$

Если внутри каждого блока находится слово-квадрат, то переменная x_k является фиктивной, в противном случае переменная x_k является существенной. Осталось только пояснить, что мы понимаем под термином слово-квадрат.

✓ *Квадратом слова* $a_1a_2\ldots a_m$ называется слово

$$(a_1a_2\ldots a_m)^2 = a_1a_2\ldots a_m a_1a_2\ldots a_m;$$

таким образом, слово-квадрат — это слово вида

$$a_1a_2\ldots a_m a_1a_2\ldots a_m.$$

Пример 2. Для булевой функции

$$f(x_1, x_2, x_3, x_4) = [\![\mathbf{0101111100001010}]\!],$$

выяснить, какие переменные у нее фиктивные.

Решение. 1. Исследуем переменную x_1. Для этого разобьем наше слово на $2^{1-1} = 1$ блока, т. е. нужно рассмотреть все наше слово как один блок. Как легко видеть, это слово не является словом-квадратом; поэтому x_1 — существенная переменная.

2. Исследуем переменную x_2. Для этого разобьем наше слово на $2^{2-1} = 2$ блока:

$$\mathbf{01011111}\,\big|\,\mathbf{00001010}$$

Вновь легко видим, что внутри обоих блоков находятся слова, которые не являются словами-квадратами; поэтому x_2 — существенная переменная.

3. Исследуем переменную x_3. Для этого разобьем наше слово на $2^{3-1} = 4$ блока:

$$\mathbf{0101}\,|\,\mathbf{1111}\,|\,\mathbf{0000}\,|\,\mathbf{1010}$$

Видим, что внутри каждого блока находится слово-квадрат; поэтому x_3 — фиктивная переменная.

4. Наконец, исследуем переменную x_4. Для этого разобьем наше слово на $2^{4-1} = 8$ блоков:

$$\mathbf{01}\,|\,\mathbf{01}\,|\,\mathbf{11}\,|\,\mathbf{11}\,|\,\mathbf{00}\,|\,\mathbf{00}\,|\,\mathbf{10}\,|\,\mathbf{10}.$$

Видим, что не во всех блоках находятся слова-квадраты; поэтому x_4 — существенная переменная.
▶

2.4. Принцип двойственности для булевых функций

Мы уже встречались с принципом двойственности (для булевых алгебр) и могли уже убедиться в его удобстве и полезности.

Для булевых функций также справедлив принцип двойственности и даже в более сильной форме. Чтобы сформулировать его, можно было бы рассуждать следующим образом: раз $\mathbb{BF}(n)$ можно рассматривать как булеву алгебру, то для нее справедлив общий для всех булевых алгебр принцип двойственности. Рассуждая так, действительно можно придти к «рабочему» для булевых функций принципу двойственности, но этот путь оказывается немного длинным и сопровождается различного рода отождествлениями. Поэтому для формулировки принципа двойственности для булевых функций избирают другой «двухходовый» путь: определение (двойственной функции) и теорема (принцип двойственности). Именно по этому пути пойдем и мы.

Определение 2.4. Для булевой функции $f(x_1,\dots,x_n)$ *двойственная* к ней функция $f^*(x_1,\dots,x_n)$ определяется следующим образом:

$$f^*(x_1,\dots,x_n) \overset{\text{def}}{:=} \overline{f(\bar{x}_1,\dots,\bar{x}_n)}.$$

Заметим, что $\mathbf{1}^*(x_1,\dots,x_n) = \mathbf{0}(x_1,\dots,x_n)$, а $\mathbf{0}^*(x_1,\dots,x_n) = \mathbf{1}(x_1,\dots,x_n)$. Действительно, для произвольных $(x_1,\dots,x_n) \in \mathbb{B}^n$ имеем

$$\begin{aligned}\mathbf{1}^*(x_1,\dots,x_n) &= \overline{\mathbf{1}(\bar{x}_1,\dots,\bar{x}_n)} = \mathbf{0} = \mathbf{0}(x_1,\dots,x_n),\\ \mathbf{0}^*(x_1,\dots,x_n) &= \overline{\mathbf{0}(\bar{x}_1,\dots,\bar{x}_n)} = \mathbf{1} = \mathbf{1}(x_1,\dots,x_n).\end{aligned}$$

Заметим прежде всего, что если функция $f(x_1,\dots,x_n)$ имеет следующее словесное представление

$$f = [\![\alpha_0\alpha_1\dots\alpha_{2^n-2}\alpha_{2^n-1}]\!],$$

то функции $f(\bar{x}_1,\dots,\bar{x}_n)$ и $\overline{f(\bar{x}_1,\dots,\bar{x}_n)}$ имеют следующие словесные представления

$$\begin{aligned}f(\bar{x}_1,\dots,\bar{x}_n) &= [\![\alpha_{2^n-1}\alpha_{2^n-2}\dots\alpha_1\alpha_0]\!] && (\text{«перевернутое слово»}),\\ \overline{f(\bar{x}_1,\dots,\bar{x}_n)} &= [\![\bar{\alpha}_{2^n-1}\bar{\alpha}_{2^n-2}\dots\bar{\alpha}_1\bar{\alpha}_0]\!] && \left(\begin{array}{l}\text{«навешивание черточки } ^- \text{ на}\\ \text{перевернутое слово»}\end{array}\right).\end{aligned}$$

Чтобы понять, почему это так, рассмотрим случай булевой функции трех переменных $f(x_1,x_2,x_3)$, из которого будет ясен весь механизм получения приведенных равенств. Итак, если

x_1	x_2	x_n	$f(x_1, x_2, x_3)$
0	**0**	**0**	α_0
0	**0**	**1**	α_1
0	**1**	**0**	α_2
0	**1**	**1**	α_3
1	**0**	**0**	α_4
1	**0**	**1**	α_5
1	**1**	**0**	α_6
1	**1**	**1**	α_7

,

то

x_1	x_2	x_3	$\bar{x}_1$	$\bar{x}_2$	$\bar{x}_3$	$f(\bar{x}_1, \bar{x}_2, \bar{x}_3)$	$\overline{f(\bar{x}_1, \bar{x}_2, \bar{x}_3)}$
0	**0**	**0**	**1**	**1**	**1**	α_7	$\bar{\alpha}_7$
0	**0**	**1**	**1**	**1**	**0**	α_6	$\bar{\alpha}_6$
0	**1**	**0**	**1**	**0**	**1**	α_5	$\bar{\alpha}_5$
0	**1**	**1**	**1**	**0**	**0**	α_4	$\bar{\alpha}_4$
1	**0**	**0**	**0**	**1**	**1**	α_3	$\bar{\alpha}_3$
1	**0**	**1**	**0**	**1**	**0**	α_2	$\bar{\alpha}_2$
1	**1**	**0**	**0**	**0**	**1**	α_1	$\bar{\alpha}_1$
1	**1**	**1**	**0**	**0**	**0**	α_0	$\bar{\alpha}_0$

.

Таким образом, если $f = [\![\alpha_0\alpha_1 \ldots \alpha_{2^n-2}\alpha_{2^n-1}]\!]$ — данная булева функция, то двойственная ей булева функция задается следующим образом:

$$f^* = [\![\bar{\alpha}_{2^n-1}\bar{\alpha}_{2^n-2} \ldots \bar{\alpha}_1\bar{\alpha}_0]\!].$$

Например, если

$$f = [\![\mathbf{0111001000111011}]\!]$$

данная булева функция, то двойственная ей булева функция задается словом

$$f^* = [\![\bar{\mathbf{1}}\bar{\mathbf{1}}\bar{\mathbf{0}}\bar{\mathbf{1}}\bar{\mathbf{1}}\bar{\mathbf{1}}\bar{\mathbf{0}}\bar{\mathbf{0}}\bar{\mathbf{0}}\bar{\mathbf{1}}\bar{\mathbf{0}}\bar{\mathbf{0}}\bar{\mathbf{1}}\bar{\mathbf{1}}\bar{\mathbf{1}}\bar{\mathbf{0}}]\!] = [\![\mathbf{0010001110110001}]\!].$$

В следующем примере на основе этого утверждения мы вычисляем двойственные функции для основных булевых функций одной и двух переменных.

Пример 3. В правой колонке следующей таблицы указаны исходные булевы функции, а в правой колонке — соответствующие им двойственные функции.

$f(x_1,\ldots,x_n)$	$f^*(x_1,\ldots,x_n)$
$x = \llbracket 01 \rrbracket$	$x = \llbracket 01 \rrbracket$
$\bar{x} = \llbracket 10 \rrbracket$	$\bar{x} = \llbracket 10 \rrbracket$
$x \vee y = \llbracket 0111 \rrbracket$	$x \wedge y = \llbracket 0001 \rrbracket$
$x \wedge y = \llbracket 0001 \rrbracket$	$x \vee y = \llbracket 0111 \rrbracket$
$x \to y = \llbracket 1101 \rrbracket$	$x \overset{*}{\to} y = \llbracket 0100 \rrbracket$
$x - y = \llbracket 0010 \rrbracket$	$x \overset{*}{-} y = \llbracket 1011 \rrbracket$
$x \oplus y = \llbracket 0110 \rrbracket$	$x \leftrightarrow y = \llbracket 1001 \rrbracket$
$x \leftrightarrow y = \llbracket 1001 \rrbracket$	$x \oplus y = \llbracket 0110 \rrbracket$
$x \mid y = \llbracket 1110 \rrbracket$	$x \downarrow y = \llbracket 1000 \rrbracket$
$x \downarrow y = \llbracket 1000 \rrbracket$	$x \mid y = \llbracket 1110 \rrbracket$
$x \overset{*}{\to} y = \llbracket 0100 \rrbracket$	$x \to y = \llbracket 1101 \rrbracket$
$x \overset{*}{-} y = \llbracket 1011 \rrbracket$	$x - y = \llbracket 0010 \rrbracket$

Из определения ясно также, что операция взятия двойственной функции является инволютивной операцией, т. е.

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

Пусть $\{x_1,\ldots,x_n\} = \{x_{11},\ldots,x_{1k_1}\} \cup \cdots \cup \{x_{m1},\ldots,x_{1k_m}\}$, т. е. $x_1,\ldots,x_n$ это символы всех различных переменных, встречающихся в множествах

$$\{x_{11}, x_{12}, \ldots, x_{1k_1}\}, \ldots, \{x_{m1}, x_{m2}, \ldots, x_{1k_m}\}.$$

Теорема 2.1. (Принцип двойственности для булевых функций). *Пусть* $f, g_1, \ldots, g_m$ *— булевы функции соответствующего числа переменных. Если*

$$\Phi(x_1, \ldots, x_n) = f\left(g_1(x_{11}, \ldots, x_{1k_1}), \ldots, g_m(x_{m1}, \ldots, x_{1k_m})\right),$$

то

$$\Phi^*(x_1, \ldots, x_n) = f^*\left(g_1^*(x_{11}, \ldots, x_{1k_1}), \ldots, g_m^*(x_{m1}, \ldots, x_{1k_m})\right).$$

◀ Доказательство сводится к непосредственному вычислению:

$$\Phi^*(x_1, \ldots, x_n) \triangleq \overline{\Phi(\bar{x}_1, \ldots, \bar{x}_n)} =$$
$$= \overline{f\left(g_1(\bar{x}_{11}, \ldots, \bar{x}_{1k_1}), \ldots, g_m(\bar{x}_{m1}, \ldots, \bar{x}_{1k_m})\right)} =$$
$$= \overline{f\left(\overline{\overline{g_1(\bar{x}_{11}, \ldots, \bar{x}_{1k_1})}}, \ldots, \overline{\overline{g_m(\bar{x}_{m1}, \ldots, \bar{x}_{1k_m})}}\right)} =$$
$$= \overline{f\left(\overline{g_1^*(x_{11}, \ldots, x_{1k_1})}, \ldots, \overline{g_m^*(x_{m1}, \ldots, x_{1k_m})}\right)} =$$
$$= f^*\left(g_1^*(x_{11}, \ldots, x_{1k_1}), \ldots, g_m^*(x_{m1}, \ldots, x_{1k_m})\right).$$

Доказательство завершено. ▶

Хотя эта теорема вполне адекватно отражает суть принципа двойственности для булевых функций, мы приведем также и следующую его переформулировку:

Принцип двойственности для булевых функций:

Если булева функция Φ построена с помощью булевых функций $f, g_1, \ldots, g_m$ посредством операции суперпозиции функций, то функция Φ^*, двойственная к функции Φ, построена с помощью булевых функций $f^*, g_1^*, \ldots, g_m^*$, двойственных к $f, g_1, \ldots, g_m$; причем порядок применения операции суперпозиции для получения Φ^* с помощью $f^*, g_1^*, \ldots, g_m^*$ соответствует порядку применения операции суперпозиции для получения функции Φ с помощью $f, g_1, \ldots, g_m$.

Пример 4. Найти выражение для функции, двойственной для булевой функции

$$\Phi(x_1, x_2, x_3, x_4) = (x_1 \to x_3) \vee ((x_1 \oplus (x_2 \downarrow x_4)) \wedge (x_3 \to x_4)).$$

Решение. По принципу двойственности для булевых функций, чтобы получить выражение для двойственной функции $\Phi^*(x_1, x_2, x_3, x_4)$, достаточно в выражении для $\Phi(x_1, x_2, x_3, x_4)$ одновременно заменить все операции на двойственные:

$$\Phi^*(x_1, x_2, x_3, x_4) = (x_1 \overset{*}{\to} x_3) \wedge ((x_1 \leftrightarrow (x_2 \,|\, x_4)) \vee (x_3 \overset{*}{\to} x_4)),$$

или с учетом легко проверяемого равенства $x \overset{*}{\to} y = \bar{x} \wedge y$ имеем

$$\Phi^*(x_1, x_2, x_3, x_4) = (\bar{x}_1 \wedge x_3) \wedge ((x_1 \leftrightarrow (x_2 \,|\, x_4)) \vee (\bar{x}_3 \wedge x_4)),$$

Действительно, положив

$$
\begin{array}{ll}
f(x,y) = x \vee y & (\text{ тогда } f^*(x,y) = x \wedge y\ ) \\
g_1(x,y) = x \to y & (\text{ тогда } g_1^*(x,y) = x \overset{*}{\to} y = \bar{x} \wedge y\ ) \\
g_2(x,y) = x \wedge y & (\text{ тогда } g_2^*(x,y) = x \vee y\ ) \\
g_3(x,y) = x \oplus y & (\text{ тогда } g_3^*(x,y) = x \leftrightarrow y\ ) \\
g_4(x,y) = x \downarrow y & (\text{ тогда } g_4^*(x,y) = x \,|\, y\ ),
\end{array}
$$

имеем

$$
\begin{aligned}
\Phi(x_1,x_2,x_3,x_4) &= f\big((x_1 \to x_3), ((x_1 \oplus (x_2 \downarrow x_4)) \wedge (x_3 \to x_4))\big) = \\
&= f\big(g_1(x_1,x_3), g_2((x_1 \oplus (x_2 \downarrow x_4)), (x_3 \to x_4))\big) = \\
&= f\big(g_1(x_1,x_3), g_2(g_3(x_1,(x_2 \downarrow x_4)), g_1(x_3,x_4))\big) = \\
&= f\big(g_1(x_1,x_3), g_2(g_3(x_1,g_4(x_2,x_4)), g_1(x_3,x_4))\big).
\end{aligned}
$$

Итак,

$$\Phi(x_1,x_2,x_3,x_4) = f\big(g_1(x_1,x_3), g_2(g_3(x_1,g_4(x_2,x_4)), g_1(x_3,x_4))\big).$$

Согласно доказанной теореме

$$\Phi^*(x_1,x_2,x_3,x_4) = f^*\big(g_1^*(x_1,x_3), g_2^*(g_3^*(x_1,g_4^*(x_2,x_4)), g_1^*(x_3,x_4))\big),$$

то есть

$$
\begin{aligned}
\Phi^*(x_1,x_2,x_3,x_4) &= g_1^*(x_1,x_3)\wedge g_2^*(g_3^*(x_1,g_4^*(x_2,x_4)),g_1^*(x_3,x_4)) = \\
&= (x_1 \xrightarrow{*} x_3)\wedge \big(g_3^*(x_1,g_4^*(x_2,x_4)\vee g_1^*(x_3,x_4)\big) = \\
&= (x_1 \xrightarrow{*} x_3)\wedge \big((x_1\leftrightarrow g_4^*(x_2,x_4))\vee (x_3 \xrightarrow{*} x_4)\big) = \\
&= (x_1 \xrightarrow{*} x_3)\wedge ((x_1\leftrightarrow (x_2\,|\,x_4))\vee (x_3 \xrightarrow{*} x_4)) = \\
&= (\bar{x}_1\wedge x_3)\wedge ((x_1\leftrightarrow (x_2\,|\,x_4))\vee (\bar{x}_3\wedge x_4)),
\end{aligned}
$$

как и утверждалось в самом начале. ►

2.5. Упражнения

1. Задать следующие булевы функции, заданные обобщенными булевыми выражениями, в виде таблицы, в виде слова и с помощью характеристического множества:
   1) $f(x,y)=(x\to y)\vee(x\oplus(\bar{x}\cdot y))$;
   2) $f(x,y)=(x\cdot(y\to x))\to\bar{x}$;
   3) $f(x,y)=(x\cdot(y\vee\bar{x}))\cdot((\bar{y}\to x)\vee y)$;
   4) $f(x,y)=(x\leftrightarrow\bar{y})\to(\bar{y}\,|(\bar{x}\cdot y))$;
   5) $f(x,y,z)=(\bar{y}\vee x)\cdot(x\to(z\vee y))$;
   6) $f(x,y,z)=((x\to y)\to z)\leftrightarrow(x\to(y\to z))$;
   7) $f(x,y,z)=((x\downarrow y)\,|\,(\bar{x}\downarrow\bar{y}))\vee((x\,|\,y)\downarrow(\bar{x}\,|\,\bar{y}))$;
   8) $f(x,y,z)=(x\to(y\to z))\vee(\bar{x}\to(\bar{y}\to\bar{z}))$;

9) $f(x,y,z) = (x \oplus \bar{y}) \downarrow (y \oplus \bar{z}) \downarrow (z \oplus \bar{x})$;

10) $f(x,y,z) = ((\bar{x} \cdot y) \downarrow y)) \to (z \to \bar{y})$;

11) $f(x,y,z) = ((x \to \bar{y}) \vee (x \oplus z)) \cdot (y \,|\, z)$;

12) $f(x,y,z) = \overline{\bar{x} \to y} \oplus ((x \to z) \leftrightarrow y) \cdot z$;

13) $f(x,y,z) = \overline{(x \leftrightarrow y) \vee (\bar{y} \to z)} \downarrow ((x \oplus z) \vee y)$.

2. По функциям $f(x_1,x_2)$ и $g(x_1,x_2)$, заданным с помощью слова, построить словесное представление функции h:

1) $f = [\![\mathbf{0111}]\!]$, $g = [\![\mathbf{1001}]\!]$,

$$h(x_1,x_2) = g(g(x_1,x_2),x_1) \to f(x_2, g(x_2,x_1);$$

2) $f = [\![\mathbf{0110}]\!]$, $g = [\![\mathbf{1101}]\!]$,

$$h(x_1,x_2) = f(x_1, g(x_2,x_1)) \leftrightarrow g(x_2, f(x_1,x_2).$$

3) $f = [\![\mathbf{1100}]\!]$, $g = [\![\mathbf{0111}]\!]$,

$$h(x_1,x_2,x_3) = f(x_1, g(x_2,x_3)) \wedge g(x_2,x_1);$$

4) $f = [\![\mathbf{0001}]\!]$, $g = [\![\mathbf{0110}]\!]$,

$$h(x_1,x_2,x_3) = f(g(x_1,x_1),x_3) \oplus g(x_2,x_3);$$

3. Доказать следующие равенства для характеристических множеств булевых функций $f(x_1,\dots,x_n)$ и $g(x_1,\dots,x_n)$:

1) $N_{\bar{f}} = \overline{N}_f$;

2) $N_{f \vee g} = N_f \cup N_g$;

Сайт ДГУ
Тиульный лист
Оглавление
страница 53 из 158
Назад
Полный экран
Закрыть
Выход

3) $N_{f\wedge g} = N_f \cap N_g$;

4) $N_{f\to g} = \overline{N}_f \cup N_g$;

5) $N_{f\oplus g} = N_f \bigtriangleup N_g = (N_f \setminus N_g) \cup (N_g \setminus N_f) = (\overline{N}_f \cap N_g) \cup (N_f \cap \overline{N}_g)$;

6) $N_{f\leftrightarrow g} = (\overline{N}_f \cup N_g) \cap (N_f \cup \overline{N}_g) = (N_f \cap N_g) \cup (\overline{N}_f \cap \overline{N}_g)$;

7) $N_{f-g} = N_f \setminus N_g$;

8) $N_{f\downarrow g} = \overline{N}_f \cap \overline{N}_g = \overline{N_f \cup N_g}$;

9) $N_{f\,|\,g} = \overline{N}_f \cup \overline{N}_g = \overline{N_f \cap N_g}$.

4. Построить таблицы Вейча следующих функций, соответствующих разбиению переменных $\{x_1, x_2\}\big|\{x_3, x_4\}$:

1) $f = [\![\mathbf{1100010110111001}]\!]$;

2) $f = [\![\mathbf{0110000101101010}]\!]$;

3) $f = [\![\mathbf{1011000011101011}]\!]$;

4) $f = [\![\mathbf{0101011010110100}]\!]$.

5. С помощью таблиц или иным способом доказать *основные булевы равенства* (см. стр. 34).

6. Используя основные булевы равенства, доказать равенство булевых функций f и g:

1) $f(x,y) = (\bar{x} \to y) \to (\bar{x}\cdot y \leftrightarrow (x \oplus y)), \quad g(x,y) = (\overline{x\cdot y} \to x) \to y$;

2) $f(x,y,z) = (x \oplus y\cdot z) \to (\bar{x} \to (y \to z))$,

$$g(x,y,z) = x \to ((y \to z) \to x);$$

3) $f(x,y,z) = (\bar{x} \to (\bar{y} \to (x \leftrightarrow z))) \cdot (x \leftrightarrow (y \to (z \vee (x \to y))))$,

$$g(x,y,z) = (x \to (y \to z)) \to x;$$

4) $f(x,y,z) = (\bar{x} \vee \bar{y} \cdot z) \to ((x \to y) \to ((y \vee z) \to \bar{x}))$,

$$g(x,y,z) = (x \to y) \to (\bar{y} \to \bar{x});$$

5) $f(x,y,z) = (x \cdot \bar{y} \vee \bar{x} \cdot z) \oplus ((y \to z) \to \bar{x} \cdot y)$,

$$g(x \cdot (\bar{y} \cdot \bar{z}) \oplus y) \oplus z).$$

6) $f(x_1, \ldots, x_n, y) = x_1 \to (x_2 \to (x_3 \to \ldots (x_n \to y) \ldots))$,

$$g(x_1, \ldots, x_n, y) = (x_1 \wedge x_2 \wedge \ldots \wedge x_n) \to y.$$

7. Построив таблицы, выяснить равны ли функции f и g:

1) $f(x,y,z) = (x \to y) \oplus ((y \to \bar{z}) \to x \cdot y)$, $g(x,y,z) = \overline{y \cdot z \to x}$;

2) $f(x,y,z) = (x \vee \bar{y}) \downarrow (\bar{x} \to (y \to z))$, $g(x,y,z) = \overline{y \to (x \vee z)}$;

3) $f(x,y,z) = x \to ((y \to z) \to y \cdot z)$,

$$g(x,y,z) = (x \vee (y \to z)) \cdot (x \oplus y);$$

4) $f(x,y,z) = \overline{(x \downarrow y) \vee (x \leftrightarrow z)} \,|\, (x \oplus y \cdot z)$,

$$g(x,y,z) = \bar{x} \cdot (y \cdot z) \vee \overline{x \to z};$$

5) $f(x,y,z) = (\bar{x} \vee y) \to ((y \,|\, \bar{z}) \to (x \leftrightarrow x \cdot z))$,

$$g(x,y,z) = (x \cdot y \vee (\overline{(x \to x\bar{y})} \to z).$$

8. Построив таблицы соответствующих функций, убедиться в справедливости следующих равенств:

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

2) $x \leftrightarrow y = (x \to y) \wedge (y \to x)$;

3) $x \downarrow y = ((x \,|\, x) \,|\, (y \,|\, y)) \,|\, ((x \,|\, x) \,|\, (y \,|\, y))$;

4) $x \vee (y \equiv z) = (x \vee y) \leftrightarrow (x \vee z)$;

5) $x \to (y \leftrightarrow z) = (x \to y) \leftrightarrow (x \to z)$;

6) $x + (y \to z) = (x \vee y) \to (x \vee z)$;

7) $x \wedge (y \to z) = (x \to y) \to (x \wedge z)$;

8) $x \to (y \vee z) = (x \to y) \vee (x \to z)$;

9) $x \to (y \wedge z) = (x \to y) \wedge (x \to z)$;

10) $x \to (y \to z) = (x \to y) \to (x \to z)$.

9. Указать фиктивные и существенные переменные функции f:

1) $f = \llbracket \mathbf{10101010} \rrbracket$;

2) $f = \llbracket \mathbf{01100110} \rrbracket$;

3) $f = \llbracket \mathbf{1011010110110101} \rrbracket$;

4) $f = \llbracket \mathbf{1100110000110011} \rrbracket$;

5) $f = \llbracket \mathbf{1001001100110010} \rrbracket$;

6) $f = \llbracket \mathbf{1100001100111100} \rrbracket$;

7) $f = \llbracket \mathbf{0110110110110111} \rrbracket$;

8) $f = \llbracket \mathbf{0000000111111110} \rrbracket$;

9) $f = [\![\mathbf{0001000101110111}]\!]$;

10) $f = [\![\mathbf{0111011110101010}]\!]$.

10. Показать, что переменная x_1 является фиктивной, преобразовав выражение, задающее функцию f к выражению, не содержащему явно переменную x_1.

1) $f(x_1, x_2) = (x_2 \to x_1) \cdot (x_2 \downarrow x_2)$;

2) $f(x_1, x_2) = (x_1 \oplus x_2) \cdot (x_1 \downarrow x_2)$;

3) $f(x_1, x_2, x_3) = ((x_1 \vee x_2 \vee \bar{x}_3) \to (x_1 \cdot (x_2 \,|\, x_3))) \oplus (x_2 \to x_1) \cdot x_3$;

4) $f(x_1, x_2, x_3, x_4) = (x_1 \to ((x_2 \to x_3) \to x_4)) \leftrightarrow \bar{x}_1 \cdot (x_2 \to x_3) \cdot x_4$;

5) $f(x_1, x_2, x_3, x_4) = ((x_1x_2 \vee x_3x_4) \cdot (x_1 \oplus x_2 \oplus x_3) \to x_4) \oplus$

$\oplus (x_1x_2 \cdot (x_3 \to x_4) \vee x_3x_4)$.

11. Перечислить существенные переменные следующих функций:

1) $f(x_1, x_2) = (x_2 \to x_1) \cdot (x_2 \downarrow x_2)$;

2) $f(x_1, x_2) = (x_1 \oplus x_2) \cdot (x_1 \downarrow x_2)$;

3) $f(x_1, x_2, x_3) = (x_1 \to x_2x_3) \cdot (x_2 \to x_1x_3) \vee (x_1 \leftrightarrow x_2)$;

4) $f(x_1, x_2, x_3) = ((x_1 \downarrow (x_2 \,|\, x_3)) \downarrow (x_2 \,|(x_1 \downarrow x_3))) \downarrow (x_1 \,|\, x_2)$;

5) $f(x_1, x_2, x_3, x_4) = (x_1x_2 \oplus x_3x_4) \vee ((x_1x_2 \leftrightarrow x_2) \to x_4) \vee \bar{x}_1x_3$.

12. Булевы функции $f(x_1, \ldots, x_n)$ и $g(y_1, \ldots, y_m)$ существенно зависят от всех своих переменных. Переменные $x_1, \ldots, x_n, y_1, \ldots, y_m$ попарно различные. Показать, что функция $f(g(y_1, \ldots, y_m), x_2, \ldots, x_n)$ существенно зависит от всех своих переменных.

13. Является ли функция f двойственной к функции g, если

1) $f = x \to y, \quad g = x \cdot \bar{y};$

2) $f = x \to y, \quad g = \overline{y \to x};$

3) $f = x \to y, \quad g = y \to x;$

4) $f = xy \vee xz \vee yz, \quad g = xy \oplus xz \oplus yz;$

5) $f = x\bar{y}z \vee x \cdot (y \leftrightarrow z), \quad g = [\![\mathbf{01101101}]\!].$

14. Найти функцию f^*, двойственную к функции f:

1) $f(x, y, z, t) = (x \vee (\bar{y} \to t)) \wedge ((x \downarrow z) \oplus (t \,|\, z));$

2) $f(x, y, z, t) = (x \cdot z \oplus (t \leftrightarrow y)) \to (\bar{t} \vee x \vee z);$

3) $f(x, y, z, t) = (z \to x) \vee (x \cdot \bar{y} \cdot t \oplus (z \vee \bar{t}));$

4) $f = [\![\mathbf{0110111001101100}]\!];$

5) $f = [\![\mathbf{1001010011101001}]\!].$

15. Доказать, что если функция $f(x_1, \ldots, x_n)$ существенно зависит от переменной x_i $(1 \leqslant i \leqslant n)$, то двойственная к ней булева функция $f^*(x_1, \ldots, x_n)$ также зависит существенно от x_i.

3. Важнейшие формы представления функций посредством булевых выражений

3.1. Предварительные факты и понятия

Напомним обозначение: если σ есть $\mathbf{0}$ или $\mathbf{1}$, то

$$x^\sigma \overset{\text{def}}{:=} x\sigma \vee \bar{x}\bar{\sigma},$$

т. е.

$$x^\sigma = \begin{cases} \bar{x}, & \text{если } \sigma = \mathbf{0}; \\ x, & \text{если } \sigma = \mathbf{1}. \end{cases}$$

Прежде всего приведем ряд определений.

✓ *Элементарной конъюнкцией ранга* k $(1 \leqslant k \leqslant n)$ или *конъюнктом ранга* k над множеством переменных $\{x_1, \ldots, x_n\}$ называется булево выражение вида

$$x_{i_1}^{\sigma_{i_1}} x_{i_2}^{\sigma_{i_2}} \ldots x_{i_k}^{\sigma_{i_k}}, \quad 1 \leqslant k \leqslant n,$$

где $\{x_{i_1}, \ldots, x_{i_k}\}$ — k-подмножество множества $\{x_1, \ldots, x_n\}$, а каждое из σ_{i_j} $(1 \leqslant j \leqslant k)$ есть $\mathbf{0}$ или $\mathbf{1}$.

Элементарной конъюнкцией ранга 0 (*пустым конъюнктом*) называется по определению булева единица $\mathbf{1}$.

✓ *Полным конъюнктом* над множеством переменных $\{x_1, \ldots, x_n\}$ называется элементарная конъюнкция ранга n над этим множеством переменных, т. е. булево выражение вида

$$x_1^{\sigma_1} x_2^{\sigma_2} \ldots x_n^{\sigma_n}.$$

✓ *Дизъюнктивной нормальной формой* (коротко, ДНФ) длины s над множеством переменных $\{x_1, \ldots, x_n\}$ называется выражение вида

$$\mathcal{D} = K_1 \vee K_2 \vee \ldots \vee K_s,$$

где $K_1, K_2, \ldots, K_s$ являются конъюнктами (их будем называть конъюнктивными членами $\mathcal{D}$) над множеством переменных $\{x_1, \ldots, x_n\}$ возможно различных рангов. (Кратко: ДНФ — это дизъюнкция конъюнктов.)

✓ *Совершенной дизъюнктивной нормальной формой* (коротко, СДНФ) над множеством переменных $\{x_1, \ldots, x_n\}$ называется выражение вида

$$\mathcal{D} = K_1 \vee K_2 \vee \ldots \vee K_s,$$

где $K_1, K_2, \ldots, K_s$ являются *полными* конъюнктами над множеством переменных $\{x_1, \ldots, x_n\}$.

✓ *Монотонным (булевым) произведением ранга* k или *монотонным конъюнктом ранга* k над множеством переменных $\{x_1, \ldots, x_n\}$ называется булево выражение вида

$$x_{i_1} x_{i_2} \ldots x_{i_k},$$

где $\{x_{i_1},\ldots,x_{i_k}\}$ — k-подмножество множества $\{x_1,\ldots,x_n\}$.
Монотонным конъюнктом ранга 0 есть по определению $\mathbf{1}$.

✓ *Полиномом Жегалкина* над множеством $\{x_1,\ldots,x_n\}$ называется булево выражение вида

$$\mathcal{G} = a_1M_1 \oplus a_2M_2 \oplus \ldots \oplus a_sM_s,$$

где $M_1, M_2, \ldots, M_s$ — все монотонные конъюнкты над множеством переменных $\{x_1,\ldots,x_n\}$, а каждое из $a_1, a_2, \ldots, a_s$ есть $\mathbf{0}$ или $\mathbf{1}$.

Двойственным образом

✓ *Элементарной дизъюнкцией ранга* k или *дизъюнктом ранга* k над множеством переменных $\{x_1,\ldots,x_n\}$ называется булево выражение вида

$$x_{i_1}^{\sigma_{i_1}} \vee x_{i_2}^{\sigma_{i_2}} \vee \ldots \vee x_{i_k}^{\sigma_{i_k}}, \quad 1 \leqslant k \leqslant n,$$

где $\{x_{i_1},\ldots,x_{i_k}\}$ — k-подмножество множества $\{x_1,\ldots,x_n\}$, а каждое из σ_{i_j} $(1 \leqslant j \leqslant k)$ есть $\mathbf{0}$ или $\mathbf{1}$.
Элементарной дизъюнкцией ранга 0 (*пустым дизъюнктом*) называется по определению булев нуль $\mathbf{0}$.

✓ *Полным дизъюнктом* над множеством $\{x_1,\ldots,x_n\}$ называется элементарная дизъюнкция ранга n над этим множеством переменных, т. е. булево выражение вида

$$x_1^{\sigma_1} \vee x_2^{\sigma_2} \vee \ldots \vee x_n^{\sigma_n}.$$

✓ *Конъюнктивной нормальной формой* (коротко, КНФ) длины s над множеством переменных $\{x_1, \ldots, x_n\}$ называется выражение вида

$$\mathcal{K} = D_1 \wedge D_2 \wedge \ldots \wedge D_s,$$

где $D_1, D_2, \ldots, D_s$ являются дизъюнктами (их будем называть дизъюнктивными членами $\mathcal{K}$) над множеством переменных $\{x_1, \ldots, x_n\}$ возможно различных рангов. (Кратко: КНФ — это конъюнкция дизъюнктов.)

✓ *Совершенной конъюнктивной нормальной формой* (коротко, СКНФ) над множеством переменных $\{x_1, \ldots, x_n\}$ называется выражение вида

$$\mathcal{K} = D_1 \wedge D_2 \wedge \ldots \wedge D_s,$$

где $D_1, D_2, \ldots, D_s$ являются *полными* дизъюнктами над множеством переменных $\{x_1, \ldots, x_n\}$.

✓ *Монотонной (булевой) суммой ранга k* или *монотонным дизъюнктом ранга k* над множеством переменных $\{x_1, \ldots, x_n\}$ называется булево выражение вида

$$x_{i_1} \vee x_{i_2} \vee \ldots \vee x_{i_k}.$$

Монотонный дизъюнкт ранга 0 есть по определению $\mathbf{0}$.

✓ *Кополиномом Жегалкина* над множеством переменных $\{x_1, \ldots, x_n\}$ будем называть булево выражение вида

$$\mathcal{J} = (a_1 \vee P_1) \leftrightarrow (a_2 \vee P_2) \leftrightarrow \ldots \leftrightarrow (a_s \vee P_s),$$

где $P_1, P_2, \ldots, P_s$ — все монотонные дизъюнкты над множеством переменных $\{x_1, \ldots, x_n\}$, а каждое из $a_1, a_2, \ldots, a_s$ есть $\mathbf{0}$ или $\mathbf{1}$.

Введем еще термин «формальное отличие …».

✓ Два конъюнкта $x_{i_1}^{\sigma_{i_1}} x_{i_2}^{\sigma_{i_2}} \ldots x_{i_k}^{\sigma_{i_k}}$ и $x_{j_1}^{\varepsilon_{j_1}} x_{j_2}^{\varepsilon_{j_2}} \ldots x_{j_m}^{\varepsilon_{j_m}}$ будем называть *формально различными*, если

$$\{x_{i_1}^{\sigma_{i_1}}, x_{i_2}^{\sigma_{i_2}}, \ldots, x_{i_k}^{\sigma_{i_k}}\} \neq \{x_{j_1}^{\varepsilon_{j_1}}, x_{j_2}^{\varepsilon_{j_2}}, \ldots, x_{j_m}^{\varepsilon_{j_m}}\}.$$

✓ Две ДНФ $\mathcal{D}$ и $\mathcal{D}'$ будем называть *формально различными*, если хотя бы в одной из них найдется конъюнктивный член, формально отличающийся от всех конъюнктивных членов другой ДНФ.

Аналогично определяются формальные отличия монотонных конъюнкций, полиномов Жегалкина и двойственных понятий.

Обоснованием введения термина «формальное отличие …» является тот неудивительный факт, что различные по форме записи булевы выражения могут реализовывать одну и ту же булеву функцию. Однако, как следует из доказываемой ниже леммы 3.3, формально различные конъюнкции, монотонные конъюнкции, СДНФ и полиномы Жегалкина действительно реализуют различные булевы функции. Но, например, две формально различные ДНФ $\mathcal{D} = x_1 \vee x_1 x_2$ и $\mathcal{D}' = x_1 x_3 \vee x_1 \bar{x}_3 \vee x_1 x_2$ задают одну и ту же булеву функцию, т. к.

$$x_1 \vee x_1 x_2 = x_1 \mathbf{1} \vee x_1 x_2 = x_1(x_3 \vee \bar{x}_3) \vee x_1 x_2 = x_1 x_3 \vee x_1 \bar{x}_3 \vee x_1 x_2.$$

Далее приведем три леммы, в которых собраны несколько фактов, связанных с введенными понятиями. Предлагаем читателю в качестве упражнения сформулировать двойственные утверждения.

Лемма 3.1. *Справедливы следующие утверждения:*

1. *Конъюнкция* $x_{i_1}x_{i_2}\dots x_{i_k}$ *принимает значение* $\mathbf{1}$ *тогда и только тогда, когда все переменные* $x_{i_1}, x_{i_2}, \dots, x_{i_k}$ *принимают значение* $\mathbf{1}$. *Конъюнкция* $x_{i_1}x_{i_2}\dots x_{i_k}$ *принимает значение* $\mathbf{0}$ *тогда и только тогда, когда хотя бы одна из переменных* $x_{i_1}, x_{i_2}, \dots, x_{i_k}$ *принимает значение* $\mathbf{0}$.

2. $x^\sigma x^\varepsilon = (\sigma \leftrightarrow \varepsilon)\cdot x^\sigma$.

3. *Произведения двух формально различных полных конъюнктов равно нулю:*

$$(x_1^{\sigma_1}x_2^{\sigma_2}\dots x_n^{\sigma_n})\cdot(x_1^{\varepsilon_1}x_2^{\varepsilon_2}\dots x_n^{\varepsilon_n}) = \begin{cases} x_1^{\sigma_1}x_2^{\sigma_2}\dots x_n^{\sigma_n}, & \text{если } \tilde\sigma = \tilde\varepsilon;\\ \mathbf{0}, & \text{если } \tilde\sigma \ne \tilde\varepsilon.\end{cases}$$

где $\tilde\sigma = (\sigma_1, \sigma_2, \dots, \sigma_n), \tilde\varepsilon = (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n)$.

◀ 1. Для двух сомножителей утверждение следует прямо из определения функции $x\cdot y$. Для произвольного числа сомножителей утверждение получается индукцией по числу сомножителей с использованием представления

$$x_{i_1}x_{i_2}\dots x_{i_{k-1}}x_{i_k} = (x_{i_1}x_{i_2}\dots x_{i_{k-1}})\cdot x_{i_k} = x\cdot y,$$

где $x = x_{i_1}x_{i_2}\dots x_{i_{k-1}}$, а $y = x_{i_k}$.

2. Получается простым перебором всех 8 возможных случаев:

x	σ	ε	$x^\sigma x^\varepsilon$	$(\sigma \leftrightarrow \varepsilon) \cdot x^\sigma$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0^0 \cdot 0^0 = \underline{1}}$	$\mathbf{(0 \leftrightarrow 0) \cdot 0^0 = \underline{1}}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{0^0 \cdot 0^1 = \underline{0}}$	$\mathbf{(0 \leftrightarrow 0) \cdot 0^0 = \underline{0}}$
$\mathbf{0}$	$\mathbf{1}$	$\mathbf{0}$	$\mathbf{0^1 \cdot 0^0 = \underline{0}}$	$\mathbf{(1 \leftrightarrow 1) \cdot 0^1 = \underline{0}}$
$\mathbf{0}$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{0^1 \cdot 0^1 = \underline{1}}$	$\mathbf{(1 \leftrightarrow 1) \cdot 0^1 = \underline{1}}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1^0 \cdot 1^0 = \underline{0}}$	$\mathbf{(0 \leftrightarrow 0) \cdot 1^0 = \underline{0}}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{1^0 \cdot 1^1 = \underline{0}}$	$\mathbf{(0 \leftrightarrow 0) \cdot 1^0 = \underline{0}}$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1^1 \cdot 1^0 = \underline{0}}$	$\mathbf{(1 \leftrightarrow 1) \cdot 1^1 = \underline{0}}$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1^1 \cdot 1^1 = \underline{1}}$	$\mathbf{(1 \leftrightarrow 1) \cdot 1^1 = \underline{1}}$

3. Следует из равенства

$$
\begin{aligned}
(x_1^{\sigma_1} x_2^{\sigma_2} \dots x_n^{\sigma_n}) \cdot (x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n}) = (x_1^{\sigma_1} x_1^{\varepsilon_1})(x_2^{\sigma_2} x_2^{\varepsilon_2}) \cdots (x_n^{\sigma_n} x_n^{\varepsilon_n}) = \\
= (\sigma_1 \leftrightarrow \varepsilon_1) x_1^{\sigma_1} (\sigma_2 \leftrightarrow \varepsilon_2) x_2^{\sigma_2} \cdots (\sigma_n \leftrightarrow \varepsilon_n) x_n^{\sigma_n} = \\
= (\sigma_1 \leftrightarrow \varepsilon_1)(\sigma_2 \leftrightarrow \varepsilon_2) \cdots (\sigma_n \leftrightarrow \varepsilon_n) x_1^{\sigma_1} x_2^{\sigma_2} \cdots x_n^{\sigma_n}.
\end{aligned}
$$

Лемма доказана. ►

В следующих утверждениях даются количественные характеристики некоторых определенных выше конструкций над множеством переменных $\{x_1, \dots, x_n\}$.

Лемма 3.2. *Пусть $\{x_1, \dots, x_n\}$ — данное множество переменных. Тогда справедливы следующие утверждения:*

1. *Число формально различных элементарных конъюнкций ранга k равно $2^k\binom{n}{k}$, а число формально различных элементарных конъюнкций всевозможных рангов (от $k=0$ до $k=n$) равно 3^n.*

2. *Число формально различных монотонных конъюнкций ранга $k\,(1\leqslant k\leqslant n)$ равно $\binom{n}{k}$, а число формально различных монотонных конъюнкций всевозможных рангов (от $k=0$ до $k=n$) равно 2^n.*

3. *Число формально различных ДНФ длины s равно $\binom{3^n}{s}$, а число формально различных ДНФ всевозможных длин равно $2^{3^n}-1$.*

4. *Число формально различных СДНФ равно $2^{2^n}-1$.*

5. *Число формально различных полиномов Жегалкина равно 2^{2^n}.*

◀ 1. Для того чтобы однозначно определить конъюнкт $x_{i_1}^{\sigma_{i_1}}\cdots x_{i_k}^{\sigma_{i_k}}$ ранга k, $(1\leqslant k\leqslant n)$ над множеством переменных $\{x_1,\ldots,x_n\}$ достаточно сделать следующие два шага:

1) выбрать k различных переменных $x_{i_1},\ldots,x_{i_k}$ из множества переменных $\{x_1,\ldots,x_n\}$ — это можно сделать $\binom{n}{k}$ способами;

2) выбрать k различных значений $\sigma_{i_1},\ldots,\sigma_{i_k}$, каждое из которых есть **0** или **1** — это можно сделать 2^k способами.

По правилу произведения количество конъюнктов ранга k равно $2^k\binom{n}{k}$.

Число конъюнктов различных рангов (от $k=0$ до $k=n$) значит равно (с учетом того, что конъюнкт ранга 0 есть по определению $\mathbf{1}$):

$$1+2\binom{n}{1}+2^2\binom{n}{2}+\ldots 2^n\binom{n}{n}=(1+2)^n=3^n.$$

2. Для того чтобы однозначно указать на монотонный конъюнкт $x_{i_1}x_{i_2}\cdots x_{i_k}$ ранга k, $(1\leqslant k\leqslant n)$ над множеством переменных $\{x_1,\ldots,x_n\}$ достаточно указать те k различных переменных $x_{i_1},\cdots,x_{i_k}$ из множества $\{x_1,\ldots,x_n\}$, которые его составляют. А это можно сделать $\binom{n}{k}$ способами.

Число монотонных конъюнктов различных рангов (от $k=0$ до $k=n$) значит равно $\sum_{k=0}^{n}\binom{n}{k}=2^n$.

3. Пусть $\{K_1,K_2,\ldots,K_m\}$ — множество всех формально различных конъюнктов. По доказанному только что, их число равно 3^n, т. е. $m=3^n$. Чтобы задать какую-то ДНФ длины $s\geqslant 1$ надо просто выбрать s элементов в этом множестве и взять их дизъюнкцию. А число таких выборов равно $\binom{m}{s}=\binom{3^n}{s}$.

Число ДНФ различных длин (от $s=1$ до $s=m$) равно $\sum_{s=1}^{m}\binom{m}{s}=2^m-1=2^{3^n}-1$.

4. Мы уже показали, что число формально различных полных конъюнктов, т. е. конъюнктов длины n, равно $2^n\binom{n}{n}=2^n$. Пусть $\{K_1,\ldots,K_m\}$ — множество всех формально различных полных конъюнктов и, значит, $m=2^n$. СДНФ можно полностью задать, указав то непустое подмножество полных конъюнктов из этого множества, которые составляют эту СДНФ. Значит формально различных СДНФ столько же сколько существует непустых подмножеств во множестве $\{K_1,K_2,\ldots,K_m\}$, т. е. равно $2^{2^n}-1$.

5. Мы показали, что число формально различных монотонных конъюнктов равно 2^n. Пусть $\{M_1,M_2,\ldots,M_m\}$ — множество всех формально различных монотонных конъюнктов и, значит,

$m = 2^n$. Полином Жегалкина есть по определению выражение вида

$$\mathcal{G} = a_1 M_1 \oplus a_2 M_2 \oplus \ldots \oplus a_m M_m,$$

где каждое из $a_1, a_2, \ldots, a_m$ есть $\mathbf{0}$ или $\mathbf{1}$. Значит число формально различных полиномов Жегалкина такое же, как количество упорядоченных наборов $(a_1, \ldots, a_m)$, где $a_j = \mathbf{0}$ или $a_j = \mathbf{1}$ $(j = 1, \ldots, m)$, т. е. равно $2^m = 2^{2^n}$. ▶

Лемма 3.3. *Справедливы следующие утверждения*

1. *Формально различные конъюнкции реализуют различные булевы функции.*
2. *Формально различные СДНФ реализуют различные булевы функции.*
3. *Формально различные полиномы Жегалкина реализуют различные булевы функции.*

◀ 1. Пусть $x_{i_1}^{\sigma_{i_1}} x_{i_2}^{\sigma_{i_2}} \ldots x_{i_k}^{\sigma_{i_k}}$ и $x_{j_1}^{\varepsilon_{j1}} x_{j2}^{\varepsilon_{j2}} \ldots x_{jm}^{\varepsilon_{jm}}$ — два формально различных конъюнкта над множеством переменных $\{x_1, \ldots, x_n\}$. Покажем, что функции

$$f(x_1, \ldots, x_n) = x_{i_1}^{\sigma_{i_1}} x_{i_2}^{\sigma_{i_2}} \ldots x_{i_k}^{\sigma_{i_k}} \quad \text{и} \quad g(x_1, \ldots, x_n) = x_{j_1}^{\varepsilon_{j1}} x_{j2}^{\varepsilon_{j2}} \ldots x_{jm}^{\varepsilon_{jm}}$$

являются различными булевыми функциями. Для этого заметим, что их характеристические множества равны

$$\begin{aligned} N_f =& \{\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{B}^n \;:\; \alpha_{i_1} = \sigma_{i_1}, \alpha_{i_2} = \sigma_{i_2}, \ldots, \alpha_{i_k} = \sigma_{i_k}\}, \\ N_g =& \{\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{B}^n \;:\; \alpha_{j_1} = \varepsilon_{j_1}, \alpha_{j_2} = \varepsilon_{j2}, \ldots, \alpha_{jm} = \varepsilon_{jm}\}, \end{aligned}$$

а так как по условию $\{x_{i_1}^{\sigma_{i_1}}, x_{i_2}^{\sigma_{i_2}}, \ldots, x_{i_k}^{\sigma_{i_k}}\} \neq \{x_{j_1}^{\varepsilon_{j_1}}, x_{j_2}^{\varepsilon_{j_2}}, \ldots, x_{j_m}^{\varepsilon_{j_m}}\}$, то

$$\{(i_1, \sigma_{i_1}), (i_2, \sigma_{i_2}), \ldots, (i_k, \sigma_{i_k})\} \neq \{(j_1, \varepsilon_{j_1}), (j_2, \varepsilon_{j_2}), \ldots, (j_m, \varepsilon_{j_m})\}.$$

Значит, n-мерные наборы

$$(\ldots, \sigma_{i_1}, \ldots, \sigma_{i_2}, \ldots, \sigma_{i_k}, \ldots) \text{ и } (\ldots, \varepsilon_{j_1}, \ldots, \varepsilon_{j_2}, \ldots, \varepsilon_{j_m}, \ldots)$$

не равны. Отсюда, $N_f \neq N_g$ и, следовательно, $f(x_1, \ldots, x_n) \neq g(x_1, \ldots, x_n)$.

2. Допустим, что две различные СДНФ

$$K_1 \vee K_2 \vee \ldots \vee K_s \text{ и } K_1' \vee K_2' \vee \ldots \vee K_t'$$

над множеством переменных $\{x_1, \ldots, x_n\}$ задают одну и ту же булеву функцию f:

$$f(x_1, \ldots, x_n) = K_1 \vee K_2 \vee \ldots \vee K_s = K_1' \vee K_2' \vee \ldots \vee K_t'.$$

Формальное различие двух данных СДНФ означает, что найдется полный конъюнкт, который является членом одной из этих СДНФ, но не является членом другой СДНФ. Пусть для определенности K_i входит в $K_1 \vee K_2 \vee \ldots \vee K_s$, но не входит в $K_1' \vee K_2' \vee \ldots \vee K_t'$. Умножая обе части равенства

$$K_1 \vee K_2 \vee \ldots \vee K_s = K_1' \vee K_2' \vee \ldots \vee K_t'$$

на K_i с учетом «ортогональности» полных конъюнктов (см. лемма 3.1), получим тождественное равенство

$$K_i = \mathbf{0}.$$

Это противоречие доказывает, что две формально различные СДНФ определяют разные булевы функции.

3. Предварительно введем обозначение и приведем несколько простых фактов.

- Положим $\tilde{\alpha}_0 = (\mathbf{0}, \dots, \mathbf{0})$ и $\tilde{\alpha}_{i_1 \dots i_k} = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{B}^n$, где

$$\alpha_i = \begin{cases} \mathbf{1}, & \text{если } i \in \{i_1, \dots, i_k\}; \\ \mathbf{0}, & \text{если } i \notin \{i_1, \dots, i_k\}. \end{cases}$$

- $\tilde{\alpha} \prec \tilde{\alpha}_{i_1 \dots i_k} \iff \tilde{\alpha} = \tilde{\alpha}_{j_1 \dots j_m}$, где $\{j_1, \dots, j_m\}$ — собственное подмножество множества $\{i_1, \dots, i_k\}$.
- Напомним, что через $\rho(\tilde{\alpha})$ мы обозначили ранговую функцию решетки $\mathbb{B}^n$, равную числу единичных компонент n-набора $\tilde{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_n)$. Значит $\rho(\tilde{\alpha}) = k$ тогда и только тогда, когда $\tilde{\alpha} = \tilde{\alpha}_{i_1 \dots i_k}$ для некоторого k-подмножества $\{i_1, \dots, i_k\}$ множества $\{1, 2, \dots, n\}$.
- $A \oplus x = A \oplus y \iff x = y$.
- Пусть булева функция $f(x_1, \dots, x_n)$ задана в виде полинома Жегалкина

$$f = c_0 \oplus c_1 x_1 \oplus \dots \oplus c_{i_1 i_2 \dots i_k} x_{i_1} x_{i_2} \cdots x_{i_k} \oplus \dots \oplus c_{12 \dots n} x_1 x_2 \cdots x_n,$$

  где каждое из $c_0, c_1, \dots, c_{i_1 i_2 \dots i_k}, \dots, c_{12 \dots n}$ равно $\mathbf{0}$ или $\mathbf{1}$. Тогда индукцией по рангу $\rho(\tilde{\alpha})$ элемента $\tilde{\alpha}$ нетрудно установить, что

$$f(\tilde{\alpha}_{i_1 \dots i_k}) = \left(\bigoplus_{\tilde{\alpha} \prec \tilde{\alpha}_{i_1 \dots i_k}} f(\tilde{\alpha}) \right) \oplus c_{i_1 i_2 \dots i_k}.$$

После приведенных приготовлений приступим непосредственно к доказательству утверждения 3 нашей леммы. Для того чтобы показать, что два формально различных полинома Жегалкина определяют две различные булевы функции, достаточно показать, что булева функция f не может быть представлена в виде двух формально различных полиномов Жегалкина. Пусть

$$\begin{gathered} f(x_1,\ldots,x_n) = \\ = a_0 \oplus a_1x_1 \oplus \ldots \oplus a_{i_1i_2\ldots i_k}x_{i_1}x_{i_2}\cdots x_{i_k} \oplus \ldots \oplus a_{12\ldots n}x_1x_2\cdots x_n = \\ = b_0 \oplus b_1x_1 \oplus \ldots \oplus b_{i_1i_2\ldots i_k}x_{i_1}x_{i_2}\cdots x_{i_k} \oplus \ldots \oplus b_{12\ldots n}x_1x_2\cdots x_n. \end{gathered}$$

Наша цель — показать, что справедливы равенства

$$a_0 = b_0, a_1 = b_1, \ldots, a_{i_1i_2\ldots i_k} = b_{i_1i_2\ldots i_k}, \ldots, a_{12\ldots n} = b_{12\ldots n}.$$

Вычисляя значение функции f на наборах вида $\tilde{\alpha}_{i_1\ldots i_k}$, получаем

$$f(\tilde{\alpha}_{i_1\ldots i_k}) = \left(\bigoplus_{\tilde{\alpha}\prec\tilde{\alpha}_{i_1\ldots i_k}} f(\tilde{\alpha})\right) \oplus a_{i_1i_2\ldots i_k} = \left(\bigoplus_{\tilde{\alpha}\prec\tilde{\alpha}_{i_1\ldots i_k}} f(\tilde{\alpha})\right) \oplus b_{i_1i_2\ldots i_k}.$$

Отсюда, с учетом того, что из $A \oplus x = A \oplus y$ следует $x = y$, получаем сразу, что $a_{i_1i_2\ldots i_k} = b_{i_1i_2\ldots i_k}$. Что и требовалось доказать. ►

3.2. Дизъюнктивная и конъюнктивная нормальные формы

Мы уже анонсировали тот факт, что произвольную булеву функцию можно задать с помощью обобщенных булевых выражений, причем многими способами. В следующих пунктах мы докажем это. В этом же пункте мы укажем, как для данного обобщенного булева выражения путем эквивалентных преобразований построить ее ДНФ и КНФ. Эти формы представления булевых выражений (булевых функций) являются важнейшими как для теории булевых функций, так и для различных ее приложений.

Итак, пусть $\mathcal{A}$ — произвольное обобщенное булево выражение. Тогда можно предложить следующий алгоритм получения ДНФ выражения $\mathcal{A}$ с помощью эквивалентных преобразований.

Алгоритм получения ДНФ:

1 шаг: Выразить «производные» булевы операции $\oplus, \to, \leftrightarrow, |, \downarrow$, $-, \overset{*}{\to}, \overset{*}{-}$ через операции $\neg, \vee, \wedge$, используя равенства:

$$\begin{aligned} A \oplus B &= A\bar{B} \vee \bar{A}B, & A \downarrow B &= \bar{A}\bar{B},\\ A \to B &= \bar{A} \vee B, & A - B &= A\bar{B},\\ A \leftrightarrow B &= AB \vee \bar{A}\bar{B}, & A \overset{*}{\to} B &= \bar{A}B,\\ A \,|\, B &= \bar{A} \vee \bar{B}, & A \overset{*}{-} B &= A \vee \bar{B}. \end{aligned}$$

2 шаг: Пользуясь законами

$$\begin{aligned} \bar{\bar{A}} &= A, && (\textit{закон двойного отрицания})\\ \overline{A \vee B} &= \bar{A}\bar{B}, && (\textit{закон Де Моргана}),\\ \overline{AB} &= \bar{A} \vee \bar{B}, && (\textit{закон Де Моргана}), \end{aligned}$$

перейти к выражению с тесным отрицанием, т. е. к такому булевому выражению, в котором знаки отрицания относятся только к переменным.

3 шаг: Пользуясь законом дистрибутивности конъюнкции по отношению к дизъюнкции

$$A \cdot (B \vee C) = A \cdot B \vee A \cdot C,$$

раскрыть все скобки.

4 шаг: Пользуясь законами

$$\begin{aligned} A \cdot A &= A, && (\textit{идемпотентность конъюнкции}) \\ A \vee A &= A, && (\textit{идемпотентность дизъюнкции}) \\ A \cdot \bar{A} &= \mathbf{0}, && (\textit{закон противоречия}) \\ A \vee \bar{A} &= \mathbf{1}, && (\textit{закон исключенного третьего}), \end{aligned}$$

удалить лишние конъюнкции и лишние переменные.

5 шаг: Избавиться от констант **0** и **1**, применяя правила

$$\begin{aligned} \mathbf{0} \vee A &= A, & \mathbf{1} \vee A &= \mathbf{1}, \\ \mathbf{0} \cdot A &= \mathbf{0}, & \mathbf{1} \cdot A &= A. \end{aligned}$$

Этот же алгоритм можно предложить и для приведения обобщенного булева выражения $\mathcal{A}$ к КНФ. Единственное отличие состоит в том, что на 3 шаге нужно использовать закон дистрибутивности дизъюнкции по отношению к конъюнкции:

$$A \vee B \cdot C = (A \vee B) \cdot (A \vee C).$$

Замечание 3.1. Следуя изложенным алгоритмам, всегда можно привести данное обобщенное булево выражение к ДНФ и КНФ — в этом их основная ценность. Однако в реальных вычислениях не обязательно точно следовать всем шагам алгоритма: если вы видите более короткий путь — следуйте ему!

Пример 5. Привести булево выражение $\overline{(x_1\bar{x}_2 \vee x_3)} \to (x_1 \oplus x_2\bar{x}_4)$ к ДНФ.

Решение. Для решения поставленной задачи воспользуемся предложенным выше алгоритмом.

$$\begin{gathered}
\text{(1 шаг)}\\
\overline{(x_1\bar{x}_2 \vee x_3)} \to (x_1 \oplus x_2\bar{x}_4) =\\
= \overline{\overline{(x_1\bar{x}_2 \vee x_3)}} \vee (x_1 \oplus x_2\bar{x}_4) = \overline{\overline{(x_1\bar{x}_2 \vee x_3)}} \vee (\bar{x}_1 x_2 \bar{x}_2 \vee x_1\overline{x_2\bar{x}_4}) =\\
\text{(2 шаг)}\\
= (x_1\bar{x}_2 \vee x_3) \vee (\bar{x}_1 x_2 \bar{x}_4 \vee x_1(\bar{x}_2 \vee \bar{\bar{x}}_4)) = x_1\bar{x}_2 \vee x_3 \vee \bar{x}_1 x_2 \bar{x}_4 \vee x_1(\bar{x}_2 \vee x_4) =\\
\text{(3 шаг)}\\
= x_1\bar{x}_2 \vee x_3 \vee \bar{x}_1 x_2 \bar{x}_4 \vee x_1\bar{x}_2 \vee x_1 x_4 =\\
\text{(4 шаг)}\\
= x_1\bar{x}_2 \vee x_3 \vee \bar{x}_1 x_2 \bar{x}_4 \vee x_1 x_4.
\end{gathered}$$

Таким образом, одна из дизъюнктивных нормальных форм нашего выражения равна $x_1\bar{x}_2 \vee x_3 \vee \bar{x}_1 x_2 \bar{x}_4 \vee x_1 x_4$. ►

Пример 6. Привести булево выражение $(x_1 \to x_2) \oplus (x_3 \to x_4)$ к КНФ.

Решение. Сначала выразим все встречающиеся в этом выражении операции через $\neg, \vee$ и $\wedge$:

$$\begin{gathered}(x_1 \to x_2) \oplus (x_3 \to x_4) = (x_1 \to x_2)\overline{(x_3 \to x_4)} \vee \overline{(x_1 \to x_2)}(x_3 \to x_4) = \\ = (\bar{x}_1 \vee x_2)\overline{(\bar{x}_3 \vee x_4)} \vee \overline{(\bar{x}_1 \vee x_2)}(\bar{x}_3 \to x_4)\end{gathered}$$

Воспользуемся теперь дистрибутивностью операции дизъюнкции относительно конъюнкции, точнее следующим следствием этой дистрибутивности:

$$AB \vee CD = (A \vee C) \cdot (A \vee D) \cdot (B \vee C) \cdot (B \vee D).$$

Используя это равенство, а также равенства $A \vee \overline{A} = \mathbf{1}$, $A \cdot \mathbf{1} = A$, получаем:

$$\begin{gathered}\underbrace{(\bar{x}_1 \vee x_2)}_{A}\underbrace{\overline{(\bar{x}_3 \vee x_4)}}_{B} \vee \underbrace{\overline{(\bar{x}_1 \vee x_2)}}_{C}\underbrace{(\bar{x}_3 \to x_4)}_{D} = \\ = \big((\bar{x}_1 \vee x_2) \vee \overline{(\bar{x}_1 \vee x_2)}\big) \cdot \big((\bar{x}_1 \vee x_2) \vee (\bar{x}_3 \vee x_4)\big) \cdot \\ \big(\overline{(\bar{x}_3 \vee x_4)} \vee \overline{(\bar{x}_1 \vee x_2)}\big) \cdot \big(\overline{(\bar{x}_3 \vee x_4)} \vee (\bar{x}_3 \vee x_4)\big) = \\ = \mathbf{1} \cdot \big((\bar{x}_1 \vee x_2) \vee (\bar{x}_3 \vee x_4)\big) \cdot \big(\overline{(\bar{x}_3 \vee x_4)} \vee \overline{(\bar{x}_1 \vee x_2)}\big) \cdot \mathbf{1} = \\ = \big(\bar{x}_1 \vee x_2 \vee \bar{x}_3 \vee x_4\big) \cdot \big(\overline{(\bar{x}_3 \vee x_4)} \vee \overline{(\bar{x}_1 \vee x_2)}\big).\end{gathered}$$

Далее используем законы Де Моргана, закон двойного отрицания и еще раз дистрибутивность:

$$
\begin{gathered}
(\bar{x}_1 \vee x_2 \vee \bar{x}_3 \vee x_4) \cdot \big(\overline{(\bar{x}_1 \vee x_2)} \vee \overline{(\bar{x}_3 \vee x_4)}\big) = \\
= (\bar{x}_1 \vee x_2 \vee \bar{x}_3 \vee x_4) \cdot (x_1 \bar{x}_2 \vee x_3 \bar{x}_4) = \\
= (\bar{x}_1 \vee x_2 \vee \bar{x}_3 \vee x_4) \cdot (x_1 \vee x_3) \cdot (x_1 \vee \bar{x}_4) \cdot (\bar{x}_2 \vee x_3) \cdot (\bar{x}_2 \vee \bar{x}_4).
\end{gathered}
$$

Таким образом, мы получили следующее представление нашего булевого выражения в виде ДНФ:

$$
(x_1 \to x_2) \oplus (x_3 \to x_4) = (\bar{x}_1 \vee x_2 \vee \bar{x}_3 \vee x_4) \cdot (x_1 \vee x_3) \cdot (x_1 \vee \bar{x}_4) \cdot (\bar{x}_2 \vee x_3) \cdot (\bar{x}_2 \vee \bar{x}_4).
$$

Задача решена. ►

3.3. Совершенная дизъюнктивная и совершенная конъюнктивная нормальные формы

Следующая теорема является очень важной теоремой теории булевых функций.

Теорема 3.1 (Разложения функции по переменным.). *Для любой булевой функции $f(x_1, \dots, x_n)$ и для любого k, $1 \leqslant k \leqslant n$, справедливы следующие разложения:*

$$
f = \bigvee_{(\sigma_1, \dots, \sigma_k) \in \mathbb{B}^k} x_1^{\sigma_1} \dots x_k^{\sigma_k} \cdot f(\sigma_1, \dots, \sigma_k, x_{k+1}, \dots, x_n), \tag{3.1}
$$

$$
f = \bigwedge_{(\sigma_1, \dots, \sigma_k) \in \mathbb{B}^k} x_1^{\bar{\sigma}_1} \vee \dots \vee x_k^{\bar{\sigma}_k} \vee f(\sigma_1, \dots, \sigma_k, x_{k+1}, \dots, x_n). \tag{3.2}
$$

◀ Покажем, что правые и левые части приведенных выше равенств принимают одинаковые значения на одних и тех же наборах значений переменных.

Доказательство равенства 3.1. Подставим произвольный набор $\tilde{\varepsilon} = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$ в правую часть:

$$\bigvee_{(\sigma_1,\sigma_2,\ldots,\sigma_k)\in\mathbb{B}^k} \varepsilon_1^{\sigma_1} \cdot \varepsilon_2^{\sigma_2} \cdot \ldots \cdot \varepsilon_k^{\sigma_k} \cdot f(\sigma_1, \sigma_2, \ldots, \sigma_k, \varepsilon_{k+1}, \ldots, \varepsilon_n).$$

Далее, вспоминая, что

$$\varepsilon^{\sigma} = \begin{cases} \mathbf{1}, & \text{если } \ \varepsilon = \sigma; \\ \mathbf{0}, & \text{если } \ \varepsilon \neq \sigma \end{cases}$$

и учитывая, что произведение равно нулю, если хотя бы один из сомножителей равен нулю, получим, что правая часть равна

$$\varepsilon_1^{\varepsilon_1} \cdot \varepsilon_2^{\varepsilon_2} \cdot \ldots \cdot \varepsilon_k^{\varepsilon_k} \cdot f(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k, \varepsilon_{k+1}, \ldots, \varepsilon_n) = f(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k, \varepsilon_{k+1}, \ldots, \varepsilon_n).$$

Доказательство равенства 3.2. Конечно, можно сказать, что доказательство этого равенства аналогично. Однако, чтобы воочию увидеть эту аналогию, приведем и его. Подставим произвольный набор $\tilde{\varepsilon} = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$ в правую часть:

$$\bigwedge_{(\sigma_1,\sigma_2,\ldots,\sigma_k)\in\mathbb{B}^k} \varepsilon_1^{\bar{\sigma}_1} \vee \varepsilon_2^{\bar{\sigma}_2} \vee \ldots \vee \varepsilon_k^{\bar{\sigma}_k} \vee f(\sigma_1, \sigma_2, \ldots, \sigma_k, \varepsilon_{k+1}, \ldots, \varepsilon_n).$$

Далее, учитывая, что

$$\varepsilon^{\bar{\sigma}} = \begin{cases} \mathbf{1}, & \text{если } \ \sigma = \bar{\varepsilon}; \\ \mathbf{0}, & \text{если } \ \sigma = \varepsilon, \end{cases} \quad \text{и} \quad \bar{\bar{\varepsilon}} = \varepsilon,$$

а также, учитывая, что булева сумма равна единице, если хотя бы одно из слагаемых равно единице, получим, что правая часть равна

$$\varepsilon_1^{\bar{\varepsilon}_1} \vee \varepsilon_2^{\bar{\varepsilon}_2} \vee \ldots \vee \varepsilon_k^{\bar{\varepsilon}_k} \vee f(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k, \varepsilon_{k+1}, \ldots, \varepsilon_n) = f(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k, \varepsilon_{k+1}, \ldots, \varepsilon_n).$$

Теорема доказана. ►

Чтобы как-то ссылаться на эти равенства мы будем называть равенство (3.1) *аддитивным разложением*, а равенство (3.2) — *мультипликативным разложением* функции f по переменным $x_1, \ldots, x_k$. В доказанной теореме, конечно-же, не существенно, что мы разлагаем функцию по подряд идущим переменным $x_1, \ldots, x_k$ — можно разлагать по любой группе переменных $x_{i_1}, \ldots, x_{i_k}$.

Пример 7. Пусть $f(x_1, x_2, x_3)$ — данная булева функция. Вот как выглядят расписанные разложения этой функции:

$$\begin{gathered}
(\textit{аддитивное разложение по } \ x_1, x_2): \\
f(x_1, x_2, x_3) = \\
= x_1 x_2 \cdot f(\mathbf{1}, \mathbf{1}, x_3) \vee x_1 \bar{x}_2 \cdot f(\mathbf{1}, \mathbf{0}, x_3) \vee \bar{x}_1 x_2 \cdot f(\mathbf{0}, \mathbf{1}, x_3) \vee \bar{x}_1 \bar{x}_2 f \cdot (\mathbf{0}, \mathbf{0}, x_3) \\
(\textit{мультипликативное разложение по } \ x_2, x_3): \\
f(x_1, x_2, x_3) = \\
= \big(\bar{x}_2 \vee \bar{x}_3 \vee f(x_1, \mathbf{1}, \mathbf{1})\big) \cdot \big(\bar{x}_2 \vee x_3 \vee f(x_1, \mathbf{1}, \mathbf{0})\big) \cdot \big(x_2 \vee \bar{x}_3 \vee f(x_1, \mathbf{0}, \mathbf{1})\big) \cdot \\
\cdot \big(x_2 \vee x_3 \vee f \cdot (x_1, \mathbf{0}, \mathbf{0})\big)
\end{gathered}$$

Полагая в вышеприведенной теореме $k = 1$, получим следующее следствие.

Следствие 3.1. Разложения функции по одной переменной. *Для любой булевой функции* $f(x_1, x_2, \dots, x_n)$ *справедливы равенства*

$$\begin{aligned} f(x_1, x_2, \dots, x_n) &= \bar{x}_1 \cdot f(\mathbf{0}, x_2, \dots, x_n) \vee x_1 \cdot f(\mathbf{1}, x_2, \dots, x_n), \\ f(x_1, x_2, \dots, x_n) &= \big(x_1 \vee f(\mathbf{0}, x_2, \dots, x_n)\big) \cdot \big(\bar{x}_1 \vee f(\mathbf{1}, x_2, \dots, x_n)\big). \end{aligned}$$

Следующая теорема, безусловно, является одной из центральных теорем теории булевых функций.

Теорема 3.2 (О совершенных нормальных формах). *Справедливы следующие утверждения:*

(СДН-форма): *Если* $f(x_1, x_2, \dots, x_n)$ *отлична от тождественного нуля, то справедливо представление:*

$$f(x_1, x_2, \dots, x_n) = \bigvee_{\substack{(\sigma_1, \sigma_2, \dots, \sigma_n) \in \mathbb{B}^n: \\ f(\sigma_1, \sigma_2, \dots, \sigma_n) = \mathbf{1}}} x_1^{\sigma_1} x_2^{\sigma_2} \cdots x_n^{\sigma_n}, \tag{3.3}$$

причем это представление единственно с точностью до следования конъюнктов.

(СКН-форма): *Если* $f(x_1, x_2, \dots, x_n)$ *отлична от тождественной единицы, то справедливо представление:*

$$f(x_1, x_2, \dots, x_n) = \bigwedge_{\substack{(\sigma_1, \sigma_2, \dots, \sigma_n) \in \mathbb{B}^n: \\ f(\sigma_1, \sigma_2, \dots, \sigma_n) = \mathbf{0}}} x_1^{\bar{\sigma}_1} \vee x_2^{\bar{\sigma}_2} \vee \cdots \vee x_n^{\bar{\sigma}_n}, \tag{3.4}$$

причем это представление единственно с точностью до следования дизъюнктов.

◀ <u>СДН-форма.</u> Пусть функция $f(x_1, x_2, \ldots, x_n)$ отлична от тождественного нуля. Применим теорему о разложении булевой функции по переменным при $k = n$:

$$f(x_1, x_2, \ldots, x_n) = \bigvee_{(\sigma_1, \sigma_2, \ldots, \sigma_n) \in \mathbb{B}^n} x_1^{\sigma_1} x_2^{\sigma_2} \cdots x_n^{\sigma_n} \cdot f(\sigma_1, \sigma_2, \ldots, \sigma_n),$$

что можно переписать в эквивалентном виде

$$\left(\bigvee_{\substack{(\sigma_1, \ldots, \sigma_n) \in \mathbb{B}^n : \\ f(\sigma_1, \ldots, \sigma_n) = \mathbf{1}}} x_1^{\sigma_1} \cdots x_n^{\sigma_n} \cdot f(\sigma_1, \ldots, \sigma_n) \right) \vee \left(\bigvee_{\substack{(\sigma_1, \ldots, \sigma_n) \in \mathbb{B}^n : \\ f(\sigma_1, \ldots, \sigma_n) = \mathbf{0}}} x_1^{\sigma_1} \cdots x_n^{\sigma_n} \cdot f(\sigma_1, \ldots, \sigma_n) \right).$$

Учитывая, что в первой скобке все значения функции равны единице, а во второй нулю (и, значит, вся вторая скобка имеет значение нуль), получаем требуемое равенство.

Единственность следует из того, что две формально различные СДН формы задают различные булевы функции (см. лемма 3.3 на стр. 68).

<u>СКН-форма.</u> И вновь, при доказательстве существования и единственности СКН-формы можно сослаться на аналогию с СДН-формой. Однако здесь мы приведем другое доказательство, основанное на принципе двойственности, чтобы продемонстрировать этот полезный прием. Пусть $f(x_1, \ldots, x_n)$ — произвольная булева функция, отличная от тождественной единицы. Тогда двойственная ей функция $g(x_1, \ldots, x_n) = f^*(x_1, \ldots, x_n)$ отлична от тождественно нулевой функции. Согласно теореме о СДН-форме она имеет единственное представление вида

$$g(x_1, x_2, \ldots, x_n) = \bigvee_{\substack{(\sigma_1, \sigma_2, \ldots, \sigma_n) \in \mathbb{B}^n : \\ g(\sigma_1, \sigma_2, \ldots, \sigma_n) = \mathbf{1}}} x_1^{\sigma_1} x_2^{\sigma_2} \cdots x_n^{\sigma_n},$$

Тогда, ввиду того, что $f(x_1,\dots,x_n)=g^*(x_1,\dots,x_n)=\overline{g(\bar{x}_1,\dots,\bar{x}_n)}$, получаем

$$f(x_1,\dots,x_n)=\overline{g(\bar{x}_1,\dots,\bar{x}_n)}=\overline{\bigvee_{\substack{(\sigma_1,\sigma_2,\dots,\sigma_n)\in\mathbb{B}^n:\\ g(\sigma_1,\sigma_2,\dots,\sigma_n)=\mathbf{1}}}\overline{x_1^{\sigma_1}}\cdots\overline{x_n^{\sigma_n}}}=$$

$$=\bigwedge_{\substack{(\sigma_1,\sigma_2,\dots,\sigma_n)\in\mathbb{B}^n:\\ g(\sigma_1,\sigma_2,\dots,\sigma_n)=\mathbf{1}}}\overline{\overline{x_1^{\sigma_1}}}\vee\dots\vee\overline{\overline{x_n^{\sigma_n}}}=\bigwedge_{\substack{(\sigma_1,\sigma_2,\dots,\sigma_n)\in\mathbb{B}^n:\\ g(\sigma_1,\sigma_2,\dots,\sigma_n)=\mathbf{1}}}x_1^{\sigma_1}\vee\dots\vee x_n^{\sigma_n}=$$

$$=\bigwedge_{\substack{(\sigma_1,\sigma_2,\dots,\sigma_n)\in\mathbb{B}^n:\\ g(\bar\sigma_1,\bar\sigma_2,\dots,\bar\sigma_n)=\mathbf{1}}}x_1^{\bar\sigma_1}\vee\dots\vee x_n^{\bar\sigma_n}=\bigwedge_{\substack{(\sigma_1,\sigma_2,\dots,\sigma_n)\in\mathbb{B}^n:\\ \overline{g(\bar\sigma_1,\bar\sigma_2,\dots,\bar\sigma_n)}=\mathbf{0}}}x_1^{\bar\sigma_1}\vee\dots\vee x_n^{\bar\sigma_n}=$$

$$=\bigwedge_{\substack{(\sigma_1,\sigma_2,\dots,\sigma_n)\in\mathbb{B}^n:\\ f(\sigma_1,\sigma_2,\dots,\sigma_n)=\mathbf{0}}}x_1^{\bar\sigma_1}\vee x_2^{\bar\sigma_2}\vee\dots\vee x_n^{\bar\sigma_n}$$

Теорема полностью доказана. ▶

Пусть

$$f(x_1,\dots,x_n)=K_1\vee\ldots\vee K_s \quad\text{и}\quad f(x_1,\dots,x_n)=D_1\wedge\ldots\wedge D_t$$

СДНФ и СКНФ булевой функции; напомним, что число s мы назвали длиной СДНФ, а t — длиной СКНФ для f. Из формул для СДНФ и СКНФ непосредственно можно извлечь следующие полезные наблюдения:

длина СДН-формы булевой функции f равна мощности его характеристического множества N_f: $s=|N_f|$;

длина СКН-формы булевой функции f равна мощности дополнения его характеристического множества N_f: $t = |\overline{N}_f|$.

Теорема о нормальных формах является конструктивной в том смысле, что сами равенства (3.3) и (3.4) диктуют нам метод приведения данной булевой функции к СДНФ и СКНФ. Для применения этого метода нам необходимо знание значений $f(\alpha_1, \ldots, \alpha_n)$ функции f на всех наборах $(\alpha_1, \ldots, \alpha_n) \in \mathbb{B}^n$. Поэтому этот метод хорош в случаях, когда функция задана таблицей своих значений, в виде слова, с помощью характеристического множества или таблицы Вейча. Если же булева функция задана в виде обобщенного булева выражения с числом переменных $n \geqslant 4$ «вручную» вычислять 2^n значений функции f оказывается утомительным занятием. Поэтому для приведения булевой функции f, заданной с помощью обобщенного булева выражения, к совершенным нормальным формам на практике чаще используют *метод эквивалентных преобразований*: *сначала булеву функцию приводят к ДНФ (соотв. КНФ), а затем, используя равенство $\mathbf{1} = x_i \vee \bar{x}_i$ (соотв. $\mathbf{0} = x_i \cdot \bar{x}_i$), доводят эту ДНФ до СДНФ (соотв. доводят КНФ до СКНФ).*

Пример 8. Привести булеву функцию

$$f(x_1, \ldots, x_n) = (x_1 \vee \bar{x}_2) \to (x_1 \oplus x_3)$$

к СДНФ и СКНФ.

Решение. Ввиду того, что наша функция является функцией 3-х переменных, недолго вычислить ее таблицу значений. Поэтому мы решим эту задачу двумя способами.

1 способ. Здесь мы найдем совершенные формы нашей булевой функции методом, основанным на формулах (3.3), (3.4) и таблице значений функции . Все вычисления удобно организовать в виде следующей таблицы, где, кроме колонки значений нашей функции выделены еще колонки СДНФ и СКНФ. В эти колонки мы выписываем те полные конъюнкты (колонка СДНФ) и полные дизъюнкты (колонка СКНФ), которые входят в соответствующие совершенные формы.

x_1	x_2	x_3	$(x_1 \vee \bar{x}_2) \to (x_1 \oplus x_3)$	СДНФ	СКНФ
0	**0**	**0**	**0**		✓ $x_1 \vee x_2 \vee x_3$
0	**0**	**1**	**1**	✓ $\bar{x}_1\bar{x}_2x_3$	
0	**1**	**0**	**1**	✓ $\bar{x}_1x_2\bar{x}_3$	
0	**1**	**1**	**1**	✓ $\bar{x}_1x_2x_3$	
1	**0**	**0**	**1**	✓ $x_1\bar{x}_2\bar{x}_3$	
1	**0**	**1**	**0**		✓ $\bar{x}_1 \vee x_2 \vee \bar{x}_3$
1	**1**	**0**	**1**	✓ $x_1x_2\bar{x}_3$	
1	**1**	**1**	**0**		✓ $\bar{x}_1 \vee \bar{x}_2 \vee \bar{x}_3$

Из данных этой таблицы сразу получаем:

$$\text{СДНФ:}\quad (x_1 \vee \bar{x}_2) \to (x_1 \oplus x_3) = \bar{x}_1\bar{x}_2x_3 \vee \bar{x}_1x_2\bar{x}_3 \vee \bar{x}_1x_2x_3 \vee x_1\bar{x}_2\bar{x}_3 \vee x_1x_2\bar{x}_3,$$
$$\text{СКНФ:}\quad (x_1 \vee \bar{x}_2) \to (x_1 \oplus x_3) = \big(x_1 \vee x_2 \vee x_3\big) \cdot \big(\bar{x}_1 \vee x_2 \vee \bar{x}_3\big) \cdot \big(\bar{x}_1 \vee \bar{x}_2 \vee \bar{x}_3\big).$$

2 способ. (СДНФ) Сначала приведем наше булево выражение к ДНФ. Будем руководствоваться при этом алгоритмом, изложенном на стр. 72. В данном случае, используя равенства

$$A \to B = \overline{A} \vee B, \quad A \oplus B = \overline{A} \cdot B \vee A \cdot \overline{B}, \quad \overline{A \vee B} = \overline{A} \cdot \overline{B}, \quad \overline{\overline{A}} = A,$$

получаем

$$(x_1 \vee \bar{x}_2) \to (x_1 \oplus x_3) = \overline{(x_1 \vee \bar{x}_2)} \vee (x_1 \oplus x_3) =$$
$$= \overline{(x_1 \vee \bar{x}_2)} \vee (\bar{x}_1 x_3 \vee x_1 \bar{x}_3) = \bar{x}_1 x_2 \vee \bar{x}_1 x_3 \vee x_1 \bar{x}_3.$$

Далее, пользуясь равенством $\mathbf{1} = x \vee \bar{x}$, дистрибутивным законом $A \cdot (B \vee C) = AB \vee AC$ и равенством $A \vee A = A$, доведем полученную ДНФ до СДНФ:

$$(x_1 \vee \bar{x}_2) \to (x_1 \oplus x_3) = \bar{x}_1 x_2 \vee \bar{x}_1 x_3 \vee x_1 \bar{x}_3 = \bar{x}_1 x_2 \mathbf{1} \vee \bar{x}_1 \mathbf{1} x_3 \vee x_1 \mathbf{1} \bar{x}_3 =$$
$$= \bar{x}_1 x_2 (x_3 \vee \bar{x}_3) \vee \bar{x}_1 (x_2 \vee \bar{x}_2) x_3 \vee x_1 (x_2 \vee \bar{x}_2) \bar{x}_3 =$$
$$= \bar{x}_1 x_2 x_3 \vee \bar{x}_1 x_2 \bar{x}_3 \vee \bar{x}_1 x_2 x_3 \vee \bar{x}_1 \bar{x}_2 x_3 \vee x_1 x_2 \bar{x}_3 \vee x_1 \bar{x}_2 \bar{x}_3 =$$
$$= \bar{x}_1 \bar{x}_2 x_3 \vee \bar{x}_1 x_2 \bar{x}_3 \vee \bar{x}_1 x_2 x_3 \vee x_1 \bar{x}_2 \bar{x}_3 \vee x_1 x_2 \bar{x}_3.$$

Таким образом, получаем

$$\text{СДНФ:} \quad (x_1 \vee \bar{x}_2) \to (x_1 \oplus x_3) = \bar{x}_1 \bar{x}_2 x_3 \vee \bar{x}_1 x_2 \bar{x}_3 \vee \bar{x}_1 x_2 x_3 \vee x_1 \bar{x}_2 \bar{x}_3 \vee x_1 x_2 \bar{x}_3.$$

Найдем теперь СКНФ. Приведем сначала наше булево выражение к КНФ. Мы воспользуемся полученным выше равенством

$$(x_1 \vee \bar{x}_2) \to (x_1 \oplus x_3) = \bar{x}_1 x_2 \vee \bar{x}_1 x_3 \vee x_1 \bar{x}_3.$$

Далее воспользуемся дистрибутивностью булевого сложения относительно булевого умножения: $A \cdot B \vee C = (A \vee C) \cdot (B \vee C)$. Ввиду некоторой психологической трудности применения этого правила (ведь обычное сложение чисел не является дистрибутивной операцией относительной умножения, т. е. для чисел не верно, что $a \cdot b + c = (a+b)\cdot(b+c)$), приведем равенство, которое следует из указанной дистрибутивности

$$\begin{gathered} AB \vee CD \vee EF = \\ = (A \vee C \vee E)\cdot(A \vee C \vee F)\cdot(A \vee D \vee E)\cdot(A \vee D \vee F)\cdot \\ (B \vee C \vee E)\cdot(B \vee C \vee F)\cdot(B \vee D \vee E)\cdot(B \vee D \vee F) \end{gathered}$$

Итак, используя это правило, а также равенства

$$A \vee A = A,\ A \vee \overline{A} = \mathbf{1},\ \mathbf{1}\cdot A = A,\ \mathbf{1} \vee A = \mathbf{1},$$

получаем (подчеркнутые сомножители равны $\mathbf{1}$):

$$\begin{gathered} (x_1 \vee \bar{x}_2) \to (x_1 \oplus x_3) = \bar{x}_1 x_2 \vee \bar{x}_1 x_3 \vee x_1 \bar{x}_3 = \\ = \underline{(\bar{x}_1 \vee \bar{x}_1 \vee x_1)}\cdot(\bar{x}_1 \vee \bar{x}_1 \vee \bar{x}_3)\cdot\underline{(\bar{x}_1 \vee x_3 \vee x_1)}\cdot\underline{(\bar{x}_1 \vee x_3 \vee \bar{x}_3)}\cdot \\ \cdot\underline{(x_2 \vee \bar{x}_1 \vee x_1)}\cdot(x_2 \vee \bar{x}_1 \vee \bar{x}_3)\cdot(x_2 \vee x_3 \vee x_1)\cdot\underline{(x_2 \vee x_3 \vee \bar{x}_3)} = \\ = (\bar{x}_1 \vee \bar{x}_3)\cdot(x_2 \vee \bar{x}_1 \vee \bar{x}_3)\cdot(x_2 \vee x_3 \vee x_1). \end{gathered}$$

Мы получили КНФ для нашей функции. Далее, пользуясь равенством $\mathbf{0} = x \cdot \bar{x}$, доводим КНФ до СКНФ:

$$\begin{gathered} (x_1 \vee \bar{x}_2) \to (x_1 \oplus x_3) = (\bar{x}_1 \vee \bar{x}_3)\cdot(\bar{x}_1 \vee x_2 \vee \bar{x}_3)\cdot(x_1 \vee x_2 \vee x_3) = \\ = (\bar{x}_1 \vee \mathbf{0} \vee \bar{x}_3)\cdot(\bar{x}_1 \vee x_2 \vee \bar{x}_3)\cdot(x_1 \vee x_2 \vee x_3) = \\ = (\bar{x}_1 \vee (x_2 \cdot \bar{x}_2) \vee \bar{x}_3)\cdot(\bar{x}_1 \vee x_2 \vee \bar{x}_3)\cdot(x_1 \vee x_2 \vee x_3) = \\ = (\bar{x}_1 \vee x_2 \vee \bar{x}_3)\cdot(\bar{x}_1 \vee \bar{x}_2 \vee \bar{x}_3)\cdot(\bar{x}_1 \vee x_2 \vee \bar{x}_3)\cdot(x_1 \vee x_2 \vee x_3) = \\ = (\bar{x}_1 \vee x_2 \vee \bar{x}_3)\cdot(\bar{x}_1 \vee \bar{x}_2 \vee \bar{x}_3)\cdot(\bar{x}_1 \vee x_2 \vee \bar{x}_3)\cdot(x_1 \vee x_2 \vee x_3) = \\ = (\bar{x}_1 \vee \bar{x}_2 \vee \bar{x}_3)\cdot(\bar{x}_1 \vee x_2 \vee \bar{x}_3)\cdot(x_1 \vee x_2 \vee x_3). \end{gathered}$$

Таким образом, получаем

$$\text{СКНФ:}\quad (x_1 \vee \bar{x}_2) \to (x_1 \oplus x_3) = (x_1 \vee x_2 \vee x_3) \cdot (\bar{x}_1 \vee x_2 \vee \bar{x}_3) \cdot (\bar{x}_1 \vee \bar{x}_2 \vee \bar{x}_3).$$

Задача решена. ►

3.4. Полином и кополином Жегалкина

Теорема 3.3. *Каждая булева функция $f(x_1, \ldots, x_n) \in \mathbb{BF}(n)$ единственным образом представима в виде полинома Жегалкина по переменным $x_1, \ldots, x_n$.*

◄ По утверждению 3 леммы 3.3 два формально различных полинома Жегалкина порождают две разные булевы функции; по утверждению же 5 леммы 3.2 число формально различных полиномов Жегалкина над множеством переменных $\{x_1, \ldots, x_n\}$ равно 2^{2^n}. Но ведь число всех булевых функций от переменных $x_1, \ldots, x_n$ также равно 2^{2^n}. Значит, каждой булевой функции $f(x_1, \ldots, x_n) \in \mathbb{BF}(n)$ должен соответствовать ровно один реализующий ее полином Жегалкина. ►

Доказательство этой теоремы является неконструктивным. Для практической реализации данной булевой функции $f \in \mathbb{BF}$ в виде полинома Жегалкина можно предложить следующий алгоритм.

Алгоритм построения полинома Жегалкина:

1 шаг: Если функция задана в виде обобщенного булева выражения, то пользуясь равенствами

$$\bar{x} = x \oplus \mathbf{1}, \qquad x - y = x \oplus x \cdot y,$$
$$x \vee y = x \oplus y \oplus x \cdot y, \qquad x \downarrow y = \mathbf{1} \oplus x \oplus y \oplus x \cdot y,$$
$$x \to y = \mathbf{1} \oplus x \oplus x \cdot y, \qquad x \,|\, y = \mathbf{1} \oplus x \cdot y,$$
$$x \leftrightarrow y = \mathbf{1} \oplus x \oplus y.$$

записать ее в виде обобщенного булевого выражения, построенного лишь с помощью операций $\wedge$ и $\oplus$. Если же функция задана каким-либо другим способом, то предварительно задать ее в виде булевого выражения, например, с помощью теоремы о СДНФ, а затем проделать указанные выше замены.

2 шаг: Пользуясь дистрибутивностью $x \cdot (y \oplus z) = x \cdot y \oplus x \cdot z$, раскрыть все скобки в полученном на первом шаге обобщенном булевом выражении. Получим:

$$f(x_1, \ldots, x_n) = K_1^{'} \oplus K_2^{'} \oplus \ldots \oplus K_r^{'},$$

где каждая из $K_i^{'}$ есть конъюнкция переменных и единиц.

3 шаг: Преобразуем все полученные конъюнкции $K_i^{'}$ в монотонные, пользуясь при этом коммутативностью булевого умножения и соотношениями $x \cdot x = x$, $\mathbf{1} \cdot \mathbf{1} = \mathbf{1}$ и $A \cdot \mathbf{1} = A$.

4 шаг: Преобразуем полученную сумму по модулю 2 в полином Жегалкина, пользуясь при этом соотношениями $A \oplus A = \mathbf{0}$ и $A \oplus \mathbf{0} = A$. В результате получим либо

$$f(x_1, \ldots, x_n) = K_1 \oplus K_2 \oplus \ldots \oplus K_m.$$

либо $f(x_1, \ldots, x_n) = \mathbf{0}$ или $f(x_1, \ldots, x_n) = \mathbf{1}$.

Искать полином Жегалкина для данной булевой функции можно также *методом неопределенных коэффициентов*. В следующем примере мы найдем полином Жегалкина для данной булевой функции двумя способами: руководствуясь предложенным выше алгоритмом и *методом неопределенных коэффициентов*.

Пример 9. Представить через полином Жегалкина булеву функцию $f(x_1, x_2, x_3) = (x_1 \vee x_2) \to (x_2 \vee x_3)$.

Решение. Решим поставленную задачу двумя способами.

<u>1 способ.</u> Пользуясь равенствами $a \vee b = a \oplus b \oplus a \cdot b$, $a \to b = \mathbf{1} \oplus a \oplus a \cdot b, A \cdot A = A$, имеем (подчеркнутые соответствующим количеством линий члены исчезают ввиду равенства $A \oplus A = \mathbf{0}$):

$$(x_1 \vee x_2) \to (x_2 \vee x_3) = (x_1 \oplus x_2 \oplus x_1 \cdot x_2) \to (x_2 \oplus x_3 \oplus x_2 \cdot x_3) =$$

$$= \mathbf{1} \oplus (x_1 \oplus x_2 \oplus x_1 \cdot x_2) \oplus \Big((x_1 \oplus x_2 \oplus x_1 \cdot x_2) \cdot (x_2 \oplus x_3 \oplus x_2 \cdot x_3) \Big) =$$

$$= \mathbf{1} \oplus x_1 \oplus \underline{x_2} \oplus \underline{\underline{x_1 \cdot x_2}} \oplus$$

$$\oplus \Big(\underline{\underline{x_1 \cdot x_2}} \oplus x_1 \cdot x_3 \oplus \underline{\underline{\underline{x_1 \cdot x_2 \cdot x_3}}} \oplus \underline{x_2} \oplus \underline{\underline{\underline{\underline{x_2 \cdot x_3}}}} \oplus x_2 \cdot x_3 \oplus x_1 \cdot x_2 \oplus$$

$$\oplus \underline{\underline{\underline{x_1 \cdot x_2 \cdot x_3}}} \oplus x_1 \cdot x_2 \cdot x_3 \Big) =$$

$$= \mathbf{1} \oplus x_1 \oplus x_1 \cdot x_2 \oplus x_1 \cdot x_3 \oplus x_1 \cdot x_2 \cdot x_3.$$

Таким образом, получаем следующее выражение в виде полинома Жегалкина для нашей функции:

$$(x_1 \vee x_2) \to (x_2 \vee x_3) = \mathbf{1} \oplus x_1 \oplus x_1 \cdot x_2 \oplus x_1 \cdot x_3 \oplus x_1 \cdot x_2 \cdot x_3.$$

<u>2 способ.</u> Будем искать полином Жегалкина для нашей булевой функции $f(x_1, x_2, x_3) = (x_1 \vee x_2) \to (x_2 \vee x_3)$ в виде полинома с неопределенными коэффициентами

$$a_0 \oplus a_1 \cdot x_1 \oplus a_2 \cdot x_2 \oplus a_3 \cdot x_3 \oplus a_{12} \cdot x_1 x_2 \oplus a_{13} \cdot x_1 x_3 \oplus a_{23} \cdot x_2 x_3 \oplus a_{123} \cdot x_1 x_2 x_3,$$

где коэффициенты $a_0, a_1, \ldots, a_{123}$ будем искать, подставляя конкретные значения вместо переменных.

Соберем вычисления в таблицу.

x_1	x_2	x_3	$(x_1 \vee x_2) \to (x_2 \vee x_3)$	$a_0 \oplus a_1 \cdot x_1 \oplus \ldots \oplus a_{123} \cdot x_1x_2x_3$
0	**0**	**0**	1	a_0
0	**0**	**1**	1	$a_0 \oplus a_3$
0	**1**	**0**	1	$a_0 \oplus a_3$
0	**1**	**1**	1	$a_0 \oplus a_2 \oplus a_3 \oplus a_{23}$
1	**0**	**0**	0	$a_0 \oplus a_1$
1	**0**	**1**	1	$a_0 \oplus a_1 \oplus a_3 \oplus a_{13}$
1	**1**	**0**	1	$a_0 \oplus a_1 \oplus a_2 \oplus a_{12}$
1	**1**	**1**	1	$a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_{12} \oplus a_{13} \oplus a_{23} \oplus a_{123}$

Из последней колонки этой таблицы последовательно (сверху вниз) находим, что

$$a_0 = \mathbf{1}, a_3 = \mathbf{0}, a_2 = \mathbf{0}, a_{23} = \mathbf{0}, a_1 = \mathbf{1}, a_{13} = \mathbf{1}, a_{12} = \mathbf{1}, a_{123} = \mathbf{1}.$$

Таким образом,

$$(x_1 \vee x_2) \to (x_2 \vee x_3) = \mathbf{1} \oplus x_1 \oplus x_1 \cdot x_2 \oplus x_1 \cdot x_3 \oplus x_1 \cdot x_2 \cdot x_3.$$

Задача решена. ►

Далее пойдет речь о кополиномах Жегалкина. Но прежде сделаем несколько замечаний:

1) Кополиномы Жегалкина являются объектами, двойственными к полиномам Жегалкина. Отсюда и название: использование приставки «ко» для двойственных объектов является общей практикой в математике; например, если дано какое-то понятие с именем «∗∗∗», то для двойственного ему понятия (в случае, если для него нет еще подходящего названия) дается имя «ко∗∗∗».

2) Можно сказать, что полиномы и кополиномы Жегалкина «равноправны» в том смысле, что они двойственны друг другу. Однако кополиномы Жегалкина используются для представления булевых функций крайне редко. Одно из объяснений может быть такое: множество $\mathbb{B}$ относительно операций $\oplus$, $\wedge$ является кольцом, а полиномы Жегалкина являются ни чем иным, как полиномами над этим кольцом, т. е. полиномы Жегалкина — достаточно обычный алгебраический объект.

3) От представления булевой функции в виде полинома Жегалкина очень легко переходить к представлению в виде кополинома Жегалкина и обратно. Для этого достаточно использовать следующие легко проверяемые равенства:

Переход: *полин. Жегалк.* $\rightsquigarrow$ *копол. Жегалк.*	*Переход:* *кополин. Жегалк.* $\rightsquigarrow$ *полин. Жегалк.*
$x \oplus y = \mathbf{0} \leftrightarrow x \leftrightarrow y$,	$x \leftrightarrow y = \mathbf{1} \oplus x \oplus y$,
$x \cdot y = x \leftrightarrow y \leftrightarrow (x \vee y)$,	$x \vee y = x \oplus y \oplus xy$,
$A \leftrightarrow A = \mathbf{1}$,	$A \oplus A = \mathbf{0}$,
$A \leftrightarrow \mathbf{1} = A$,	$A \oplus \mathbf{0} = A$,
эквиваленция четного числа $\mathbf{0}$ *равна* $\mathbf{1}$,	*сумма по модулю 2 четного числа* $\mathbf{1}$ *равна* $\mathbf{0}$,
эквиваленция нечетного числа $\mathbf{0}$ *равна* $\mathbf{0}$	*сумма по модулю 2 нечетного числа* $\mathbf{1}$ *равна* $\mathbf{1}$.

Теорема 3.4. *Каждая булева функция $f(x_1, \ldots, x_n) \in \mathbb{BF}(n)$ единственным образом представима в виде кополинома Жегалкина по переменным $x_1, \ldots, x_n$.*

◀ Пусть $f(x_1,\dots,x_n)$ — произвольно фиксированная булева функция. Тогда для нее существует единственная двойственная ей булева функция $f^*(x_1,\dots,x_n)$. Представим эту функцию в виде полинома Жегалкина (такое представление единственно):

$$f^*(x_1,\dots,x_n) = \\ = a_0 \oplus a_1x_1 \oplus \dots \oplus a_{i_1\dots i_k}x_{i_1}\cdots x_{i_k} \oplus \dots \oplus a_{12\dots n}x_1x_2\cdots x_n.$$

Тогда ввиду равенств $f^{**} = f$, $\mathbf{1}^* = \mathbf{0}$, $\mathbf{0}^* = \mathbf{1}$, принципа двойственности и того факта, что двойственной операцией для «$\wedge$» является «$\vee$», а двойственной для «$\oplus$» является операция «$\leftrightarrow$», получаем:

$$f(x_1,\dots,x_n) = \\ = \bar{a}_0 \leftrightarrow (\bar{a}_1 \vee x_1) \leftrightarrow \dots \leftrightarrow (\bar{a}_{i_1\dots i_k} \vee x_{i_1} \vee \dots \vee x_{i_k}) \leftrightarrow \dots \leftrightarrow \\ \leftrightarrow (\bar{a}_{12\dots n} \vee x_1 \vee x_2 \vee \dots \vee x_n).$$

Доказательство завершено. ▶

Алгоритм построения кополинома Жегалкина:

1 шаг: Если функция задана в виде обобщенного булева выражения, то пользуясь равенствами

$$\bar{x} = x \leftrightarrow \mathbf{0}, \qquad x - y = \mathbf{0} \leftrightarrow y \leftrightarrow (x \vee y),$$
$$x \wedge y = x \leftrightarrow y \leftrightarrow (x \vee y), \qquad x \,|\, y = \mathbf{0} \leftrightarrow x \leftrightarrow y \leftrightarrow (x \vee y),$$
$$x \to y = y \leftrightarrow (x \vee y), \qquad x \downarrow y = \mathbf{0} \leftrightarrow (x \vee y),$$
$$x \oplus y = \mathbf{0} \leftrightarrow (x \vee y),$$

записать ее в виде обобщенного булевого выражения, построенного лишь с помощью операций $\vee$ и $\leftrightarrow$. Если же функция задана каким-либо другим способом, то предварительно задать ее в виде булевого выражения, например, с помощью теоремы о СДНФ, а затем проделать указанные выше замены.

2 шаг: Пользуясь дистрибутивностью $x \vee (y \leftrightarrow z) = (x \vee y) \leftrightarrow (x \vee z)$, раскрыть все скобки в полученном на первом шаге обобщенном булевом выражении. Получим:

$$f(x_1, \ldots, x_n) = E_1' \leftrightarrow E_2' \leftrightarrow \ldots \leftrightarrow E_r',$$

где каждая из E_i' есть дизъюнкция переменных и нулей.

3 шаг: Преобразуем все полученные дизъюнкции E_i' в монотонные дизъюнкции E_j, пользуясь при этом коммутативностью булевого умножения и соотношениями $x \vee x = x$, $\mathbf{0} \vee \mathbf{0} = \mathbf{0}$ и $A \vee \mathbf{0} = A$.

4 шаг: Преобразуем полученное выражение в кополином Жегалкина, пользуясь при этом соотношениями $A \leftrightarrow A = \mathbf{1}$ и $A \leftrightarrow \mathbf{1} = A$. В результате получим либо

$$f(x_1, \ldots, x_n) = E_1 \leftrightarrow E_2 \leftrightarrow \ldots \leftrightarrow E_m.$$

либо $f(x_1, \ldots, x_n) = \mathbf{0}$ или $f(x_1, \ldots, x_n) = \mathbf{1}$.

Так же, как и в случае полинома Жегалкина, поиск кополинома для булевой функции можно осуществлять методом неопределенных коэффициентов.

Пример 10. Представить посредством кополинома Жегалкина булеву функцию $f(x_1, x_2, x_3) = (x_1x_2)\,|(x_1 \to x_3)$.

Решение. `1 способ.` Воспользуемся равенствами

$$A \cdot B = A \leftrightarrow B \leftrightarrow (A \vee B),\ \ A \to B = B \leftrightarrow (A \vee B),\ \ A\,|\,B = \mathbf{0} \leftrightarrow (A \vee B),$$

чтобы выразить нашу булеву функцию только с помощью операций $\leftrightarrow$, $\vee$ и постоянных:

$$(x_1x_2)\,|(x_1 \to x_3) = \big(x_1 \leftrightarrow x_2 \leftrightarrow (x_1 \vee x_2)\big)\,|\,\big(x_3 \leftrightarrow (x_3 \vee x_1)\big) =$$
$$= \mathbf{0} \leftrightarrow \big(x_1 \leftrightarrow x_2 \leftrightarrow (x_1 \vee x_2)\big) \vee \big(x_3 \leftrightarrow (x_1 \vee x_3)\big).$$

Далее воспользуемся дистрибутивным законом $A \vee (B \leftrightarrow C) = (A \vee B) \leftrightarrow (A \vee C)$:

$$\mathbf{0} \leftrightarrow \big(x_1 \leftrightarrow x_2 \leftrightarrow (x_1 \vee x_2)\big) \vee \big(x_3 \leftrightarrow (x_1 \vee x_3)\big) =$$
$$= \mathbf{0} \leftrightarrow \big(x_1 \vee x_3\big) \leftrightarrow \big(x_1 \vee x_1 \vee x_3\big) \leftrightarrow \big(x_2 \vee x_3\big) \leftrightarrow$$
$$\leftrightarrow \big(x_2 \vee x_1 \vee x_3\big) \leftrightarrow \big(x_1 \vee x_2 \vee x_3\big) \leftrightarrow \big(x_1 \vee x_2 \vee x_1 \vee x_3\big).$$

Заключенные в скобки дизъюнкции преобразуем в монотонные дизъюнкции:

$$\mathbf{0} \leftrightarrow \big(x_1 \vee x_3\big) \leftrightarrow \big(x_1 \vee x_3\big) \leftrightarrow \big(x_2 \vee x_3\big) \leftrightarrow \big(x_1 \vee x_2 \vee x_3\big) \leftrightarrow$$
$$\leftrightarrow \big(x_1 \vee x_2 \vee x_3\big) \leftrightarrow \big(x_1 \vee x_2 \vee x_3\big).$$

Наконец, исходя из равенств $A \leftrightarrow A = \mathbf{1}$, $A \leftrightarrow \mathbf{1} = A$, получим (пары подчеркнутых соответствующим числом линий выражений дают $\mathbf{1}$):

$$\mathbf{0} \leftrightarrow \underline{(x_1 \vee x_3)} \leftrightarrow \underline{(x_1 \vee x_3)} \leftrightarrow (x_2 \vee x_3) \leftrightarrow \underline{\underline{(x_1 \vee x_2 \vee x_3)}} \leftrightarrow$$
$$\leftrightarrow \underline{\underline{(x_1 \vee x_2 \vee x_3)}} \leftrightarrow (x_1 \vee x_2 \vee x_3) =$$
$$= \mathbf{0} \leftrightarrow (x_2 \vee x_3) \leftrightarrow (x_1 \vee x_2 \vee x_3).$$

В итоге получаем следующее представление нашей функции в виде кополинома Жегалкина:

$$(x_1x_2)\,|\,(x_1 \to x_3) = \mathbf{0} \leftrightarrow (x_2 \vee x_3) \leftrightarrow (x_1 \vee x_2 \vee x_3).$$

<u>2 способ.</u> Будем искать кополином Жегалкина для нашей функции $f(x_1, x_2, x_3) = (x_1x_2)\,|\,(x_1 \to x_3)$ в виде кополинома с неопределенными коэффициентами

$$a_0 \leftrightarrow (a_1 \vee x_1) \leftrightarrow (a_2 \vee x_2) \leftrightarrow (a_3 \vee x_3) \leftrightarrow$$
$$\leftrightarrow (a_{12} \vee x_1 \vee x_2) \leftrightarrow (a_{13} \vee x_1 \vee x_3) \leftrightarrow (a_{23} \vee x_2 \vee x_3) \leftrightarrow (a_{123} \vee x_1 \vee x_2 \vee x_3),$$

где коэффициенты $a_0, a_1, \ldots, a_{123}$ будем искать, подставляя конкретные значения вместо переменных.

Соберем вычисления в таблицу.

x_1	x_2	x_3	$(x_1x_2)\,\vert\,(x_1 \to x_3)$	$a_0 \leftrightarrow (a_1 \vee x_1) \leftrightarrow \ldots \leftrightarrow (a_{123} \vee x_1 \vee x_2 \vee x_3)$
0	**0**	**0**	**0**	$a_0 \leftrightarrow a_1 \leftrightarrow a_2 \leftrightarrow a_3 \leftrightarrow a_{12} \leftrightarrow a_{13} \leftrightarrow a_{23} \leftrightarrow a_{123}$
0	**0**	**1**	**0**	$a_0 \leftrightarrow a_1 \leftrightarrow a_2 \leftrightarrow a_{12}$
0	**1**	**0**	**0**	$a_0 \leftrightarrow a_1 \leftrightarrow a_3 \leftrightarrow a_{13}$
0	**1**	**1**	**0**	$a_0 \oplus a_1$
1	**0**	**0**	**1**	$a_0 \leftrightarrow a_2 \leftrightarrow a_3 \leftrightarrow a_{23}$
1	**0**	**1**	**0**	$a_0 \leftrightarrow a_2$
1	**1**	**0**	**0**	$a_0 \leftrightarrow a_3$
1	**1**	**1**	**0**	a_0

Из последней колонки этой таблицы последовательно (снизу вверх) находим, что

$$a_0 = \mathbf{0}, a_3 = \mathbf{1}, a_2 = \mathbf{1}, a_{23} = \mathbf{0}, a_1 = \mathbf{1}, a_{13} = \mathbf{1}, a_{12} = \mathbf{1}, a_{123} = \mathbf{0}.$$

Таким образом,

$$(x_1x_2)\,|\,(x_1 \to x_3) = \mathbf{0} \leftrightarrow (x_2 \vee x_3) \leftrightarrow (x_1 \vee x_2 \vee x_3).$$

Задача решена. ▶

3.5. Упражнения

1. С помощью эквивалентных преобразований привести функцию f к ДНФ:

1) $f(x_1, x_2, x_3) = (\bar{x}_1 \vee \bar{x}_2 \vee x_3) \cdot (x_1x_2 \vee \bar{x}_3)$;
2) $f(x_1, x_2, x_3) = (\bar{x}_1\bar{x}_2 \oplus x_3) \cdot (x_1x_3 \vee \bar{x}_2)$;
3) $f(x_1, x_2, x_3) = \overline{(x_1 \to (x_2 \to x_3))} \oplus (x_1\,|\,(x_2 \oplus x_3))$;
4) $f(x_1, x_2, x_3, x_4) = (x_1 \vee x_2\bar{x}_3\bar{x}_4) \cdot ((\bar{x}_1 \vee x_4) \oplus x_2x_3) \vee \bar{x}_2 \cdot (x_3 \vee \overline{x_1\bar{x}_4})$;
5) $f(x_1, x_2, x_3, x_4) = (x_1 \to x_2) \cdot (x_2 \to \bar{x}_3) \cdot (x_3 \to x_1\bar{x}_4)$.

2. С помощью эквивалентных преобразований привести функцию f к КНФ:

1) $f(x_1, x_2, x_3) = x_1\bar{x}_2 \vee \bar{x}_2x_3 \vee (x_1 \to x_2x_3)$;
2) $f(x_1, x_2, x_3) = (\bar{x}_1 \to (x_2 \to x_3)) \oplus x_1\bar{x}_2x_3$;
3) $f(x_1, x_2, x_3) = (x_1 \leftrightarrow (x_2 \to x_3)) \vee (x_2 \to x_1x_3)$;
4) $f(x_1, x_2, x_3, x_4) = \bar{x}_1x_2 \vee \bar{x}_2x_3 \vee \bar{x}_3x_4 \vee x_1\bar{x}_4$;

5) $f(x_1, x_2, x_3, x_4) = (x_1 \leftrightarrow x_2) \vee (x_1 x_3 \leftrightarrow x_4) \vee x_2 \bar{x}_3$.

3. Применяя преобразования вида $A = A \cdot \bar{x} \vee A \cdot \bar{x}$ и $A \vee A = A$, построить из заданной ДНФ функции f ее СДНФ:

1) $f(x_1, x_2, x_3) = x_1 \bar{x}_3 \vee \bar{x}_2$;

2) $f(x_1, x_2, x_3) = \bar{x}_1 \bar{x}_2 \vee \bar{x}_2 x_3 \vee x_1$;

3) $f(x_1, x_2, x_3) = \bar{x}_2 \vee x_2 \vee \bar{x}_1 x_3$;

4) $f(x_1, x_2, x_3, x_4) = x_1 x_2 \bar{x}_3 \vee x_1 \bar{x}_3 x_4$;

5) $f(x_1, x_2, x_3, x_4) = x_1 x_2 \vee \bar{x}_2 x_4 \vee x_3 \bar{x}_4$.

4. Применяя преобразования вида $A = (A \vee x) \cdot (A \vee \bar{x})$ и $A \cdot A = A$, построить из заданной КНФ функции f ее СКНФ:

1) $f(x_1, x_2, x_3) = (x_1 \vee \bar{x}_2) \cdot x_3$;

2) $f(x_1, x_2, x_3) = (\bar{x}_1 \vee x_3) \cdot (\bar{x}_1 \vee x_3) \cdot x_3$;

3) $f(x_1, x_2, x_3) = x_1 \cdot \bar{x}_2 \cdot (x_1 \vee x_3) \cdot (\bar{x}_2 \vee \bar{x}_3)$;

4) $f(x_1, x_2, x_3, x_4) = (x_1 \vee x_2 \vee \bar{x}_3) \cdot (x_1 \vee \bar{x}_2 \vee x_4)$;

5) $f(x_1, x_2, x_3, x_4) = (x_1 \vee x_2) \cdot (\bar{x}_2 \vee x_3) \cdot (\bar{x}_3 \vee \bar{x}_4)$.

5. Использую табличное задание, построить СДНФ и СКНФ булевой функции f:

1) $f(x_1, x_2, x_3) = (x_1 \vee x_2) \to x_3$;

2) $f(x_1, x_2, x_3) = ((x_2 \downarrow x_3) \downarrow x_1) \oplus (x_1 \to x_3)$;

3) $f(x_1, x_2, x_3) = (x_1 \to x_2 \bar{x}_3) \vee (x_1 \oplus x_2 \oplus x_3)$;

4) $f(x_1, x_2, x_3, x_4) = (x_1 \oplus x_2) \cdot (x_3 \to \bar{x}_2 x_4)$;

5) $f(x_1, x_2, x_3, x_4) = (x_1 \to x_2 x_3 x_4) \cdot (x_3 \to x_1 \bar{x}_3)$.

6. Построить СДНФ и СКНФ булевой функции f, заданной с помощью характеристического множества N_f:

1) $N_f = \{(\mathbf{0}, \mathbf{1}, \mathbf{1}), (\mathbf{1}, \mathbf{0}, \mathbf{1}), (\mathbf{1}, \mathbf{1}, \mathbf{0}), (\mathbf{1}, \mathbf{1}, \mathbf{1})\}$;

2) $N_f = \{(\mathbf{1}, \mathbf{1}, \mathbf{1}), (\mathbf{0}, \mathbf{0}, \mathbf{1}), (\mathbf{1}, \mathbf{0}, \mathbf{1}), (\mathbf{0}, \mathbf{1}, \mathbf{1}), (\mathbf{0}, \mathbf{1}, \mathbf{0})\}$;

3) $N_f = \{(\mathbf{1}, \mathbf{0}, \mathbf{1}), (\mathbf{1}, \mathbf{0}, \mathbf{1}), (\mathbf{1}, \mathbf{0}, \mathbf{0})\}$;

4) $N_f = \{(\mathbf{0}, \mathbf{0}, \mathbf{1}, \mathbf{1}), (\mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{1}), (\mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{0}), (\mathbf{1}, \mathbf{1}, \mathbf{0}, \mathbf{1}), (\mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{0})\}$;

5) $N_f = \{(\mathbf{0}, \mathbf{0}, \mathbf{1}, \mathbf{0}), (\mathbf{1}, \mathbf{0}, \mathbf{0}, \mathbf{1}), (\mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{0}), (\mathbf{0}, \mathbf{0}, \mathbf{1}, \mathbf{1}),$
$(\mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{1}), (\mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{0}), (\mathbf{1}, \mathbf{1}, \mathbf{0}, \mathbf{1}), (\mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{0})\}$.

7. Построить СДНФ и СКНФ булевой функции, заданной в виде слова:

1) $f(x_1, x_2, x_3) = [\![\mathbf{01010101}]\!]$;

2) $f(x_1, x_2, x_3) = [\![\mathbf{11010101}]\!]$;

3) $f(x_1, x_2, x_3) = [\![\mathbf{10000100}]\!]$;

4) $f(x_1, x_2, x_3, x_4) = [\![\mathbf{1110001110101000}]\!]$;

5) $f(x_1, x_2, x_3, x_4) = [\![\mathbf{0101010110101001}]\!]$.

8. Найти длину СДНФ функции f:

1) $f(x_1, \ldots, x_n) = \bigvee\limits_{1 \leqslant i < j \leqslant n} x_i x_j, \quad n \geqslant 2$;

2) $f(x_1, \ldots, x_n) = \bigwedge\limits_{1 \leqslant i < j \leqslant n} (x_i \to x_j), \quad n \geqslant 2$;

3) $f(x_1, \ldots, x_n) = x_1 \to (x_2 \to (\ldots \to (x_{n-1} \to x_n) \ldots)), \ n \geqslant \ 2$;

4) $f(x_1, \dots, x_n) = x_1 x_2 \cdots x_n \oplus x_3 \oplus \dots \oplus x_n, \quad n \geqslant 3;$

5) $f(x_1, \dots, x_n) = (x_1 \vee x_2) \cdot (\tilde{x}_1 \vee \tilde{x}_2) \to x_3 \cdot x_4 \cdots x_n, \quad n \geqslant 3.$

9. Найти длину СДНФ функции $f(x_1, \dots, x_n) \oplus g(x_1, \dots, x_n)$, если известны длины СДНФ следующих функций:

1) $f(x_1, \dots, x_n) \wedge g(x_1, \dots, x_n)$ и $f(x_1, \dots, x_n) \vee g(x_1, \dots, x_n);$

2) $f(x_1, \dots, x_n) \to g(x_1, \dots, x_n)$ и $g(x_1, \dots, x_n) \to f(x_1, \dots, x_n).$

10. Показать, что переменная x_i является фиктивной переменной булевой функции $f(x_1, \dots, x_n)$ тогда и только тогда, когда в СДНФ этой функции вместе с каждой элементарной конъюнкцией вида $x_i^{\sigma_i} K$ содержится и элементарная конъюнкция вида $x_i^{\overline{\sigma}_i} K$.

11. Показать, что переменная x_i является фиктивной переменной булевой функции $f(x_1, \dots, x_n)$ тогда и только тогда, когда полином Жегалкина, реализующий эту функцию, не содержит эту переменную x_i.

12. Методом неопределенных коэффициентов найти полином и кополином Жегалкина для функций:

1) $f = [\![\mathbf{1001}]\!];$

2) $f = [\![\mathbf{0100}]\!];$

3) $f = [\![\mathbf{11111000}]\!];$

4) $f = [\![\mathbf{01101000}]\!];$

5) $f = [\![\mathbf{01100110}]\!];$

6) $f = [\![\mathbf{1000000000000001}]\!];$

7) $f = [\![\mathbf{0000100010010000}]\!];$

8) $f(x_1, x_2, x_3) = (x_1 \,|\, x_2) \,|\, x_3$;
9) $f(x_1, x_2, x_3) = (x_1 \downarrow x_2) \downarrow x_3$;
10) $f(x_1, x_2, x_3) = x_1(x_2 \vee x_3)$;
11) $f(x_1, x_2, x_3) = x_1 \to (x_2 \to x_3)$.

13. Методом преобразований найти полином и кополином Жегалкина для функций:

1) $f(x_1, x_2, x_3) = x_1 \to (x_2 \to \bar{x}_1 x_2)$;
2) $f(x_1, x_2, x_3) = (x_1 \downarrow x_2) \,|(x_2 \downarrow x_3)$;
3) $f(x_1, x_2, x_3) = x_1 \downarrow ((x_1 \to \bar{x}_2) \vee x_3)$;
4) $f(x_1, x_2, x_3) = (x_1 \to (x_2 \to x_3)) \cdot ((x_1 \to x_2) \to x_3)$;
5) $f(x_1, x_2, x_3) = (x_1 \oplus x_2) \vee (x_2 \downarrow x_3)$;
6) $f(x_1, x_2, x_3, x_4) = (x_1 \to x_2) \to (x_3 \to x_1 x_4)$;
7) $f(x_1, x_2, x_3, x_4) = x_1 \cdot (x_2 \leftrightarrow x_1 \bar{x}_3) \cdot (x_2 \vee x_4)$;
8) $f(x_1, x_2, x_3, x_4) = (x_1 \to x_4) \vee (x_2 \,|\, \bar{x}_3) \vee (x_3 \to x_4)$.

14. Выяснить на скольких наборах из $\mathbb{B}^n$ обращается в **1** полином P (иначе говоря, вычислить мощность характеристического множества N_P):

1) $P(x_1, \ldots, x_n) = x_1 x_2 \oplus x_1 x_3 \oplus \ldots \oplus x_1 x_n, \quad n \geqslant 2$;
2) $P(x_1, \ldots, x_n) = x_1 x_2 \oplus x_3 \oplus \ldots \oplus x_n, \quad n \geqslant 3$;
3) $P(x_1, \ldots, x_n) = x_1 x_2 \oplus x_1 x_3 \oplus x_4 \oplus \ldots \oplus x_n, \quad n \geqslant 4$;
4) $P(x_1, \ldots, x_n) = x_1 x_2 x_3 \oplus \bigoplus_{i=4}^{n} x_1, \quad n \geqslant 4$;

5) $P(x_1,\dots,x_n) = x_1x_2\cdots x_k \oplus x_{k+1}x_{k+2}\cdots x_n, \quad 1 \leqslant k \leqslant n;$

6) $P(x_1,\dots,x_n) = \bigoplus\limits_{i=1}^{n}(x_1\cdots x_i \oplus 1), \quad n \geqslant 1;$

7) $P(x_1,\dots,x_n) = \bigoplus\limits_{i=1}^{n} x_1\cdots x_{i-1}x_{i+1}\cdots x_n, \quad n \geqslant 2;$

8) $P(x_1,\dots,x_n) = x_1 \oplus \bigoplus\limits_{1\leqslant i<j\leqslant n} x_ix_j, \quad n \geqslant 2;$

9) $P = (x_1,\dots,x_n) = \bigoplus\limits_{1\leqslant i<j\leqslant n} x_ix_j \oplus \bigoplus\limits_{i=1}^{n} x_i, \quad n \geqslant 2.$

4. Замыкание и полные системы функций

4.1. Замыкание класса функций и принцип индукции

Пусть $A \subseteq \mathbb{BF}$, т. е. A — некоторое множество булевых функций.

Определение 4.1. Понятие *формулы над A* дается следующим рекурсивным определением:

1. любая функция из A является *формулой над A*;
2. если $f(x_1,\dots,x_n) \in A$ и H_i, $1 \leqslant i \leqslant n$, есть либо переменная, либо формула над A, то выражение вида
$$f(H_1,\dots,H_n)$$

также является *формулой над* A;

3. только такие объекты являются *формулами над* A, которые можно построить с помощью пунктов 1 и 2 данного определения.

Определение 4.2. Пусть A — некоторое множество булевых функций. *Замыканием* A называется множество всех булевых функций, которые можно выразить формулами над A.

Замыкание множества функций A будем обозначать через $[A]$.

Индуктивный взгляд на данное выше рекурсивное определение понятия формулы над A состоит в следующем «поуровневом» определении.

1 «уровень». Все функции из A являются *формулами над* A («уровня» $= 1$).

2 «уровень». Если $f(x_1, \dots, x_n) \in A$ и H_i, $1 \leqslant i \leqslant n$ есть либо переменная, либо формула над A «уровня» < 2, то выражение вида

$$f(H_1, \dots, H_n)$$

также является *формулой над* A («уровня» $\leqslant 2$).

3 «уровень». Если $f(x_1, \dots, x_n) \in A$ и H_i, $1 \leqslant i \leqslant n$ есть либо переменная, либо формула над A «уровня» < 3, то выражение вида

$$f(H_1, \dots, H_n)$$

также является *формулой над* A («уровня» $\leqslant 3$).

. . . .

k «уровень». Если $f(x_1, \ldots, x_n) \in A$ и H_i, $1 \leqslant i \leqslant n$ есть либо переменная, либо формула над A «уровня» $< k$, то выражение вида

$$f(H_1, \ldots, H_n)$$

также является *формулой над* A («уровня» $\leqslant k$).

. . . .

Такой взгляд на определение понятия формулы над A подсказывает индуктивный способ доказательства утверждений о функциях из $[A]$.

Пусть $\mathcal{P}$ есть некоторое свойство, которым могут обладать, а могут и не обладать булевы функции и A — некоторый класс булевых функций.

Индуктивный принцип доказательства утверждения, что все функции из $[A]$ обладают свойством $\mathcal{P}$, заключается в следующем:

База индукции: *все функции из* A *обладают свойством* $\mathcal{P}$*;*

Индуктивный шаг: *пусть* $f(x_1, \ldots, x_n)$ *— произвольная функция из* A *и* $H_1, \ldots, H_n$ *— переменные или формулы над* A *«уровня»* $< n$*, которые обладают свойством* $\mathcal{P}$*. Тогда, если функция*

$$f(H_1, \ldots, H_n)$$

также обладает свойством $\mathcal{P}$, то можно сделать вывод, что
все формулы из A обладают свойством $\mathcal{P}$.

Булевы функции f и g будем называть *конгруентными*, если одна из них может быть получена из другой заменой переменных (без отождествления). Например, функции $x \cdot \bar{y}$ и $x \cdot \bar{z}$ являются конгруентными, а функции $x \cdot y$ и $z \cdot z$ не являются конгруентными. При рассмотрении вопросов, связанных с замкнутыми классами, бывает удобно указывать по одному представителю из множества попарно конгруентных функций. Например, класс $\{x, y, z, \ldots, x_1, x_2, \ldots\}$ будет обозначаться через $\{x\}$.

Следующие свойства операции замыкания $A \mapsto [A]$ получаются непосредственно из определения.

Предложение 4.1. *Для произвольных множеств $A, B \subseteq \mathbb{BF}$ справедливы соотношения:*

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

Класс булевых функций A называется

✓ *замкнутым*, если $[A] = A$;

- ✓ *полным*, если $[A] = \mathbb{BF}$;
- ✓ *базисом*, если $[A] = \mathbb{BF}$, но $[A \setminus \{f\}] \neq \mathbb{BF}$ для произвольного $f \in A$;
- ✓ *предполным*, если $[A] \neq \mathbb{BF}$, но $[A \cup \{f\}] = \mathbb{BF}$ для произвольной булевой функции $f \notin A$.

4.2. Полные системы функций

В этом пункте мы интересуемся полными системами функций, т. е. такими системами функций A, что любая булева функция является формулой над A (напомним, что в класс A вместе с каждой указанной в нем функцией входят и все конгруэнтные ей функции).

Из теоремы о СДНФ сразу же получаем, что система $A = \{x \vee y, x \wedge y, \ \bar{x}\ \}$ является полной системой. Действительно, если булева функция f отлична от тождественного нуля, то по этой теореме имеем, что f выражается в виде совершенной дизъюнктивной нормальной формы, в которую входят только булевы суммы $\vee$, произведения $\wedge$ и дополнения $\bar{}$. Если же $f \equiv \mathbf{0}$, то $f = x \cdot \bar{x}$.

Следующая простая лемма бывает полезна при установлении полноты некоторых систем функций.

Лемма 4.1. *Если класс A является полным и всякая функция из A является формулой над B, то класс B также является полным.*

◀ Тот факт, что всякая функция из A является формулой над B, равносилен тому, что $A \subseteq [B]$. Так как класс A является полным, то $[A] = \mathbb{BF}$. Отсюда, пользуясь свойствами операции замыкания из предложения 4.1, получаем

$$[B] \supseteq A \Longrightarrow [[B]] \supseteq [A] \Longrightarrow [B] = \mathbb{BF}\,.$$

Это и означает полноту класса B. ▶

Теорема 4.1. *Следующие системы булевых функций являются полными в $\mathbb{BF}$. Более того, каждая из приведенных систем является базисом в $\mathbb{BF}$.*

1. $\{x \vee y,\ \bar{x}\ \}$ *(дизъюнктивный базис);*
2. $\{x \wedge y,\ \bar{x}\ \}$ *(конъюнктивный базис);*
3. $\{x \to y,\ \bar{x}\ \}$ *(импликативный базис);*
4. $\{x \,|\, y\}$ *(базис Шеффера);*
5. $\{x \downarrow y\}$ *(базис Пирса);*
6. $\{\mathbf{1}, x \wedge y, x \oplus y\}$ *(базис Жегалкина);*
7. $\{\mathbf{0}, \mathbf{1}, x \wedge y, x \oplus y \oplus z\}$.

◀Доказательство полноты всех этих систем функций проведем по одной и той же схеме: обозначив любую из приведенных систем через B, покажем, что каждая из функций, входящих в $A = \{x \vee y, x \wedge y,\ \bar{x}\ \}$ является формулой над B; а т. к. система $A = \{x \vee y, x \wedge y,\ \bar{x}\ \}$, как мы отмечали, полна, то полнота системы B будет следовать из леммы 4.1.

1. $B = \{x \vee y,\ \bar{x}\ \}$. Имеем $x \wedge y = \overline{\bar{x} \vee \bar{y}}$. Отсюда $A \subseteq [B]$ и, значит, B — полная система.

2. $B = \{x \wedge y,\ \bar{x}\ \}$. Имеем $x \vee y = \overline{\bar{x} \wedge \bar{y}}$. Отсюда $A \subseteq [B]$ и, значит, B — полная система.

3. $B = \{x \to y,\ \bar{x}\ \}$. Имеем $x \vee y = \bar{x} \to y, x \wedge y = \overline{x \to \bar{y}}$. Отсюда $A \subseteq [B]$ и, значит, B — полная система.

4. $B = \{x\,|\,y\}$. Имеем $\bar{x} = x\,|\,x,\ \ x \vee y = (x\,|\,x)\,|(y\,|\,y),\ \ x \wedge y = (x\,|\,y)\,|(x\,|\,y)$. Отсюда $A \subseteq [B]$ и, значит, B — полная система.

5. $B = \{x \downarrow y\}$. Имеем $\bar{x} = x \downarrow x,\ \ x \vee y = (x \downarrow y) \downarrow (x \downarrow y),\ \ x \vee y = (x \downarrow x) \downarrow (y \downarrow y)$. Отсюда $A \subseteq [B]$ и, значит, B — полная система.

6. $B = \{x \wedge y, x \oplus y, \mathbf{1}\}$. Имеем $\bar{x} = x \oplus \mathbf{1},\ \ x \vee y = x \oplus y \oplus (x \wedge y)$. Отсюда $A \subseteq [B]$ и, значит, B — полная система. ▶

7. $B = \{\mathbf{0}, \mathbf{1}, x \wedge y, x \oplus y \oplus z\}$. Имеем $\bar{x} = x \oplus \mathbf{1} \oplus \mathbf{0},\ \ x \vee y = x \oplus y \oplus x \cdot y$. Отсюда $A \subseteq [B]$ и, значит, B — полная система.

Тот факт, что приведенные системы образуют базис мы докажем позже в пункте 7.1 на стр. 149.

4.3. Упражнения

1. Построить множество всех функций, зависящих от переменных x_1, x_2 и принадлежащих замыканию множества A:

1) $A = \{\bar{x}\}$;
2) $A = \{x_1 \oplus x_2\}$;
3) $A = \{\mathbf{0}, \bar{x}\}$;
4) $A = \{x_1 \wedge x_2\}$;
5) $A = \{x_1 \oplus x_2 \oplus x_3\}$;
6) $A = \{x_1x_2 \vee x_2\bar{x}_3 \vee \bar{x}_3x_1\}$.

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

1) $f = \bar{x},\ A = \{\mathbf{0}, x \to y\}$;
2) $f = x \oplus y,\ A = \{x \downarrow y\}$;
3) $f = x,\ A = \{x \oplus y\}$;
4) $f = x \oplus y \oplus z,\ A = \{x \leftrightarrow y\}$;
5) $f = xy,\ A = \{xy \oplus z\}$;
6) $f = x \vee y,\ A = \{x \to y\}$;
7) $f = x \oplus y,\ A = \{x\bar{y}, x \vee \bar{y}\}$;
8) $f = xy,\ A = \{x\vee, x \oplus y\}$.

3. Доказать предложение 4.1 на стр. 104.

4. Выяснить, является ли множество A замкнутым классом:

$$1)\ A = \{\mathbf{0}, \mathbf{1}\};\quad 2)\ A = \{\bar{x}\};\quad 3)\ A = \{x, \bar{x}\};\quad 4)\ A = \{\mathbf{1}, \bar{x}\};$$

$$5)\ A = \{x_1 \cdot x_2 \cdot \dots \cdot x_n \mid n = 1, 2, \dots\};$$

$$6)\ A = \{x_1 \oplus x_2 \oplus \ldots \oplus x_n \mid n = 1, 2, \dots\};$$

$$7)\ A = \{\mathbf{0}, x_1 \vee x_2 \vee \ldots \vee x_n \mid n = 1, 2, \dots\};$$

$$8)\ A = \{x_1 \oplus x_2 \oplus \ldots \oplus x_{2n-1} \mid n = 1, 2, \dots\};$$

$$9)\ A = \{\mathbf{0}, x_1 \oplus x_2 \oplus \ldots \oplus x_{2n-1} \mid n = 1, 2, \dots\};$$

$$10)\ A = \{\mathbf{0}, \mathbf{1}, x_1 \oplus x_2 \oplus \ldots \oplus x_n \oplus \sigma \mid \sigma \in \{\mathbf{0}, \mathbf{1}\},\ n = 1, 2, \dots\}.$$

5. Доказать, что каждый предполный класс содержит тождественную функцию.

6. Доказать, что всякий замкнутый класс, содержащий функцию, отличную от константы, содержит и функцию x.

7. Доказать, что множество всех булевых функций $\mathbb{B}$ непредставимо в виде объединения непустых попарно непересекающихся замкнутых классов.

8. Доказать, что если замкнутый класс имеет конечный базис, то всякий базис этого класса конечен.

9. Доказать, что в замкнутом классе $[x \to y]$ содержатся только такие булевы функции, которые могут быть представлены (с точностью до обозначения переменных) в виде $x_i \vee f(x_1, \dots, x_n)$, где $f(x_1, \dots, x_n) \in \mathbb{B}^n$.

10. Пусть функция $f(x_1, \dots, x_n)$ принадлежит множеству $[x \to y]$ и зависит существенно не менее чем от двух переменных. Доказать, что $|N_f| > 2^{n-1}$.

5. Замкнутые классы Поста

5.1. Класс функций, сохраняющих нуль

Определение 5.1. Систему всех булевых функций, которые на нулевом наборе своих аргументов принимают нулевое значение, обозначим через $\mathbf{T_0}$ и назовем *классом функций, сохраняющих нуль*. Таким образом,

$$\mathbf{T_0} \stackrel{\text{def}}{:=} \{\, f \in \mathbb{BF} \mid f(\mathbf{0}, \mathbf{0}, \ldots, \mathbf{0}) = \mathbf{0}\}.$$

Пример 11. Проверка следующих утверждений тривиальна.

Функций из класса $\mathbf{T_0}$: $\mathbf{0}$, x $x \cdot y$, $x \vee y$, $x \oplus y$, $x - y$,
Функций не из класса $\mathbf{T_0}$: $\mathbf{1}$, $\bar{x}$, $x \to y$, $x \leftrightarrow y$, $x \downarrow y$, $x \mid y$.

Теорема 5.1. *Класс функций, сохраняющих нуль* $\mathbf{T_0}$*, замкнут:*

$$[\mathbf{T_0}] = \mathbf{T_0}.$$

◀ Докажем теорему, применяя принцип индукции. В качестве свойства $\mathcal{P}$ возьмем свойство «булева функция f сохраняет нуль.»

(*База индукции*). Здесь нечего доказывать, т. к. всякая функция из $\mathbf{T_0}$ по определению сохраняет нуль.

(*Шаг индукции*). Пусть $f(x_1, \ldots, x_n)$ — произвольная функция из $\mathbf{T_0}$ и $H_1, \ldots, H_n$ — переменные или формулы над $\mathbf{T_0}$ «уровня» $< k$, которые сохраняют нуль и

$$g(x_1, \ldots, x_s) = f(H_1, \ldots, H_n).$$

Тогда

$$g(\mathbf{0},\ldots,\mathbf{0}) = f(H_1|_{\tilde{\mathbf{0}}},\ldots,H_n|_{\tilde{\mathbf{0}}}) = f(\mathbf{0},\ldots,\mathbf{0}) = \mathbf{0}.$$

(Здесь через $H_i|_{\tilde{\mathbf{0}}}$ обозначено значение формулы или переменной H_i на нулевом наборе $\tilde{\mathbf{0}} = (\mathbf{0},\ldots,\mathbf{0})$).

Таким образом, $f(H_1,\ldots,H_n) \in \mathbf{T_0}$. По принципу индукции получаем, что все функции из $[\mathbf{T_0}]$ сохраняют нуль, т. е. $[\mathbf{T_0}] = \mathbf{T_0}$. ►

Ввиду замкнутости класса $\mathbf{T_0}$ и ввиду того, что существуют булевы функции, не сохраняющие нуль (см. примеры перед теоремой), то получаем, что $[\mathbf{T_0}] \neq \mathbb{BF}$. Иными словами, *класс функций* $\mathbf{T_0}$ *не является полным.*

Лемма 5.1. (О функциях, не сохраняющих нуль). *Функции, не сохраняющие нуль, принимают значение единица на нулевом наборе значений своих аргументов:*

$$\textit{если} \quad f \notin \mathbf{T_0}, \quad \textit{то} \quad f(\mathbf{0},\mathbf{0},\ldots,\mathbf{0}) = \mathbf{1}.$$

◄ Очевидно. ►

Лемма 5.2. *Число булевых функций f от n переменных $x_1,\ldots,x_n$, сохраняющих нуль, равно $\frac{1}{2}2^{2^n}$:*

$$|\mathbf{T_0} \cap \mathbb{BF}(n)| = \frac{1}{2}2^{2^n}.$$

◀ В словесной форме функции $f(x_1, \dots, x_n)$, сохраняющие нуль, имеют вид

$$f = [\![\mathbf{0}\alpha_1\alpha_2 \dots \alpha_{2^n-1}]\!],$$

где $\alpha_1, \alpha_2, \dots, \alpha_{2^n-1}$ есть $\mathbf{0}$ или $\mathbf{1}$. А число таких слов равно $2^{2^n-1} = \frac{1}{2}2^{2^n}$. ▶

5.2. Класс функций, сохраняющих единицу

Определение 5.2. Систему всех булевых функций, которые на единичном наборе своих аргументов принимают значение единица, обозначим через $\mathbf{T_1}$ и назовем *классом функций, сохраняющих единицу*. Таким образом,

$$\mathbf{T_1} :\stackrel{\text{def}}{=} \{\, f \in \mathbb{BF} \mid f(\mathbf{1}, \mathbf{1}, \dots, \mathbf{1}) = \mathbf{1}\}.$$

Пример 12. Проверка следующих утверждений тривиальна.

$$\begin{array}{llllll}
\text{Функций из класса } \mathbf{T_1}: & \mathbf{1}, & x & x \cdot y, & x \vee y, & x \to y, & x \leftrightarrow y, \\
\text{Функций не из класса } \mathbf{T_1}: & \mathbf{0}, & \bar{x}, & x - y, & x \oplus y, & x \downarrow y, & x \mid y.
\end{array}$$

Теорема 5.2. *Класс функций, сохраняющих единицу* $\mathbf{T_1}$, *замкнут:* $[\mathbf{T_1}] = \mathbf{T_1}$.

◀ Доказательство точно такое же (с очевидными изменениями), как и для случая класса $\mathbf{T_0}$.

Применим принцип индукции. В качестве свойства $\mathcal{P}$ берем теперь, конечно, свойство «булева функция f сохраняет единицу».

(*База индукции*). Здесь нечего доказывать, т. к. всякая функция из $\mathbf{T_1}$ по определению сохраняет единицу.

(*Шаг индукции*). Пусть $f(x_1, \dots, x_n)$ — произвольная функция из $\mathbf{T_1}$ и $H_1, \dots, H_n$ — переменные или формулы над $\mathbf{T_1}$ «уровня» $< k$, которые сохраняют единицу и

$$g(x_1, \dots, x_s) = f(H_1, \dots, H_n).$$

Тогда

$$g(\mathbf{1}, \dots, \mathbf{1}) = f(H_1|_{\tilde{\mathbf{1}}}, \dots, H_n|_{\tilde{\mathbf{1}}}) = f(\mathbf{1}, \dots, \mathbf{1}) = \mathbf{1}.$$

(Здесь через $H_i|_{\tilde{\mathbf{1}}}$ обозначено значение формулы или переменной H_i на единичном наборе $\tilde{\mathbf{1}} = (\mathbf{1}, \dots, \mathbf{1})$).

Таким образом, $f(H_1, \dots, H_n) \in \mathbf{T_1}$. По принципу индукции получаем, что все функции из $[\mathbf{T_1}]$ сохраняют единицу, т. е. $[\mathbf{T_1}] = \mathbf{T_1}$. ►

Ввиду замкнутости класса $\mathbf{T_1}$ и ввиду того, что существуют булевы функции, не сохраняющие единицу (см. примеры перед теоремой), то получаем, что $[\mathbf{T_1}] \neq \mathbb{BF}$. Иными словами, *класс функций* $\mathbf{T_1}$ *не является полным.*

Лемма 5.3. (О функциях, не сохраняющих единицу). *Функции, не сохраняющие единицу, принимают значение нуль на единичном наборе значений своих аргументов:*

$$\textit{если} \quad f \notin \mathbf{T_1}, \quad \textit{то} \quad f(\mathbf{1}, \mathbf{1}, \dots, \mathbf{1}) = \mathbf{0}.$$

◄ Очевидно. ►

Лемма 5.4. *Число булевых функций f от n переменных $x_1, \ldots, x_n$, сохраняющих единицу равно $\frac{1}{2}2^{2^n}$:*

$$|\,\mathbf{T_1} \cap \mathbb{BF}(n)\,| = \frac{1}{2}2^{2^n}.$$

◀ В словесной форме функции $f(x_1, \ldots, x_n)$, сохраняющие единицу имеют вид

$$f = [\![\alpha_0\alpha_1\alpha_2 \ldots \alpha_{2^n-2}\mathbf{1}]\!],$$

где $\alpha_0, \alpha_1, \ldots, \alpha_{2^n-2}$ есть $\mathbf{0}$ или $\mathbf{1}$. А число таких слов равно $2^{2^n-1} = \frac{1}{2}2^{2^n}$. ▶

5.3. Класс линейных функций

Определение 5.3. Булева функция $f(x_1, \ldots, x_n)$ называется *линейной*, если ее можно задать в виде

$$f(x_1, \ldots, x_n) = a_0 \oplus a_1x_1 \oplus a_2x_2 \oplus \ldots \oplus a_nx_n,$$

где $a_0, a_1, a_2, \ldots, a_n \in \mathbb{B} = \{\mathbf{0}, \mathbf{1}\}$.

Иными словами, можно сказать, что булева функция является линейной, если ее выражение в виде полинома Жегалкина не содержит монотонных конъюнкций ранга > 1.

Класс всех линейных булевых функций обозначим через $\mathbf{L}$.

Замечание 5.1. Отметим, что линейная булева функция

$$f : \mathbb{B}^n \to \mathbb{B}$$

— это обычная линейная функция, если рассматривать $\mathbb{B}^n$ как n-мерное линейное пространство над полем $\mathbb{B}$.

Пример 13. Проверить справедливость следующих утверждений

$$\begin{array}{lcccccc} \text{Функций из } \mathbf{L}: & \mathbf{0}, & \mathbf{1}, & x & \bar{x}, & x \leftrightarrow y, & x \oplus y. \\ \text{Функций не из } \mathbf{L}: & x \vee y, & x \cdot y, & x \to y & x - y & x \downarrow y, & x \,|\, y. \end{array}$$

Решение. Проверка состоит в представлении каждой из этих булевых функций в виде полинома Жегалкина:

$$\begin{aligned} \mathbf{0} &= \mathbf{0}, & x \vee y &= x \oplus y \oplus x \cdot y, \\ \mathbf{1} &= \mathbf{1}, & x \cdot y &= x \cdot y, \\ x &= x, & x - y &= x \oplus x \cdot y, \\ \bar{x} &= \mathbf{1} \oplus x, & x \to y &= \mathbf{1} \oplus x \oplus x \cdot y, \\ x \oplus y &= x \oplus y, & x \,|\, y &= \mathbf{1} \oplus x \oplus y \oplus x \cdot y, \\ & & x \downarrow y &= \mathbf{1} \oplus x \cdot y. \end{aligned}$$

Из этих представлений видим, что функции первого столбца являются линейными, а функции второго — нет. ►

Теорема 5.3. *Класс линейных функций* **L** *замкнут:* $[\mathbf{L}] = \mathbf{L}$.

◀ Докажем, что всякая формула над $\mathbf{L}$ является линейной, используя принцип индукции. В качестве свойства $\mathcal{P}$ возьмем свойство «булева функция f является линейной».

(*База индукции*). Здесь нечего доказывать, т. к. всякая функция из $\mathbf{L}$ по определению является линейной функцией.

(*Шаг индукции*). Пусть $f(x_1, \ldots, x_n)$ — произвольная функция из $\mathbf{L}$

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

и $H_1, \ldots, H_n$ — переменные или формулы над $\mathbf{L}$ «уровня» $< k$, которые являются линейными функциями. Рассмотрим функцию

$$f(H_1, \ldots, H_n) = a_0 \oplus a_1 H_1 \oplus \ldots \oplus a_n H_n.$$

Так как H_i есть либо переменная (заметим, что переменная является линейной функцией), либо линейная функция, то $a_i H_i$ продолжает оставаться линейной. А так как сумма линейных функций также есть линейная, то получаем, что $f(H_1, \ldots, H_n)$ является линейной функцией, что по принципу индукции завершает доказательство. ▶

Ввиду замкнутости класса линейных функций $\mathbf{L}$ и ввиду того, что существуют нелинейные булевы функции (см. примеры перед теоремой), то получаем, что $[\mathbf{L}] \neq \mathbb{BF}$. Иными словами, *класс линейных функций* $\mathbf{L}$ *не является полным.*

Лемма 5.5. ***(О нелинейных функциях).*** *Из любой нелинейной булевой функции $f(x_1, \ldots, x_n)$, подставляя вместо всех переменных $x_1, \ldots, x_n$ выражения $\mathbf{0}, \mathbf{1}, x, \bar{x}, y, \bar{y}$, можно получить $x \cdot y$ или $\overline{x \cdot y}$.*

◀ Пусть функция $f(x_1, \ldots, x_n)$ — нелинейная. Рассмотрим полином Жегалкина этой функции. Из ее нелинейности следует, что в нем присутствуют в качестве слагаемых монотонные конъюнкции ранга > 1 $x_{i_1}x_{i_2}\cdots$. Не ограничивая общности рассуждений, будем считать, что присутствует произведение вида $x_1x_2\cdots$. Таким образом, полином Жегалкина этой функции можно представить в виде:

$$\begin{gathered} f(x_1,\dots,x_n) = \\ = x_1x_2\cdot P_1(x_3,\dots,x_n)\oplus x_1\cdot P_2(x_3,\dots,x_n)\oplus x_2\cdot P_3(x_3,\dots,x_n)\oplus \\ \oplus P_3(x_3,\dots,x_n), \end{gathered}$$

причем $P_1(x_3,\dots,x_n)\not\equiv \mathbf{0}$. Последнее означает, что найдутся элементы $a_3,a_4,\dots,a_n\in\mathbb{B}=\{\mathbf{0},\mathbf{1}\}$ такие, что $P_1(a_3,\dots,a_n)=\mathbf{1}$. Рассмотрим вспомогательную функцию $\varphi(x_1,x_2)$, которая получается из $f(x_1,\dots,x_n)$ при подстановке вместо переменных $x_3,x_4,\dots,x_n$ эти найденные значения $a_3,a_4,\dots,a_n$:

$$\varphi(x_1,x_2)=f(x_1,x_2,a_3,a_4,\dots,a_n)=x_1\cdot x_2\cdot\mathbf{1}\oplus x_1\cdot b\oplus x_2\cdot c\oplus d,$$

где $b=P_2(a_3,\dots,a_n), c=P_3(a_3,\dots,a_n), d=P_4(a_3,\dots,a_n)$. Тогда, подставляя в функцию $f(x_1,\dots,x_n)$ вместо переменных $x_1,x_2,x_3,x_4,\dots,x_n$ соответсвенно $x\oplus c, y\oplus b, a_3,a_4,\dots,a_n$ и имея в виду, что

$$x\oplus\alpha=\begin{cases} x, & \text{если } \alpha=\mathbf{0};\\ \bar{x}, & \text{если } \alpha=\mathbf{1},\end{cases}$$

получаем

$$\begin{gathered} f(x\oplus c,y\oplus b,a_3,a_4,\dots,a_n)=\varphi(x\oplus c,y\oplus b)= \\ =(x\oplus c)\cdot(y\oplus b)\oplus(x\oplus c)\cdot b\oplus(y\oplus b)\cdot c\oplus d= \\ =x\cdot y\oplus x\cdot b\oplus y\cdot c\oplus b\cdot c\oplus x\cdot b\oplus b\cdot c\oplus y\cdot c\oplus b\cdot c\oplus d= \\ =x\cdot y\oplus(bc\oplus d)=\begin{cases} x\cdot y, & \text{если } bc\oplus d=\mathbf{0};\\ \overline{x\cdot y}, & \text{если } bc\oplus d=\mathbf{1}.\end{cases} \end{gathered}$$

Лемма доказана. ►

Лемма 5.6. *Число линейных булевых функций от переменных $x_1, \ldots, x_n$ равно 2^{n+1}:*

$$|\,\mathbf{L} \cap \mathbb{BF}(n)\,| = 2^{n+1}.$$

◀ Так как полином Жегалкина единственен для всякой булевой функции, то отображение

$$a_0 \oplus a_1x_1 \oplus a_2x_2 \oplus \ldots \oplus a_nx_n \longmapsto (a_0, a_1, a_2, \ldots, a_n)$$

является биективным отображением из множества $\mathbf{L} \cap \mathbb{BF}(n)$ на множество $\mathbb{B}^{n+1}$. Отсюда по правилу равенства получаем

$$|\,\mathbf{L} \cap \mathbb{BF}(n)\,| = |\mathbb{B}^{n+1}| = 2^{n+1}.$$

Лемма доказана. ▶

5.4. Класс самодвойственных функций

Определение 5.4. Булева функция $f(x_1, \ldots, x_n)$ называется *самодвойственной*, если

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

т. е.

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

Класс всех самодвойственных булевых функций обозначим через $\mathbf{S}$.

Пример 14. Проверить, справедливость следующих утверждений

$$\begin{array}{ll} \text{Функций из } \mathbf{S}: & x,\quad \bar{x},\quad x \oplus y \oplus z,\quad xy \vee yz \vee zx, \\ \text{Функций не из } \mathbf{S}: & \mathbf{0},\quad \mathbf{1},\quad x \vee y,\quad x \cdot y,\quad x - y,\quad x \to y,\quad x \downarrow y,\quad x \,|\, y. \end{array}$$

Решение. Напомним (см. стр. 46), что если булева функция $f(x_1, \ldots, x_n)$ имеет словесное представление

$$f = [\![\alpha_0\alpha_1 \ldots \alpha_{2^n-2}\alpha_{2^n-1}]\!],$$

то двойственная к ней функция $f^*(x_1, \ldots, x_n)$ имеет следующее «перевернутое с черточками» словесное представление

$$f^* = \overline{f(\bar{x}_1, \ldots, \bar{x}_n)} = [\![\bar{\alpha}_{2^n-1}\bar{\alpha}_{2^n-2} \ldots \bar{\alpha}_1\bar{\alpha}_0]\!].$$

Таким образом, $f(x_1, \ldots, x_n) = \overline{f(\bar{x}_1, \ldots, \bar{x}_n)}$ тогда и только тогда, когда $\alpha_0 = \bar{\alpha}_{2^n-1}, \alpha_1 = \bar{\alpha}_{2^n-2}, \ldots, \alpha_{2^n-2} = \bar{\alpha}_1, \alpha_{2^n-1} = \bar{\alpha}_0$; из чего приходим к выводу: для того чтобы булева функция $f(x_1, \ldots, x_n)$ была самодвойственной необходимо и достаточно, чтобы ее словесное представление было «зеркально-симметричным», т. е. имело вид:

$$f = [\![\alpha_0\alpha_1 \ldots \alpha_{k-1}\alpha_k\bar{\alpha}_k\bar{\alpha}_{k-1} \ldots \bar{\alpha}_1\bar{\alpha}_0]\!],$$

где $k = 2^{n-1} = 2^n/2$.

Теперь осталось представить в словесной форме проверяемые булевы функции и посмотреть, обладают ли эти словесные представления «зеркальной симметрией».

$$\begin{array}{rrr} x = [\![\mathbf{01}]\!], & \mathbf{0} = [\![\mathbf{00}]\!], & \mathbf{1} = [\![\mathbf{11}]\!], \\ \bar{x} = [\![\mathbf{10}]\!], & x \vee y = [\![\mathbf{0111}]\!], & x \wedge y = [\![\mathbf{0001}]\!], \\ x \oplus y \oplus z = [\![\mathbf{01101001}]\!], & x - y = [\![\mathbf{0010}]\!], & x \oplus y = [\![\mathbf{0110}]\!], \\ xy \vee yz \vee zx = [\![\mathbf{00010111}]\!], & x \to y = [\![\mathbf{1101}]\!], & x \leftrightarrow y = [\![\mathbf{1001}]\!], \\ & x \,|\, y = [\![\mathbf{1110}]\!], & x \downarrow y = [\![\mathbf{1000}]\!]. \end{array}$$

Как видим, функции первой колонки обладают свойством «зеркальной симметрии», а функции второй и третьей колонки не обладают этим свойством. ►

Теорема 5.4. *Класс самодвойственных функций* $\mathbf{S}$ *замкнут:* $[\mathbf{S}] = \mathbf{S}$.

◄ Докажем, что всякая формула над $\mathbf{S}$ является самодвойственной, используя принцип индукции. В качестве свойства $\mathcal{P}$ возьмем свойство «булева функция f является самодвойственной».

(*База индукции*). Здесь нечего доказывать, т. к. всякая функция из $\mathbf{S}$ по определению является самодвойственной функцией.

(*Шаг индукции*). Пусть $f(x_1, \ldots, x_n)$ — произвольная функция из $\mathbf{S}$ и $H_1, \ldots, H_n$ — переменные или формулы над $\mathbf{S}$ «уровня» $< k$, которые являются самодвойственными функциями. Рассмотрим функцию

$$g = f(H_1, \ldots, H_n).$$

Так как H_i есть либо переменная (заметим, что переменные являются самодвойственными функциями), либо самодвойственная функция, то $H_i^* = H_i$. А так как сама функция f также самодвойственна, то по принципу двойственности для булевых функций получаем, что

$$g^* = f^*(H_1^*, \ldots, H_n^*) = f(H_1, \ldots, H_n) = g,$$

т. е. $g = f(H_1, \ldots, H_n)$ также является самодвойственной функцией, что по принципу индукции завершает доказательство. ►

Ввиду замкнутости класса самодвойственных функций $\mathbf{S}$ и ввиду того, что существуют несамодвойственные булевы функции (см. примеры перед теоремой), то получаем, что $[\mathbf{S}] \neq \mathbb{BF}$. Иными словами, *класс самодвойственных функций* $\mathbf{S}$ *не является полным.*

Лемма 5.7. (О несамодвойственных функциях). *Из любой несамодвойственной булевой функции $f(x_1, \dots, x_n)$, подставляя вместо всех переменных $x_1, \dots, x_n$ выражения $x, \bar{x}$, можно получить постоянную булеву функцию $\mathbf{0}$ или $\mathbf{1}$.*

◀ Пусть функция f несамодвойственна, т. е. $\overline{f(\bar{x}_1, \dots, \bar{x}_n)} \neq f(x_1, \dots, x_n)$. Тогда найдется набор $\tilde{\sigma} = (\sigma, \dots, \sigma) \in \mathbb{B}^n$ такой, что

$$\overline{f(\bar{\sigma}_1, \dots, \bar{\sigma}_n)} \neq f(\sigma_1, \dots, \sigma_n).$$

Последнее равносильно тому, что

$$f(\bar{\sigma}_1, \dots, \bar{\sigma}_n) = f(\sigma_1, \dots, \sigma_n).$$

Далее, рассмотрим функцию $g(x) = f(x \oplus \sigma_1, \dots, x \oplus \sigma_n)$, которая, как следует из равенств

$$x \oplus \sigma = \begin{cases} x, & \text{если } \sigma = \mathbf{0}; \\ \bar{x}, & \text{если } \sigma = \mathbf{1}, \end{cases}$$

получается из $f(x_1, \dots, x_n)$ заменой переменных $x_1, \dots, x_n$ на выражения x или $\bar{x}$. Утверждаем, что эта функция постоянная. Действительно,

$$g(\mathbf{0}) = f(\sigma_1, \dots, \sigma_n) \quad \text{и} \quad g(\mathbf{1}) = f(\bar{\sigma}_1, \dots, \bar{\sigma}_n), \quad \text{т. е.} \quad g(\mathbf{0}) = g(\mathbf{1}).$$

Лемма доказана ▶

Лемма 5.8. *Число самодвойственных булевых функций f от n переменных $x_1, \dots, x_n$ равно $2^{2^{n-1}}$:*

$$|\, \mathbf{S} \cap \mathbb{BF}(n) \,| = 2^{2^{n-1}}.$$

◀ Как мы уже отмечали, словесное представление самодвойственной функции имеет вид $f = [\![\alpha_0\alpha_1\ldots\alpha_{k-1}\bar\alpha_{k-1}\ldots\bar\alpha_1\bar\alpha_0]\!]$, где $k = 2^n/2 = 2^{n-1}$. Поэтому отображение

$$[\![\alpha_0\alpha_1\ldots\alpha_{k-1}\bar\alpha_{k-1}\ldots\bar\alpha_1\bar\alpha_0]\!] \longmapsto (\alpha_0, \alpha_1, \ldots, \alpha_{k-1})$$

устанавливает биективное соответствие между множеством самодвойственных функций $\mathbf{S}$ от n переменных $x_1, \ldots, x_n$ и множеством $\mathbb{B}^k$ наборов $(\alpha_0, \alpha_1, \ldots, \alpha_{k-1})$ (здесь, $k = 2^n/2 = 2^{n-1}$). По правилу равенства отсюда получаем

$$|\,\mathbf{S} \cap \mathbb{BF}(n)\,| = |\mathbb{B}^k| = 2^k = 2^{2^{n-1}}.$$

Лемма доказана. ▶

5.5. Класс монотонных функций

Сначала напомним несколько обозначений. Для элементов из $\mathbb{B} = \{\mathbf{0}, \mathbf{1}\}$ полагаем $\mathbf{0} < \mathbf{1}$. Для элементов $\tilde\alpha = (\alpha_1, \ldots, \alpha_n), \tilde\beta = (\beta_1, \ldots, \beta_n)$ из $\mathbb{B}^n$

- $\tilde\alpha \preccurlyeq \tilde\beta$ означает, что $\alpha_1 \leqslant \beta_1, \ldots, \alpha_n \leqslant \beta_n$;
- $\tilde\alpha \prec \tilde\beta$ означает, что $\tilde\alpha \preccurlyeq \tilde\beta$ и $\tilde\alpha \neq \tilde\beta$;
- $\tilde\alpha \prec\cdot\, \tilde\beta$ означает, что $\tilde\alpha \prec \tilde\beta$ и n-мерные наборы $\tilde\alpha$ и $\tilde\beta$ различаются лишь одной компонентой, т. е.

$$\tilde\alpha \prec\cdot\, \tilde\beta \iff \begin{cases} \tilde\alpha = (\sigma_1, \ldots, \sigma_{k-1}, \mathbf{0}, \sigma_{k+1}, \ldots, \sigma_n), \\ \tilde\beta = (\sigma_1, \ldots, \sigma_{k-1}, \mathbf{1}, \sigma_{k+1}, \ldots, \sigma_n) \end{cases}$$

для некоторого $k, 1 \leqslant k \leqslant n$.

Определение 5.5. Булева функция $f(x_1, \ldots, x_n)$ называется *монотонной*, если для любых сравнимых $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ и $\tilde{\beta} = (\beta_1, \ldots, \beta_n)$ выполняется импликация

$$\text{если} \quad \tilde{\alpha} \preccurlyeq \tilde{\beta}, \quad \text{то} \quad f(\tilde{\alpha}) \leqslant f(\tilde{\beta}).$$

Класс всех монотонных булевых функций обозначим через $\mathbf{M}$.

Пример 15. Проверить справедливость следующих утверждений:

$$\begin{array}{llllllll} \text{Функций из } \mathbf{M}: & \mathbf{0}, & \mathbf{1}, & x, & x \cdot y, & x \vee y, & xy \vee yz \vee zx, & \\ \text{Функций не из } \mathbf{M}: & \bar{x}, & x \oplus y, & x \to y, & x \leftrightarrow y, & x - y, & x \downarrow y, & x \,|\, y. \end{array}$$

Теорема 5.5. *Класс монотонных функций* $\mathbf{M}$ *замкнут:*

$$[\mathbf{M}] = \mathbf{M}.$$

◀ Докажем, что всякая формула над $\mathbf{M}$ является монотонной, используя принцип индукции. В качестве свойства $\mathcal{P}(f)$ возьмем свойство «булева функция f является монотонной».

(*База индукции*). Здесь нечего доказывать, т. к. всякая функция из $\mathbf{M}$ по определению является монотонной функцией.

(*Шаг индукции*). Пусть $f(x_1, \ldots, x_n)$ — произвольная функция из $\mathbf{M}$ и $H_1, \ldots, H_n$ — переменные или формулы над $\mathbf{M}$ «уровня» $< k$, которые являются монотонными функциями. Рассмотрим функцию

$$g(x_1, \ldots, x_m) = f(H_1, \ldots, H_n).$$

Пусть далее $\tilde{\alpha} = (\alpha_1, \dots, \alpha_m)$ и $\tilde{\beta} = (\beta_1, \dots, \beta_m)$ произвольные m-мерные наборы такие, что $\tilde{\alpha} \preccurlyeq \tilde{\beta}$. Так как H_i есть либо переменная (заметим, что переменные являются монотонными функциями), либо монотонная функция, то

$$H_1|_{\tilde{\alpha}} \leqslant H_1|_{\tilde{\beta}}, \dots, H_n|_{\tilde{\alpha}} \leqslant H_n|_{\tilde{\beta}},$$

то есть

$$\left(H_1|_{\tilde{\alpha}}, \dots, H_n|_{\tilde{\alpha}}\right) \preccurlyeq \left(H_1|_{\tilde{\beta}}, \dots, H_n|_{\tilde{\beta}}\right),$$

где $H_i|_{\tilde{\alpha}}$ обозначено значение формулы или переменной H_i на наборе $\tilde{\alpha}$. Далее, т. к. функция $f(x_1, \dots, x_n)$ является монотонной, то

$$g(\tilde{\alpha}) = g(\alpha_1, \dots, \alpha_m) = f\left(H_1|_{\tilde{\alpha}}, \dots, H_n|_{\tilde{\alpha}}\right) \leqslant$$
$$\leqslant f\left(H_1|_{\tilde{\beta}}, \dots, H_n|_{\tilde{\beta}}\right) = g(\beta_1, \dots, \beta_m) = g(\tilde{\beta}).$$

Таким образом, функция $g(x_1, \dots, x_m) = f(H_1, \dots, H_n)$ является монотонной, что по принципу индукции завершает доказательство. ►

Ввиду замкнутости класса монотонных функций $\mathbf{M}$ и ввиду того, что существуют немонотонные булевы функции (см. примеры перед теоремой), получаем, что $[\mathbf{M}] \neq \mathbb{BF}$. Иными словами, *класс монотонных функций* $\mathbf{M}$ *не является полным.*

Лемма 5.9. (О немонотонных функциях). *Из любой немонотонной булевой функции $f(x_1, \dots, x_n)$ путем подстановки вместо всех переменных $x_1, \dots, x_n$ выражения* $\mathbf{0}, \mathbf{1}$ *и x можно получить булеву функцию отрицания $\varphi(x) = \bar{x}$.*

◀ Пусть $f(x_1, \ldots, x_n)\colon \mathbb{B}^n \to \mathbb{B}$ — немонотонная булева функция. Тогда найдутся такие n-мерные наборы $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ и $\tilde{\beta} = (\beta_1, \ldots, \beta_n)$ из $\mathbb{B}^n$, что

$$\tilde{\alpha} \prec \tilde{\beta}, \quad \text{но} \quad f(\tilde{\alpha}) > f(\tilde{\beta}),$$

и, значит, $f(\tilde{\alpha}) = \mathbf{1}$, а $f(\tilde{\beta}) = \mathbf{0}$. Пусть $i_1, i_2, \ldots, i_k\,(1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n)$ — это те индексы компонент, в которых различаются наборы $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ и $\tilde{\beta} = (\beta_1, \ldots, \beta_n)$, т. е. $\alpha_{i_1} \neq \beta_{i_1}, \alpha_{i_2} \neq \beta_{i_2}, \ldots, \alpha_{i_k} \neq \beta_{i_k}$. А т. к., по условию $\tilde{\alpha} < \tilde{\beta}$, то $\alpha_{i_1} < \beta_{i_1}, \alpha_{i_2} < \beta_{i_2}, \ldots, \alpha_{i_k} < \beta_{i_k}$, и, значит, $\alpha_{i_1} = \alpha_{i_2} = \ldots = \alpha_{i_k} = \mathbf{0}$, а $\beta_{i_1} = \beta_{i_2} = \ldots = \beta_{i_k} = \mathbf{1}$.

Рассмотрим теперь последовательность наборов из $\mathbb{B}^n$

$$\tilde{\alpha}_0, \tilde{\alpha}_1, \tilde{\alpha}_2, \ldots, \tilde{\alpha}_k,$$

построенную следующим образом:

$$\begin{array}{l} \tilde{\alpha}_0 = \tilde{\alpha}, \\ \tilde{\alpha}_1 \text{ получена из } \tilde{\alpha}_0 \text{ заменой } \alpha_{i_1} = \mathbf{0} \text{ на } \mathbf{1}, \\ \tilde{\alpha}_2 \text{ получена из } \tilde{\alpha}_1 \text{ заменой } \alpha_{i_2} = \mathbf{0} \text{ на } \mathbf{1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \tilde{\alpha}_k \text{ получена из } \tilde{\alpha}_{k-1} \text{ заменой } \alpha_{i_k} = \mathbf{0} \text{ на } \mathbf{1}. \end{array}$$

Из построения ясно, что

$$\tilde{\alpha} = \tilde{\alpha}_0 \prec \tilde{\alpha}_1 \prec \tilde{\alpha}_2 \prec \ldots \prec \tilde{\alpha}_k = \tilde{\beta}$$

и соседние наборы $\tilde{\alpha}_i$ и $\tilde{\alpha}_{i+1}$ отличаются только одной компонентой, т. е.

$$\tilde{\alpha} = \tilde{\alpha}_0 \prec\!\cdot\; \tilde{\alpha}_1 \prec\!\cdot\; \tilde{\alpha}_2 \prec\!\cdot\; \ldots \prec\!\cdot\; \tilde{\alpha}_k = \tilde{\beta}. \tag{5.1}$$

Далее, поскольку $f(\tilde{\alpha}) = \mathbf{1}$, а $f(\tilde{\beta}) = \mathbf{0}$, то среди наборов обязательно найдутся два соседних $\tilde{\alpha}_i$ и $\tilde{\alpha}_{i+1}$, такие, что $f(\tilde{\alpha}_i) = \mathbf{1}$, а $f(\tilde{\alpha}_{i+1}) = \mathbf{0}$ (в противном случае оказалось бы, что $f(\tilde{\beta}) = \mathbf{1}$). Пусть эти два набора $\tilde{\alpha}_i$ и $\tilde{\alpha}_{i+1}$ различаются r-ой компонентой:

$$\tilde{\alpha}_i = (\alpha_1, \alpha_2, \ldots, \alpha_{r-1}, \mathbf{0}, \alpha_r, \ldots, \alpha_n), \ \ \tilde{\alpha}_{i+1} = (\alpha_1, \alpha_2, \ldots, \alpha_{r-1}, \mathbf{1}, \alpha_r, \ldots, \alpha_n).$$

Рассмотрим функцию

$$\varphi(x) = f(\alpha_1, \alpha_2, \ldots, \alpha_{r-1}, x, \alpha_r, \ldots, \alpha_n),$$

которая получается из функции $f(x_1, \ldots, x_n)$ заменой $x_1, \ldots, x_n$ выражениями $\mathbf{0}, \mathbf{1}$ и x. Мы утверждаем, что $\varphi(x) = \bar{x}$. Действительно,

$$\varphi(\mathbf{0}) = f(\alpha_1, \alpha_2, \ldots, \alpha_{r-1}, \mathbf{0}, \alpha_{r+1}, \ldots, \alpha_n) = f(\tilde{\alpha}_i) = \mathbf{1},$$
$$\varphi(\mathbf{1}) = f(\alpha_1, \alpha_2, \ldots, \alpha_{r-1}, \mathbf{1}, \alpha_{r+1}, \ldots, \alpha_n) = f(\tilde{\alpha}_{i+1}) = \mathbf{0}.$$

Единственная булева функция одной переменной действующая так — это функция $\varphi(x) = \bar{x}$. ▶

Замечание 5.2. Далее по логике изложения, принятой автором, должна следовать лемма о количестве элементов в классе $\mathbf{M} \cap \mathbb{BF}(n)$. Но здесь, как говорится, «нашла коса на камень»: точная и приемлемая формула для числа монотонных булевых функций пока неизвестно (и вряд ли таковая существует). Задача подсчета числа монотонных булевых функций переменных называется проблемой Дедекинда. Подробное обсуждение этой проблемы выходит за рамки нашего учебного пособия. Мы ограничимся лишь констатацией результатов.

Введем обозначение: через $D(n)$ (в честь Дедекинда) обозначим количество монотонных функций от n переменных, т. е.

$$D(n) :\stackrel{\text{def}}{=} |\mathbf{M} \cap \mathbb{BF}(n)|.$$

История математических результатов для D(n):

- ✓ Уорд М. (M. Ward), 1946 г.,

$$D(n) > 2^{\binom{n}{\lfloor n/2 \rfloor}}.$$

- ✓ Ямамото К. (K. Yamamoto), 1953 г.,

$$D(n) \quad \text{является четным числом при четных} \quad n.$$

- ✓ Гилберт Е. (E. Gilbert), 1954 г.,

$$D(n) < n^{\binom{n}{\lfloor n/2 \rfloor}} + 2.$$

- ✓ Ямамото К. (K. Yamamoto), 1954 г.,

$$\log_2 D(n) < \binom{n}{\lfloor n/2 \rfloor} \left(1 + O(n^{-1})\right) \log_2 \sqrt{\frac{\pi n}{2}}.$$

- ✓ Коробков В. К., 1965 г.,

$$D(n) < 2^{4{,}24\binom{n}{\lfloor n/2 \rfloor}}.$$

- ✓ Ансель Ж. (G. Hansel), 1966 г.,

$$D(n) < 3^{\binom{n}{\lfloor n/2 \rfloor}}.$$

✓ Клейтман Д. (D. Kleitman), 1969 г.,

$$2^{(1+\alpha_n)\binom{n}{\lfloor n/2\rfloor}} \leqslant D(n) \leqslant 2^{(1+\beta_n)\binom{n}{\lfloor n/2\rfloor}},$$

где $\alpha_n = ce^{-n/4}$, $\beta_n = c'(\log n)/n^{1/2}$.

✓ Коршунов А. Д., 1981 г.,
(a) если $n \to \infty$ по четным числам, то

$$|\mathbf{M}(n)| \sim 2^{\binom{n}{n/2}} \exp\left\{\binom{n}{n/2-1}\left(\frac{1}{2^{n/2}} + \frac{n^2}{2^{n+5}} - \frac{n}{2^{n+4}}\right)\right\},$$

(b) если $n \to \infty$ по нечетным числам, то

$$|\mathbf{M}(n)| \sim 2\cdot 2^{\binom{n}{(n-1)/2}} \exp\left\{\binom{n}{(n-3)/2}\left(\frac{1}{2^{(n+3)/2}} - \frac{n^2}{2^{n+6}} - \frac{n}{2^{n+3}}\right)\right.$$

$$\left. + \binom{n}{(n-1)/2}\left(\frac{1}{2^{(n+1)/2}} + \frac{n^2}{2^{n+4}}\right)\right\}.$$

✓ Кисилевич А. (A. Kisielewicz), 1988 г.,

$$D(n) = \sum_{k=1}^{2^{2^n}} \prod_{j=1}^{2^n-1} \prod_{i=0}^{j-1} (1 - b_i^k b_j^k \prod_{m=0}^{\log_2 i} (1 - b_m^i + b_m^i b_m^j)),$$

где $b_i^k = \lfloor k/2^i \rfloor - 2\lfloor k/2^{i+1} \rfloor$.

История вычислений D(n):

- ✓ $D(2) = 3,$ Дедекинд Р., 1897 г.
- ✓ $D(3) = 6,$ Дедекинд Р., 1897 г.
- ✓ $D(3) = 20,$ Дедекинд Р., 1897 г.
- ✓ $D(4) = 168,$ Дедекинд Р., 1897 г.
- ✓ $D(5) = 7\,581,$ Черч Р. (R. Church), 1940 г.
- ✓ $D(6) = 7\,828\,354,$ Уорд М. (M. Ward), 1946 г.
- ✓ $D(7) = 2\,414\,682\,040\,998,$ Черч Р. (R. Church), 1940 г.
- ✓ $D(8) = 56\,130\,437\,228\,687\,557\,907\,788$ Вейдеман Д. (D. Wiedemann), 1991г.
- ✓ отметим также, что $D(9) > 10^{42}$.

Отметим, что существует метод записи формулы для любой «хорошо» определенной функции натурального аргумента ([12]). Так, используя этот метод, можно записать формулу для знаменитой функции $\pi(n)$, выражающей количество простых чисел, не превосходящих n:

$$\pi(n) = 2 + \sum_{s=4}^{n} \operatorname{sgn} \prod_{k=2}^{\sqrt{2}} \left(\frac{s}{n} - \left\lfloor \frac{s}{n} \right\rfloor \right).$$

Этим же методом получается точная формула Кисилевича для интересующей нас функции ([12]):

$$D(n) = \sum_{k=1}^{2^{2^n}} \prod_{j=1}^{2^n-1} \prod_{i=0}^{j-1} (1 - b_i^k b_j^k \prod_{m=0}^{\log_2 i} (1 - b_m^i + b_m^i b_m^j)), \tag{5.2}$$

где $b_i^k = \lfloor k/2^i \rfloor - 2\lfloor k/2^{i+1} \rfloor$.

Хотя эти формулы и не кажутся столь «страшными», но они малоинформативны: содержательно они являются всего лишь записями соответствующих определений, а вычислительный потенциал этих формул невелик — так по формуле (5.2) удалось подсчитать только значения до $D(5)$.

Далее приведем критерий монотонности булевой функции, представленной в виде слова.

Лемма 5.10. *Справедливы следующие утверждения*

1. *Для монотонности булевой функции* $f\colon \mathbb{B}^n \to \mathbb{B}$ *необходимо и достаточно выполнения условия: для всех* $\tilde{\alpha}, \tilde{\beta} \in \mathbb{B}^n$

$$f(\tilde{\alpha}) \leqslant f(\tilde{\beta}), \quad \text{если} \quad \tilde{\alpha} \prec\cdot \tilde{\beta}. \tag{5.3}$$

2. *Пусть функция* $f\colon \mathbb{B}^n \to \mathbb{B}$ *представлена словом* $f = [\![\sigma_0\sigma_1 \ldots \sigma_{2^n-1}]\!]$. *Для монотонности* f *необходимо и достаточно выполнение условия: для всех* k, $1 \leqslant k \leqslant n$

$$\sigma_i \leqslant \sigma_{i+2^{n-k}}, \quad \text{если} \quad \left\lfloor \frac{i}{2^{n-k+1}} \right\rfloor = \left\lfloor \frac{i+2^{n-k}}{2^{n-k+1}} \right\rfloor. \tag{5.4}$$

◀ 1. Необходимость очевидна. Докажем достаточность. По условию

$$\text{из}\quad \tilde{\alpha} \prec\cdot\, \tilde{\beta} \quad \text{следует} \quad f(\tilde{\alpha}) \leqslant f(\tilde{\beta})$$

для произвольных $\tilde{\alpha}, \tilde{\beta}$ из $\mathbb{B}^n$. Покажем, что для любых $\tilde{\alpha}, \tilde{\beta} \in \mathbb{B}^n$

$$\text{из}\quad \tilde{\alpha} \leqslant \tilde{\beta} \quad \text{следует} \quad f(\tilde{\alpha}) \leqslant f(\tilde{\beta}).$$

Пусть $\tilde{\alpha} \leqslant \tilde{\beta}$. Тогда, как показано в доказательстве леммы 5.9 о немонотонных функциях (см. равенство (5.1)), найдутся $\tilde{\alpha}_0, \tilde{\alpha}_1, \tilde{\alpha}_2, \ldots, \tilde{\alpha}_k \in \mathbb{B}^n$ такие, что

$$\tilde{\alpha} = \tilde{\alpha}_0 \prec\cdot\, \tilde{\alpha}_1 \prec\cdot\, \tilde{\alpha}_2 \prec\cdot\, \ldots \prec\cdot\, \tilde{\alpha}_k = \tilde{\beta}.$$

Поэтому, используя исходные условия, получаем

$$f(\tilde{\alpha}) = f(\tilde{\alpha}_0) \leqslant f(\tilde{\alpha}_1) \leqslant f(\tilde{\alpha}_2) \leqslant \ldots \leqslant f(\tilde{\alpha}_k) = f(\tilde{\beta}),$$

т. е. $f(\tilde{\alpha}) \leqslant f(\tilde{\beta})$. Что и требовалось показать.

2. Пусть $f = [\![\sigma_0\sigma_1 \ldots \sigma_{2^n-1}]\!]$ и $\tilde{\alpha}, \tilde{\beta} \in \mathbb{B}^n$. Тогда, согласно словесному представлению,

$$\text{если}\quad \nu(\tilde{\alpha}) = i \quad\text{и}\quad \nu(\tilde{\beta}) = j\,, \quad \text{то} \quad f(\tilde{\alpha}) = \sigma_i \quad\text{и}\quad f(\tilde{\beta}) = \sigma_j.$$

Далее, для $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n), \tilde{\beta} = (\beta_1, \ldots, \beta_n) \in \mathbb{B}^n$ по лемме 1.1 на стр. 16 имеем

$$\begin{cases} \tilde{\alpha} \prec\cdot\, \tilde{\beta}, \\ \alpha_k = \mathbf{0}, \beta_k = \mathbf{1} \end{cases} \Longleftrightarrow \begin{cases} \nu(\tilde{\beta}) = \nu(\tilde{\alpha}) + 2^{n-k}, \\ \left\lfloor \frac{\nu(\tilde{\beta})}{2^{n-k+1}} \right\rfloor = \left\lfloor \frac{\nu(\tilde{\alpha})}{2^{n-k+1}} \right\rfloor. \end{cases}$$

С учетом всего этого получаем, что для функции $f = [\![\sigma_0\sigma_1 \dots \sigma_{2^n-1}]\!]$ условие (5.3) равносильно условию
$$\sigma_i \leqslant \sigma_j, \quad \text{если} \quad \begin{cases} j = i + 2^{n-k}, \\ \left\lfloor \frac{j}{2^{n-k+1}} \right\rfloor = \left\lfloor \frac{i}{2^{n-k+1}} \right\rfloor, \end{cases}$$
т. е. условию
$$\sigma_i \leqslant \sigma_{i+2^{n-k}}, \quad \text{если} \quad \left\lfloor \frac{i}{2^{n-k+1}} \right\rfloor = \left\lfloor \frac{i+2^{n-k}}{2^{n-k+1}} \right\rfloor,$$
для любого k, $1 \leqslant k \leqslant n$. Это и доказывает требуемое утверждение. ▶

Основываясь на утверждении 2 предыдущей леммы, можно предложить следующий способ решения вопроса о монотонности булевой функции в случае, когда булева функция представлена словом.

Пусть булева функция f представлена словом $\sigma_0\sigma_1 \dots \sigma_{2^n-1}$. Разделим это слово «посередине» на два слова
$$\sigma_0\sigma_1 \dots \sigma_{2^{n-1}-1} \quad \text{и} \quad \sigma_{2^{n-1}}\sigma_{2^{n-1}+1} \dots \sigma_{2^n-1}.$$
Для удобства будем называть первое слово $\sigma_0 \dots \sigma_{2^{n-1}-1}$ *левой* половинкой (исходного слова) и переобозначим его через $\alpha_1\alpha_2 \dots \alpha_{2^{n-1}}$, а второе слово $\sigma_{2^{n-1}} \dots \sigma_{2^n-1}$ назовем *правой* половинкой (исходного слова) и переобозначим его через $\beta_1\beta_2 \dots \beta_{2^{n-1}}$. Далее мы будем сравнивать слова по правилу:
$$\alpha_1\alpha_2 \dots \alpha_k \preccurlyeq \beta_1\beta_2 \dots \beta_k,$$
если
$$(\alpha_1, \alpha_2, \dots, \alpha_k) \preccurlyeq (\beta_1, \beta_2, \dots, \beta_k),$$

т. е. если $\alpha_i \leqslant \beta_i$ для всех $i = 1, \ldots, k$.

Итак, разбиваем посередине слово $\sigma_0\sigma_1 \ldots \sigma_{2^n-1}$, представляющее булеву функцию f:

$$\alpha_1\alpha_2 \ldots \alpha_{2^{n-1}} \text{ (левая половинка) и } \beta_1\beta_2 \ldots \beta_{2^{n-1}} \text{ (правая половинка).}$$

Если

$$\text{«левая половинка»} \not\preccurlyeq \text{«правая половинка»},$$

т. е. если $\alpha_1\alpha_2 \ldots \alpha_{2^{n-1}} \not\preccurlyeq \beta_1\beta_2 \ldots \beta_{2^{n-1}}$, то функция f немонотонна. В противном случае, т. е., если

$$\text{«левая половинка»} \preccurlyeq \text{«правая половинка»},$$

то с каждой из половинок $\alpha_1\alpha_2 \ldots \alpha_{2^{n-1}}$ и $\beta_1\beta_2 \ldots \beta_{2^{n-1}}$ поступаем так же, как и с исходным словом.

Действуя таким образом, мы либо придем к выводу о немонотонности булевой функции f, либо получим, что при *всех описанных разбиениях*

$$\text{«левая половинка»} \preccurlyeq \text{«правая половинка»}.$$

В последнем случае функция f монотонна.

Говоря неформально, но зато коротко и выразительно, проверка монотонности булевой функции $f = [\![\sigma_0\sigma_1 \ldots \sigma_{2^n-1}]\!]$ сводится к правилу — дели пополам и сравнивай половинки: если всегда левая половинка $\preccurlyeq$ правой половинки, то f монотонна; в противном случае f немонотонна.

Пример 16. Является ли функция f монотонной, если

1) $f = [\![\mathbf{0001\,1101}]\!]$.

2) $f = [\![\mathbf{0101\,0111}]\!]$.

Решение. 1) Разбиваем слово **00011101** и сравниваем левую и правую половинки:

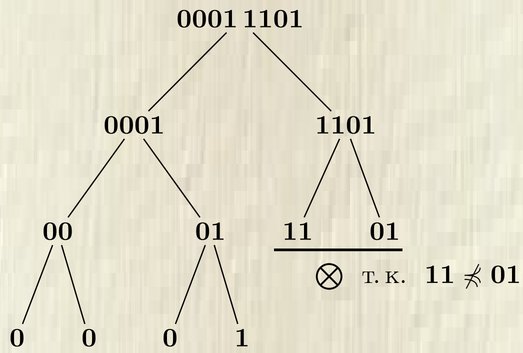
$$\mathbf{0001} \preccurlyeq \mathbf{1101}.$$

Разбиваем слова **0001**, **1101** и сравниваем половинки:

$$\mathbf{00} \preccurlyeq \mathbf{01}, \ \ \mathbf{11} \not\preccurlyeq \mathbf{01}.$$

Значит, f немонотонна.

Приведенные вычисления удобно организовать в виде двоичного дерева:



Сайт ДГУ
Тиульный лист
Оглавление
страница 134 из 158
Назад
Полный экран
Закрыть
Выход

2) Разбиваем слово **01010111** и сравниваем левую и правую половинки:

$$\mathbf{0101} \preccurlyeq \mathbf{0111}.$$

Разбиваем слова **0101**, **0111** и сравниваем половинки:

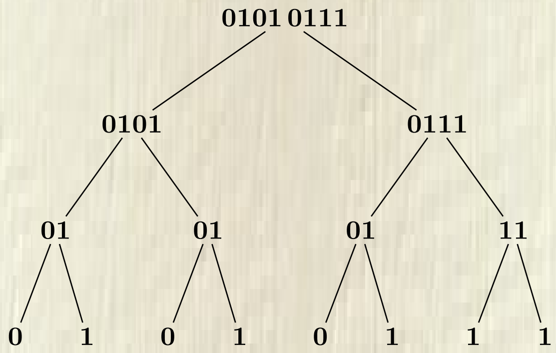
$$\mathbf{01} \preccurlyeq \mathbf{01}, \ \ \mathbf{01} \preccurlyeq \mathbf{11}.$$

Разбиваем слова **01**, **01**, **01**, **11** и сравниваем половинки:

$$\mathbf{0} \preccurlyeq \mathbf{1}, \ \mathbf{0} \preccurlyeq \mathbf{1}, \ \mathbf{0} \preccurlyeq \mathbf{1}, \ \mathbf{1} \preccurlyeq \mathbf{1}.$$

Значит, f монотонна.

Наглядно приведенные вычисления можно организовать в виде двоичного дерева:



Задача решена. ►

5.6. Классы Поста попарно различны

В этом пункте устанавливается только тот факт, что классы Поста $\mathbf{T_0}, \mathbf{T_1}, \mathbf{L}, \mathbf{S}, \mathbf{M}$ попарно различны. Как видно из следующей таблицы, чтобы установить это достаточно рассмотреть только три функции $\mathbf{0}, \mathbf{1}$ и $\bar{x}$.

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

Здесь знак «$+$» означает, что функция из строки принадлежит классу из столбца, а знак «$-$», что функция из строки не принадлежит соответствующему классу.

Однако нам в дальнейшем понадобится более сильное утверждение.

Лемма 5.11. *Если P и Q — два различных класса Поста, то в P найдется функция, не принадлежащая Q, и в Q найдется функция, не принадлежащая P.*

◀ Справедливость этой леммы подтверждает следующая таблица.

	$\mathbf{T_0}$	$\mathbf{T_1}$	$\mathbf{L}$	$\mathbf{S}$	$\mathbf{M}$
$\mathbf{0}$	$+$	$-$	$+$	$-$	$+$
$\mathbf{1}$	$-$	$+$	$+$	$-$	$+$
$\bar{x}$	$-$	$-$	$+$	$+$	$-$
$x \cdot y$	$+$	$+$	$-$	$-$	$+$
$x \oplus y \oplus z$	$+$	$+$	$+$	$+$	$-$
$xy \oplus yz \oplus zx$	$+$	$+$	$-$	$+$	$+$

Решающее свойство этой таблицы заключается в том, что в произвольных двух столбцах этой таблицы (соответствующих двум различным классам Поста), найдутся по крайней мере две строки (соответствующие функциям), в которых стоят $+\ -$ и $-\ +$. Так, например, $\mathbf{L} \setminus \mathbf{M} \neq \varnothing$ и $\mathbf{M} \setminus \mathbf{L} \neq \varnothing$, потому что $x \oplus y \oplus z \in \mathbf{L} \setminus \mathbf{M}$ и $x \cdot y \in \mathbf{M} \setminus \mathbf{L}$. Лемма доказана. ▶

5.7. Упражнения

1. Выяснить, принадлежит ли функция f множеству $\mathbf{T_1} \setminus \mathbf{T_0}$:

1) $f = (x_1 \to x_2)(x_2 \to x_3)(x_3 \to x_1)$;
2) $f = x_1 \to (x_2 \to (x_3 \to x_1))$;
3) $f = x_1x_2x_3 \vee \bar{x}_1x_2 \vee \bar{x}_2$;
4) $f = [\![\mathbf{10010110}]\!]$;
5) $f = [\![\mathbf{11011001}]\!]$;
6) $f = [\![\mathbf{00010010}]\!]$.

2. Выяснить, при каких n функция f принадлежит множеству $\mathbf{T_0} \setminus \mathbf{T_1}$:

1) $f = x_1 \oplus x_2 \oplus \ldots \oplus x_n$;
2) $f = \bigoplus\limits_{1 \leqslant i < j \leqslant n} x_ix_j$;
3) $f = \bigoplus\limits_{1 \leqslant i < j \leqslant n} (x_i \vee x_j)$;
4) $f = \mathbf{1} \oplus (x_1 \to x_2)(x_2 \to x_3)(x_3 \to x_4) \ldots$

$$\ldots(x_{n-1} \to x_n)(x_n \to x_1);$$

5) $f = \bigoplus_{i=1}^{n-2} (x_i \to (x_{i+1} \to x_{i+2}));$

6) $f = \bigoplus_{i=1}^{n-2} ((x_i \to x_{i+1}) \to x_{i+2}).$

7) $f = \bigoplus_{1 \leqslant i < j < k \leqslant n} m(x_i, x_j, x_k)$, где $m(x, y, z)$ — функция баллотировки (см. стр. 32);

3. Сколькими способами можно расставить скобки в выражении $x_1 \to x_2 \to x_1 \to x_2 \to x_1$, чтобы получилась формула, реализующая функцию из $\mathbf{T_0}$?

4. Представив функцию f полиномом, выяснить, является ли она линейной:

1) $f = x \to y;$
2) $f = \overline{x \to y} \oplus \bar{x}y;$
3) $f = x\bar{y}(x \leftrightarrow y);$
4) $f = xy \vee \bar{x}\bar{y} \vee z;$
5) $f = xy\bar{z} \vee x\bar{y};$
6) $f = m(x, y, z) \oplus \bar{x}\bar{y}\bar{z} \oplus xyz.$

5. Выяснить, является ли линейной функция f, заданная словом:

1) $f = [\![\mathbf{1001}]\!];$
2) $f = [\![\mathbf{1101}]\!];$
3) $f = [\![\mathbf{10010110}]\!];$
4) $f = [\![\mathbf{11000011}]\!];$
5) $f = [\![\mathbf{10100001}]\!];$
6) $f = [\![\mathbf{10100101}]\!].$

6. Заменить в «шаблоне»-функции прочерки символами $\mathbf{1}$ и $\mathbf{0}$ так, чтобы получилось словесное представление линейной функции f. Выразить f полиномом:

1) $f = \llbracket \mathbf{10 - 1} \rrbracket$;
2) $f = \llbracket \mathbf{0 - 11} \rrbracket$;
3) $f = \llbracket \mathbf{100 - - 0 - -} \rrbracket$;
4) $f = \llbracket \mathbf{-001 - -1-} \rrbracket$;
5) $f = \llbracket \mathbf{1 - 101 - - -} \rrbracket$;
6) $f = \llbracket \mathbf{-0 - 1 - - 00} \rrbracket$.

7. Подставляя на места переменных нелинейной функции f функции из множества $\{\mathbf{0}, \mathbf{1}, x, y\}$, получить хотя бы одну из функций $xy, x\bar{y}, \overline{xy}$:

1) $f = x_1x_2 \vee x_2\bar{x}_3 \vee \bar{x}_3x_1$;
2) $f = (x_1 \vee x_2 \vee x_3)(\bar{x}_1 \vee \bar{x}_2 \vee \bar{x}_3 \vee x_4)$;
3) $f = (x_1 \to x_3) \vee \overline{x_2x_3}$;
4) $f = \llbracket \mathbf{01100111} \rrbracket$;
5) $f = \llbracket \mathbf{11010101} \rrbracket$;
6) $f = \llbracket \mathbf{11001110} \rrbracket$.

8. Выяснить, является ли функция f самодвойственной:

1) $f = x_1x_2 \vee x_2x_3 \vee x_3x_1$;

2) $f = x_1 \oplus x_2 \oplus x_3 \oplus \mathbf{1}$;

3) $f = (x_1 \vee \bar{x}_2 \vee x_3)x_4 \vee x_1\bar{x}_2x_3$;

4) $f = x_1x_2 \vee x_3$;

5) $f = x_1x_2 \oplus x_2x_3 \oplus x_3x_1 \oplus x_2 \oplus x_3$.

9. Выяснить, является ли самодвойственной функция f, заданная с помощью слова:

1) $f = [\![\mathbf{1010}]\!]$;
2) $f = [\![\mathbf{1001}]\!]$;
3) $f = [\![\mathbf{01100110}]\!]$;
4) $f = [\![\mathbf{01110001}]\!]$;
5) $f = [\![\mathbf{01001101}]\!]$;
6) $f = [\![\mathbf{1100100101101100}]\!]$;
7) $f = [\![\mathbf{1110011100011000}]\!]$;
8) $f = [\![\mathbf{1000001110001100}]\!]$;
9) $f = [\![\mathbf{1001101110111001}]\!]$;
10) $f = [\![\mathbf{1100001110100101}]\!]$.

10. Заменить прочерки в «шаблоне»-функции символами **1** и **0** так, чтобы получилось словесное представление самодвойственной функции f:

1) $f = [\![\mathbf{1} - \mathbf{0} -]\!]$;
2) $f = [\![- \ \mathbf{01}-]\!]$;
3) $f = [\![\mathbf{01} - -]\!]$;
4) $f = [\![\mathbf{01} - \mathbf{0} - \mathbf{0} - -]\!]$;
5) $f = [\![- - \mathbf{01} - -\mathbf{11}]\!]$.

11. Определить, какие из переменных функции f следует заменить на x, а какие на $\bar{x}$ с тем, чтобы получить константу:

1) $f = [\![\mathbf{10110110}]\!]$;
2) $f = [\![\mathbf{11011000}]\!]$;
3) $f = [\![\mathbf{10100100}]\!]$;
4) $f = [\![\mathbf{10101000}]\!]$;
5) $f = [\![\mathbf{11001110}]\!]$.

12. Доказать, что если $f \in \mathbf{S}$, то $|N_f| = 2^{n-1}$. Привести пример, показывающий, что обратное утверждение неверно.

13. Выяснить, при каких n функция f является самодвойственной:

1) $f = x_1 \oplus x_2 \oplus \ldots \oplus x_n$;

2) $f = \bigvee\limits_{1 \leqslant i < j \leqslant n} x_i x_j$;

3) $f = \bigoplus\limits_{1 \leqslant i < j \leqslant n} x_i x_j$;

4) $f = (x_1 \vee x_2) \oplus (x_2 \vee x_3) \oplus \ldots \oplus (x_{n-1} \vee x_n) \oplus (x_n \vee x_1)$;

5) $f = (x_1 \to x_2)(x_2 \to x_3) \ldots (x_{n-1} \to x_n)(x_n \to x_1)$;

6) $f = (x_1 \to x_2) \oplus (x_2 \to x_3) \oplus \ldots \oplus (x_{n-1} \to x_n) \oplus$
$\oplus (x_n \to x_1) \oplus x_1 \oplus x_2 \oplus \ldots \oplus x_n$;

7) $f = \bigvee\limits_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} x_{i_1} x_{i_2} \ldots x_{i_k}, \quad 1 \leqslant k \leqslant n.$

14. Проверить, является ли функция f монотонной:

1) $f = (x_1 \oplus x_2) \wedge (x_1 \leftrightarrow x_2)$;

2) $f = x_1 \to (x_2 \to x_1)$;

3) $f = x_1 \to (x_1 \to x_2)$;

4) $f = x_1 \bar{x}_2 \bar{x}_3 \vee x_1 \bar{x}_2 x_3 \vee x_1 x_2 \bar{x}_3 \vee x_1 x_2 x_3 \vee \bar{x}_1 x_2 x_3$;

5) $f = x_1 \bar{x}_2 \bar{x}_3 \vee \bar{x}_1 x_2 x_3 \vee x_1 x_2 \bar{x}_3 \vee x_1 x_2 x_3 \vee \bar{x}_1 \bar{x}_2 x_3$;

6) $f = x_1 x_2 \oplus x_1 x_3 \oplus x_3 x_1$.

15. По словесному представлению булевой функции f выяснить, является ли она монотонной:

1) $f = [\![\mathbf{00110111}]\!]$;
2) $f = [\![\mathbf{01010111}]\!]$;
3) $f = [\![\mathbf{01100110}]\!]$;
4) $f = [\![\mathbf{00010111}]\!]$;
5) $f = [\![\mathbf{0010001101111111}]\!]$;
6) $f = [\![\mathbf{0001010101110111}]\!]$.

16. Для немонотонной функции f указать два соседних набора $\tilde{\alpha}, \tilde{\beta}$ значений переменных таких, что $\tilde{\alpha} < \tilde{\beta}$ и $f(\tilde{\alpha}) > f(\tilde{\beta})$:

a) $f = x_1x_2x_3 \vee \bar{x}_1x_2$;
b) $f = x_1 \oplus x_2 \oplus x_3$;
c) $f = x_1x_2 \oplus x_3$;
d) $f = x_1 \vee x_2\bar{x}_3$;
e) $f = x_1x_3 \oplus x_2x_4$;
f) $f = (x_1x_2x_4 \to x_2x_3) \oplus x_4$.

17. По данному «шаблону» булевой функции f определить сколькими способами можно вместо прочерков поставить символы **0** или **1** так, чтобы получилась монотонная функция:

1) $f = [\![--]\!]$;
2) $f = [\![-\ \mathbf{00}\ -]\!]$;
3) $f = [\![-\ \mathbf{10}\ -]\!]$;

4) $f = [\![- - - - - \mathbf{0}\mathbf{0} -]\!]$;

5) $f = [\![- - - \mathbf{1} - - \mathbf{0} -]\!]$;

6) $f = [\![- \mathbf{1} - - \mathbf{0} - - -]\!]$.

18. Выяснить, при каких $n \geqslant 1$ функция f, зависящая от n переменных, монотонна:

1) $f = x_1 \oplus x_2 \oplus \ldots \oplus x_n$;

2) $f = \bigoplus\limits_{1 \leqslant i < j \leqslant n} x_i x_j$;

3) $f = x_1 x_2 \ldots x_n \to (x_1 \oplus x_2 \oplus \ldots \oplus x_n)$;

4) $f = \bigoplus\limits_{m=1}^{n} \bigoplus\limits_{1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant n} x_{i_1} x_{i_2} \ldots x_{i_m}$.

19. Доказать, что функция $f \in \mathbb{BF}(n)$ монотонна тогда и только тогда, когда $f(\tilde{\alpha}) \leqslant f(\tilde{\alpha} \vee \tilde{\beta})$ для любых $\tilde{\alpha}, \tilde{\beta} \in \mathbb{B}^n$.

20. Доказать, что функция $f \in \mathbb{BF}(n)$ монотонна тогда и только тогда, когда $f(\tilde{\alpha} \wedge \tilde{\beta}) \leqslant f(\tilde{\alpha})$ для любых $\tilde{\alpha}, \tilde{\beta} \in \mathbb{B}^n$.

21. Доказать, что:

1) $\mathbf{L} \cap \mathbf{S} \cap \mathbf{T_0} = \mathbf{L} \cap \mathbf{S} \cap \mathbf{T_1} = \mathbf{L} \cap \mathbf{T_0} \cap \mathbf{T_1} = \mathbf{L} \cap \mathbf{S} \cap \mathbf{T_0} \cap \mathbf{T_1}$;

2) $\mathbf{S} \cap \mathbf{T_1} = \mathbf{S} \cap \mathbf{T_0} = \mathbf{S} \cap \mathbf{T_1} \cap \mathbf{T_0}$.

22. Подсчитать число функций, зависящих от n переменных $x_1, \dots, x_n$ и принадлежащих множеству A:

1) $A = \mathbf{T_0} \cap \mathbf{T_1}$;
2) $A = \mathbf{T_0} \cup \mathbf{T_1}$;
3) $A = \mathbf{T_0} \cap \mathbf{L}$;
4) $A = \mathbf{T_1} \cap \mathbf{S}$;
5) $A = \mathbf{T_0} \cup \mathbf{L}$;
6) $A = \mathbf{L} \cap \mathbf{T_1}$;
7) $(\mathbf{L} \cup \mathbf{T_1}) \cap \mathbf{S}$;
8) $\mathbf{T_0} \cap \mathbf{L} \cap \mathbf{S}$;
9) $\mathbf{T_0} \cup \mathbf{S} \cup \mathbf{L}$;
10) $(\mathbf{L} \cup \mathbf{S}) \setminus \mathbf{T_1}$;
11) $(\mathbf{L} \setminus \mathbf{T_0}) \cup \mathbf{S}$;
12) $(\mathbf{S} \cup \mathbf{T_0}) \cup \mathbf{T_1}$.
13) $(\mathbf{L} \cap \mathbf{S}) \setminus (\mathbf{T_0} \cup \mathbf{T_1})$;
14) $\mathbf{S} \setminus (\mathbf{L} \cup \mathbf{T_0} \cup \mathbf{T_1})$;
15) $(\mathbf{L} \cap \mathbf{S}) \setminus (\mathbf{T_0} \cap \mathbf{T_1})$;
16) $(\mathbf{L} \cap \mathbf{T_0}) \setminus (\mathbf{S} \cap \mathbf{T_1})$;
17) $(\mathbf{T_0} \cap \mathbf{T_1} \cap \mathbf{S}) \setminus \mathbf{L}$;
18) $(\mathbf{L} \setminus \mathbf{S}) \cup (\mathbf{T_0} \setminus \mathbf{T_1})$.

23. Подсчитать число функций, зависящих от n переменных $x_1, \dots, x_n$ и принадлежащих множеству A:

1) $A = \mathbf{M} \setminus (\mathbf{T_1} \cup \mathbf{T_0})$;
2) $A = \mathbf{M} \setminus (\mathbf{T_1} \cap \mathbf{T_0})$;
3) $A = \mathbf{L} \setminus (\mathbf{M} \cup \mathbf{S})$;
4) $A = \mathbf{M} \cap \mathbf{L}$;
5) $A = \mathbf{M} \cap \mathbf{L} \cap \mathbf{S}$.

6. Теорема Поста

6.1. Теорема Поста о полных системах функций

Теорема 6.1. (Теорема Поста о полноте). *Для того чтобы система булевых функций A являлась полной в $\mathbb{BF}$, необходимо и достаточно, чтобы она целиком не содержалась ни в одном из классов Поста* $\mathbf{T_0}, \mathbf{T_1}, \mathbf{L}, \mathbf{S}, \mathbf{M}$.

◀Необходимость. Пусть A — полная система. Через N обозначим любой из классов Поста $\mathbf{T_0}, \mathbf{T_1}, \mathbf{L}, \mathbf{S}, \mathbf{M}$. Так как классы $\mathbf{T_0}, \mathbf{T_1}, \mathbf{L}, \mathbf{S}, \mathbf{M}$ замкнуты и неполны, то $[N] = N \neq \mathbb{BF}$. Допустим, что $A \subseteq N$. Но тогда $[A] \subseteq [N]$, и, значит, $[A] \neq \mathbb{BF}$. Получили противоречие с полнотой класса A.

Достаточность. Пусть класс функций A не содержится целиком ни в одном из классов Поста $\mathbf{T_0}, \mathbf{T_1}, \mathbf{L}, \mathbf{S}, \mathbf{M}$, т. е.

$$A \nsubseteq \mathbf{T_0}, A \nsubseteq \mathbf{T_1}, A \nsubseteq \mathbf{L}, A \nsubseteq \mathbf{S}, A \nsubseteq \mathbf{M}.$$

Отсюда получаем, что найдутся пять функций в A, которые мы обозначим через $f_\mathbf{0}, f_\mathbf{1}, f_\mathbf{L}, f_\mathbf{S}$ и $f_\mathbf{M}$, такие, что

$$f_\mathbf{0} \notin \mathbf{T_0}, f_\mathbf{1} \notin \mathbf{T_1}, f_\mathbf{L} \notin \mathbf{L}, f_\mathbf{S} \notin \mathbf{S}, f_\mathbf{M} \notin \mathbf{M}.$$

Мы покажем, что система $\{f_\mathbf{0}, f_\mathbf{1}, f_\mathbf{L}, f_\mathbf{S}, f_\mathbf{M}\}$, состоящая из этих пяти функций, является полной в $\mathbb{BF}$. Из этого будет следовать и полнота класса A, содержащего эти функции:

$$[A] \supseteq [\{f_\mathbf{0}, f_\mathbf{1}, f_\mathbf{L}, f_\mathbf{S}, f_\mathbf{M}\}] = \mathbb{BF}, \quad \text{т. е.} \quad [A] = \mathbb{BF}\,.$$

Доказательство полноты системы $\{f_\mathbf{0}, f_\mathbf{1}, f_\mathbf{L}, f_\mathbf{S}, f_\mathbf{M}\}$ разобьем на три части: покажем, что отрицание $\bar{x}$ является функцией над $\{f_\mathbf{0}, f_\mathbf{1}, f_\mathbf{L}, f_\mathbf{S}, f_\mathbf{M}\}$, константы $\mathbf{0}$ и $\mathbf{1}$ являются функциями над $\{f_\mathbf{0}, f_\mathbf{1}, f_\mathbf{L}, f_\mathbf{S}, f_\mathbf{M}\}$ и конъюнкция $x \cdot y$ является функцией над $\{f_\mathbf{0}, f_\mathbf{1}, f_\mathbf{L}, f_\mathbf{S}, f_\mathbf{M}\}$.

(1) *Отрицание $\bar{x}$ является функцией над $\{f_\mathbf{0}, f_\mathbf{1}, f_\mathbf{L}, f_\mathbf{S}, f_\mathbf{M}\}$.* Возьмем булеву функцию $f_\mathbf{0}(x_1, \ldots, x_n) \notin \mathbf{T_0}$ и введем в рассмотрение функцию $\varphi_\mathbf{0}(x) = f_\mathbf{0}(x, x, \ldots, x)$. Так как функция $f_\mathbf{0}$ не сохраняет нуль, то $\varphi_\mathbf{0}(\mathbf{0}) = f_\mathbf{0}(\mathbf{0}, \mathbf{0}, \ldots, \mathbf{0}) = \mathbf{1}$. В таком случае для функции одной переменной $\varphi_\mathbf{0}(x)$ возможны два варианта: либо $\varphi_\mathbf{0}(x) = \bar{x}$, либо $\varphi_\mathbf{0}(x) \equiv \mathbf{1}$.

Рассмотрим теперь функцию $f_\mathbf{1}(x_1, \ldots, x_n) \notin \mathbf{T_1}$ и аналогично введем функцию $\varphi_\mathbf{1}(x) = f_\mathbf{1}(x, x, \ldots, x)$. Так как функция $f_\mathbf{1}$ не сохраняет единицу, то $\varphi_\mathbf{1}(\mathbf{1}) = f_\mathbf{1}(\mathbf{1}, \mathbf{1}, \ldots, \mathbf{1}) = \mathbf{0}$. Значит для функции одной переменной $\varphi_\mathbf{1}(x)$ возможны два варианта: либо $\varphi_\mathbf{1}(x) = \bar{x}$, либо $\varphi_\mathbf{1}(x) \equiv \mathbf{0}$.

Если хотя бы в одном из приведенных выше вариантов получилась функция отрицания $\bar{x}$, то пункт (1) завершен.

Если же в обоих случаях получились константы $\varphi_{\mathbf{0}}(x) \equiv \mathbf{1}$ и $\varphi_{\mathbf{1}}(x) \equiv \mathbf{0}$, то это означает, что константы являются функциями над $\{f_{\mathbf{0}}, f_{\mathbf{1}}, f_{\mathbf{L}}, f_{\mathbf{S}}, f_{\mathbf{M}}\}$. Но тогда согласно лемме о немонотонной функции, подставляя в немонотонную функцию $f_{\mathbf{M}}$ вместо всех переменных константы $\varphi_{\mathbf{0}}(x) \equiv \mathbf{1}, \varphi_{\mathbf{1}}(x) \equiv \mathbf{0}$ и x, можно получить отрицание.

Итак,при любом варианте получаем, что отрицание является формулой над системой $\{f_{\mathbf{0}}, f_{\mathbf{1}}, f_{\mathbf{L}}, f_{\mathbf{S}}, f_{\mathbf{M}}\}$. Пункт (1) показан.

(2) *Константы* $\mathbf{0}$ *и* $\mathbf{1}$ *являются функциями над* $\{f_{\mathbf{0}}, f_{\mathbf{1}}, f_{\mathbf{L}}, f_{\mathbf{S}}, f_{\mathbf{M}}\}$. Рассмотрим несамодвойственную функцию $f_{\mathbf{S}} \notin \mathbf{S}$. Согласно лемме о несамодвойственной функции, подставляя вместо всех переменных функции $f_{\mathbf{S}}$ функцию отрицания $\bar{x}$ и переменную x можно получить константы $\mathbf{0}$ и $\mathbf{1}$. Но мы в предыдущем пункте показали, что отрицание является формулой над $\{f_{\mathbf{0}}, f_{\mathbf{1}}, f_{\mathbf{L}}, f_{\mathbf{S}}, f_{\mathbf{M}}\}$. Значит константы являются формулами над $\{f_{\mathbf{0}}, f_{\mathbf{1}}, f_{\mathbf{L}}, f_{\mathbf{S}}, f_{\mathbf{M}}\}$. Пункт (2) показан.

(3) *Конъюнкция* $x \cdot y$ *является функцией над* $\{f_{\mathbf{0}}, f_{\mathbf{1}}, f_{\mathbf{L}}, f_{\mathbf{S}}, f_{\mathbf{M}}\}$. Рассмотрим нелинейную функцию $f_{\mathbf{L}} \notin \mathbf{L}$. Согласно лемме о нелинейной функции, подставляя вместо всех переменных функции $f_{\mathbf{L}}$ константы и отрицания, можно получить либо конъюнкцию $x \cdot y$, либо отрицание конъюнкции $\overline{x \cdot y}$. Однако ввиду того, что после первого пункта (1) у нас уже есть отрицание как формула над $\{f_{\mathbf{0}}, f_{\mathbf{1}}, f_{\mathbf{L}}, f_{\mathbf{S}}, f_{\mathbf{M}}\}$ и $\overline{\overline{x \cdot y}} = x \cdot y$, приходим к выводу, что конъюнкция $x \cdot y$ является формулой над $\{f_{\mathbf{0}}, f_{\mathbf{1}}, f_{\mathbf{L}}, f_{\mathbf{S}}, f_{\mathbf{M}}\}$. Пункт (3) показан.

Итак, мы установили, что $\{x \cdot y, \bar{x}\} \subseteq [\{f_{\mathbf{0}}, f_{\mathbf{1}}, f_{\mathbf{L}}, f_{\mathbf{S}}, f_{\mathbf{M}}\}]$. Вспоминая, что $\{x \cdot y, \bar{x}\}$ полная система в $\mathbb{BF}$, получаем

$$[\{f_{\mathbf{0}}, f_{\mathbf{1}}, f_{\mathbf{L}}, f_{\mathbf{S}}, f_{\mathbf{M}}\}] = [[\{f_{\mathbf{0}}, f_{\mathbf{1}}, f_{\mathbf{L}}, f_{\mathbf{S}}, f_{\mathbf{M}}\}]] \supseteq [\{x \cdot y, \bar{x}\}] = \mathbb{BF},$$

т. е. $[\{f_{\mathbf{0}}, f_{\mathbf{1}}, f_{\mathbf{L}}, f_{\mathbf{S}}, f_{\mathbf{M}}\}] = \mathbb{BF}$ и, значит, $\{f_{\mathbf{0}}, f_{\mathbf{1}}, f_{\mathbf{L}}, f_{\mathbf{S}}, f_{\mathbf{M}}\}$ — полная система. Доказательство завершено. ►

6.2. Упражнения

1. Выяснить, полна ли система функций:

1) $A = \{xy, x \vee y, x \oplus y, xy \vee yz \vee zx\}$;
2) $A = \{xy, x \vee y, x \oplus y \oplus x \oplus \mathbf{1}\}$;
3) $A = \{\mathbf{1}, \bar{x}, x(y \leftrightarrow z) \oplus \bar{x}(y \oplus z), x \leftrightarrow y\}$;
4) $A = \{\mathbf{0}, \bar{x}, x(y \vee z) \oplus yz\}$;
5) $A = \{\bar{x}, x(y \leftrightarrow z) \leftrightarrow (y \vee z), x \oplus y \oplus z\}$;
6) $A = \{\bar{x}, x(y \leftrightarrow z) \leftrightarrow yz, x \oplus y \oplus z\}$;
7) $A = \{xy(x \vee y), xy \oplus x \oplus y, \mathbf{1}, xy \oplus yz \oplus zx\}$;
8) $A = \{xy(x \oplus z), \mathbf{1}\}$;
9) $A = \{x \to y, \bar{x} \to \bar{y}x, x \oplus y \oplus z, \mathbf{1}\}$;
10) $A = \{x \to y, x \oplus y\}$.

2. Выяснить, полна ли система A булевых функций:

1) $A = \{f_1 = [\![\mathbf{0110}]\!], f_2 = [\![\mathbf{11000011}]\!], f_3 = [\![\mathbf{10010110}]\!]\}$;
2) $A = \{f_1 = [\![\mathbf{0111}]\!], f_2 = [\![\mathbf{01011010}]\!], f_3 = [\![\mathbf{01111110}]\!]\}$;
3) $A = \{f_1 = [\![\mathbf{0111}]\!], f_2 = [\![\mathbf{10010110}]\!]\}$;
4) $A = \{f_1 = [\![\mathbf{0101}]\!], f_2 = [\![\mathbf{11101000}]\!], f_3 = [\![\mathbf{01101001}]\!]\}$;
5) $A = \{f_1 = [\![\mathbf{1001}]\!], f_2 = [\![\mathbf{11101000}]\!]\}$;
6) $A = \{f_1 = [\![\mathbf{11}]\!], f_2 = [\![\mathbf{0111}]\!], f_3 = [\![\mathbf{00110111}]\!]\}$;

7) $A = \{f_1 = [\![\mathbf{10}]\!], f_2 = [\![\mathbf{00110111}]\!]\}$;

8) $A = \{f_1 = [\![\mathbf{11}]\!], f_2 = [\![\mathbf{00}]\!], f_3 = [\![\mathbf{00110101}]\!]\}$;

9) $A = \{f_1 = [\![\mathbf{10000001}]\!], f_2 = [\![\mathbf{0111}]\!], f_3 = [\![\mathbf{1011}]\!]\}$;

10) $A = \{f_1 = [\![\mathbf{10000001}]\!], f_2 = [\![\mathbf{0110}]\!], f_3 = [\![\mathbf{1001}]\!]\}$.

3. Выяснить, полна ли система функций $A = \{f_1, f_2\}$, если:

1) $f_1 \in \mathbf{S} \setminus \mathbf{M}$, $f_2 \notin \mathbf{L} \cup \mathbf{S}$, $f_1 \to f_2 = \mathbf{1}$;

2) $f_1 \notin \mathbf{L} \cup \mathbf{T_0} \cup \mathbf{T_1}$, $f_2 \in \mathbf{M} \cap \mathbf{L}$, $f_1 \to f_2 = \mathbf{1}$;

3) $f_1 \notin \mathbf{T_0} \cup \mathbf{L}$, $f_2 \notin \mathbf{S}$, $f_1 \to f_2 = \mathbf{1}$;

4) $f_1 \in (\mathbf{S} \cup \mathbf{L}) \setminus \mathbf{T_0}$, $f_2 \in \mathbf{M} \setminus (\mathbf{T_1} \cap \mathbf{L})$, $f_1 \to f_2 = \mathbf{1}$.

4. Выяснить, при каких n функция $f(x_1, \ldots, x_n)$ является шефферовой (т. е. образует полную систему функций):

1) $f = \mathbf{1} \oplus x_1x_2 \oplus \ldots \oplus x_ix_{i+1} \oplus \ldots \oplus x_{n-1}x_n \oplus x_nx_1$;

2) $f = \mathbf{1} \oplus x_1x_2 \oplus \ldots \oplus x_ix_{i+1} \oplus \ldots \oplus x_{n-1}x_n$;

3) $f = \mathbf{1} \oplus \bigvee\limits_{1 \leqslant i < j \leqslant n} \bar{x}_j\bar{x}_j$;

4) $f = \mathbf{1} \oplus (x_1 \to x_2) \oplus (x_2 \to x_3) \oplus \ldots \oplus (x_{n-1} \to x_1)$;

5) $f = (x_1 \,|\, x_2) \oplus (x_2 \,|\, x_3) \oplus \ldots \oplus (x_{n-1} \,|\, x_n) \oplus (x_n \,|\, x_1)$;

6) $f = (x_1 \,|\, x_2) \oplus (x_2 \,|\, x_3) \oplus \ldots \oplus (x_{n-1} \,|\, x_n)$;

7) $f = \mathbf{1} \oplus \bigoplus\limits_{1 \leqslant i < j \leqslant n} x_ix_j$.

5. Доказать, что, если f монотонна и зависит существенно не менее чем от двух переменных, то система $\{\mathbf{0}, \bar{f}\}$ полна.

6. Доказать, что если $f \notin \mathbf{T_0} \cup \mathbf{T_1} \cup \mathbf{S}$, то f — шефферова функция.

7. Подсчитать число шефферовых функций в $\mathbb{BF}(n)$.

8. Пусть A — множество функций из $\mathbb{BF}(n)$, $n \geqslant 2$ такое, что $|A| > \frac{1}{2} \cdot 2^{2^n}$. Доказать, что система A полна.

7. Теорема о числе функций в базисе и теорема о предполных классах

7.1. Теорема о максимальном числе функций в базисе

Напомним, что базисом (в $\mathbb{BF}$) мы называем такую полную (в $\mathbb{BF}$) систему булевых функций A, что при удалении из нее произвольной функции она перестает быть полной:

$$\text{система } A \text{ полная} \Longleftrightarrow \begin{cases} 1)\ [A] = \mathbb{BF}, \\ 2)\ [A \setminus \{f\}] \neq \mathbb{BF} \quad \text{для любого} \quad f \in A. \end{cases}$$

В следующей таблице приведены некоторые базисы, состоящие из одной, двух, трех и четырех функций.

базисы из 1-ой функции	базисы из 2-х функций	базис из 3-х функций	базис из 4-х функций
$\{x \downarrow y\}$	$\{x \vee y,\ \bar{x}\ \}$	$\{x \wedge y, x \oplus y, \mathbf{1}\}$	$\{\mathbf{0}, \mathbf{1}, x \wedge y, x \oplus y \oplus z\}$
$\{x \mid y\}$	$\{x \wedge y,\ \bar{x}\ \}$		
	$\{x \to y,\ \bar{x}\ \}$		

◀ В теореме 4.1 на стр. 106 мы доказали, что приведенные в таблице системы образуют полные системы булевых функций. Докажем теперь (как и было обещано в конце доказательства той теоремы), что эти системы функций образуют базис в $\mathbb{BF}$.

Системы из первой колонки очевидным образом образуют базис, т. к. выбрасывание единственной функции из этих систем приводит к пустому классу.

При доказательстве базисности остальных систем воспользуемся критерием Поста полноты систем функций: удаляя из приведенных систем какую-либо функцию мы покажем, что оставшиеся функции целиком лежат в некотором из классов Поста.

Для систем из второй, третьей и четвертой колонок имеем:

$\{x \vee y,\ \bar{x}\ \}$ базис, т. к. $\left\{\begin{array}{l} \{x \vee y,\ \bar{x}\ \} \setminus \{x \vee y\} = \{\ \bar{x}\ \} \subset \mathbf{L}, \\ \{x \vee y,\ \bar{x}\ \} \setminus \{\ \bar{x}\ \} = \{x \vee y\} \subset \mathbf{T_0}. \end{array}\right.$

$\{x \wedge y,\ \bar{x}\ \}$ базис, т. к. $\left\{\begin{array}{l} \{x \wedge y,\ \bar{x}\ \} \setminus \{x \wedge y\} = \{\ \bar{x}\ \} \subset \mathbf{L}, \\ \{x \wedge y,\ \bar{x}\ \} \setminus \{\ \bar{x}\ \} = \{x \wedge y\} \subset \mathbf{T_0}. \end{array}\right.$

$\{x \to y,\ \bar{x}\ \}$ базис, т. к. $\left\{\begin{array}{l} \{x \to y,\ \bar{x}\ \} \setminus \{x \to y\} = \{\ \bar{x}\ \} \subset \mathbf{L}, \\ \{x \to y,\ \bar{x}\ \} \setminus \{\ \bar{x}\ \} = \{x \to y\} \subset \mathbf{T_1}. \end{array}\right.$

$\{\mathbf{1}, x\wedge y, x\oplus y\}$ базис, т. к.

$$\left(\begin{array}{l} \{\mathbf{1}, x\wedge y, x\oplus y\}\setminus\{\mathbf{1}\} = \{x\wedge y, x\oplus y\}\subset \mathbf{T_0},\\ \{\mathbf{1}, x\wedge y, x\oplus y\}\setminus\{x\wedge y\} = \{\mathbf{1}, x\oplus y\}\subset \mathbf{L},\\ \{\mathbf{1}, x\wedge y, x\oplus y\}\setminus\{x\vee y\} = \{\mathbf{1}, x\wedge y\}\subset \mathbf{T_1}.\end{array}\right.$$

$\{\mathbf{0}, \mathbf{1}, x\wedge y, x\oplus y\oplus z\}$ базис, т. к.

$$\left(\begin{array}{l} \{\mathbf{0}, \mathbf{1}, x\wedge y, x\oplus y\oplus z\}\setminus\{\mathbf{0}\} = \{\mathbf{1}, x\wedge y, x\oplus y\oplus z\}\subset \mathbf{T_1},\\ \{\mathbf{0}, \mathbf{1}, x\wedge y, x\oplus y\oplus z\}\setminus\{\mathbf{1}\} = \{\mathbf{0}, x\wedge y, x\oplus y\oplus z\}\subset \mathbf{T_0},\\ \{\mathbf{0}, \mathbf{1}, x\wedge y, x\oplus y\oplus z\}\setminus\{x\wedge y\} = \{\mathbf{0}, \mathbf{1}, x\oplus y\oplus z\}\subset \mathbf{L},\\ \{\mathbf{0}, \mathbf{1}, x\wedge y, x\oplus y\oplus z\}\setminus\{x\oplus y\oplus z\} = \{\mathbf{0}, \mathbf{1}, x\wedge y\}\subset \mathbf{M}.\end{array}\right.$$

Тем самым базисность приведенных систем показана. ►

Оказывается, что базис в $\mathbb{BF}$ не может содержать более четырех функций.

Теорема 7.1. *Максимальное число функций в базисе равно четырем.*

◄ Покажем, что из произвольной полной в $\mathbb{BF}$ системы функций A можно всегда выделить полную в $\mathbb{BF}$ подсистему, содержащую не более четырех функций. Действительно, если A — полная в $\mathbb{BF}$ система, то согласно теореме Поста в ней найдутся пять функций $f_\mathbf{0}, f_\mathbf{1}, f_\mathbf{L}, f_\mathbf{S}$ и $f_\mathbf{M}$ такие, что

$$f_\mathbf{0}\notin \mathbf{T_0}, f_\mathbf{1}\notin \mathbf{T_1}, f_\mathbf{L}\notin \mathbf{L}, f_\mathbf{S}\notin \mathbf{S}, f_\mathbf{M}\notin \mathbf{M}.$$

По той же теореме Поста получаем, что система $\{f_\mathbf{0}, f_\mathbf{1}, f_\mathbf{L}, f_\mathbf{S}, f_\mathbf{M}\}$, состоящая из этих пяти функций является полной в $\mathbb{BF}$. Рассмотрим функцию $f_\mathbf{0}$. Так как $f_\mathbf{0}\notin \mathbf{T_0}$, то $f_\mathbf{0}(\mathbf{0}, \mathbf{0}, \ldots, \mathbf{0}) = \mathbf{1}$. Для этой функции возможны два случая.

1-й *случай.* $f_0(\mathbf{1},\mathbf{1},\ldots,\mathbf{1}) = \mathbf{1}$. В таком случае функция f_0 несамодвойственна. Действительно,

$$f_0^*(\mathbf{0},\mathbf{0},\ldots,\mathbf{0}) = \overline{f_0(\bar{\mathbf{0}},\bar{\mathbf{0}},\ldots,\bar{\mathbf{0}})} = \overline{f_0(\mathbf{1},\mathbf{1},\ldots,\mathbf{1})} = \bar{\mathbf{1}} = \\ = \mathbf{0} \neq \mathbf{1} = f_0(\mathbf{0},\mathbf{0},\ldots,\mathbf{0}).$$

Итак, $f_0 \notin \mathbf{S}$. Но тогда по теореме Поста система, состоящая из четырех функций $\{f_0, f_1, f_{\mathbf{L}}, f_{\mathbf{M}}\}$ полна в $\mathbb{BF}$.

2-й *случай.* $f_0(\mathbf{1},\mathbf{1},\ldots,\mathbf{1}) = \mathbf{0}$. В таком случае функция f_0 не только не сохраняет единицу, но и немонотонна. Действительно,

$$(\mathbf{0},\mathbf{0},\ldots,\mathbf{0}) < (\mathbf{1},\mathbf{1},\ldots,\mathbf{1}), \quad \text{но} \quad f_0(\mathbf{0},\mathbf{0},\ldots,\mathbf{0}) > f_0(\mathbf{1},\mathbf{1},\ldots,\mathbf{1}).$$

Итак, в этом случае $f_0 \notin \mathbf{T_1}$ и $f_0 \notin \mathbf{M}$. Снова по теореме Поста получаем тогда, что система, состоящая из трех функций $\{f_0, f_{\mathbf{L}}, f_{\mathbf{S}}\}$ полна в $\mathbb{BF}$.

Теорема полностью доказана. ►

7.2. Теорема о предполных классах

Выше мы могли видеть какую важную роль играют классы Поста $\mathbf{T_0}, \mathbf{T_1}, \mathbf{L}, \mathbf{S}, \mathbf{M}$ при изучении вопросов полноты систем функций. В этом пункте мы установим еще одно замечательное свойство классов Поста.

Как мы выяснили в параграфе 5, классы Поста являются замкнутыми неполными классами в $\mathbb{BF}$.

Напомним, что предполным мы назвали класс A, который сам неполон, но добавление любой новой булевой функции в этот класс превращает его в полный класс:

$$A \text{ — предполный класс} \iff \begin{cases} 1)\ [A] \neq \mathbb{BF}, \\ 2)\ [A \cup \{f\}] = \mathbb{BF} \ \text{ для любого } f \in \mathbb{BF} \setminus A. \end{cases}$$

Исключительная роль классов Поста состоит и в том, что они являются единственными предполными классами в $\mathbb{BF}$.

Теорема 7.2. *Классы Поста* $\mathbf{T_0}, \mathbf{T_1}, \mathbf{L}, \mathbf{S}, \mathbf{M}$ *являются единственными предполными классами в* $\mathbb{BF}$.

◀ Сначала докажем, что все классы Поста являются предполными. Пусть P обозначает любой из классов Поста $\mathbf{T_0}, \mathbf{T_1}, \mathbf{L}, \mathbf{S}, \mathbf{M}$, а P_1, P_2, P_3, P_4 оставшиеся классы Поста. Пусть, далее f — произвольная булева функция, не принадлежащая P. Тогда система $P \cup \{f\}$ не содержится ни в одном из классов Поста. Действительно, $P \cup \{f\}$ не содержится в классах P_1, P_2, P_3, P_4, т. к. по лемме 5.11 уже в классе P есть функции, не принадлежащие P_1, P_2, P_3, P_4; далее, система $P \cup \{f\}$ не содержится и в P, т. к. $f \notin P$. Раз $P \cup \{f\}$ не содержится ни в одном из классов Поста, то по теореме Поста $P \cup \{f\}$ — полная система.

Теперь докажем, что всякий предполный класс A совпадает с одним из классов $\mathbf{T_0}, \mathbf{T_1}, \mathbf{L}, \mathbf{S}, \mathbf{M}$. Раз система функций A является неполным классом, то по теореме Поста A целиком содержится в одном из классов $\mathbf{T_0}, \mathbf{T_1}, \mathbf{L}, \mathbf{S}, \mathbf{M}$. Обозначим через P тот из классов Поста, который содержит A: $A \subseteq P$. Допустим, что $A \neq P$. Тогда найдется булева функция f такая, что $f \in P$, но $f \notin A$. Теперь, с одной стороны $A \cup \{f\} \subseteq P$ и, значит, $[A \cup \{f\}] \subseteq [P] \neq \mathbb{BF}$; с другой стороны, ввиду того, что A — предполный класс имеем $[A \cup \{f\}] = \mathbb{BF}$. Полученное противоречие доказывает, что A обязан совпадать с одним из классов Поста. ▶

7.3. Упражнения

1. Проверить, является ли система функций A базисом в BF:

1) $A = \{x \to y, x \oplus y, x \vee y\}$;
2) $A = \{x \oplus y \oplus yz, x \oplus y \oplus \mathbf{1}\}$;
3) $A = \{x \oplus y \oplus z, x \vee y, \mathbf{0}, \mathbf{1}\}$;
4) $A = \{xy \vee z, xy \oplus z, xy \leftrightarrow z\}$;
5) $A = \{x \oplus y \oplus z, x \oplus y \oplus z \oplus \mathbf{1}, xy \oplus yz \oplus zx, \bar{x}\}$;
6) $A = \{x \oplus y \oplus z, xy \oplus yz \oplus zy, \mathbf{0}, \mathbf{1}\}$;
7) $A = \{x \oplus y, x \leftrightarrow yz\}$;
8) $A = \{xy \oplus yz \oplus zt, x \vee y, \mathbf{0}, \mathbf{1}\}$.

2. Из полной в $\mathbb{BF}$ системы A выделить всевозможные базисы:

1) $A = \{\mathbf{1}, \bar{x}, xy(x \oplus y), x \oplus y \oplus xy \oplus yz \oplus zx\}$;
2) $A = \{\mathbf{0}, x \oplus y, x \to y, xy \leftrightarrow xz\}$;
3) $A = \{\mathbf{0}, \mathbf{1}, x \oplus y \oplus z, xy \oplus xz \oplus yz, xy \oplus z, x \vee y\}$;
4) $A = \{zy, x \vee y, xy \vee z, x \oplus y, x \to y\}$;
5) $A = \{xy \oplus z, x \oplus y \oplus \mathbf{1}, x\bar{y}, \bar{x}\}$;
6) $A = \{xy \vee \bar{z}, \bar{x}, x \to y, \mathbf{0}, x \oplus zy\}$;
7) $A = \{xy, xy \vee z, x \oplus y, x \to y, \bar{x}\}$;
8) $A = \{x \oplus y, x \leftrightarrow y, x \oplus y \oplus z, xy, x \to y\}$.

3. Доказать, что в $\mathbb{BF}$ нет базисов, содержащих четыре функции.

Литература

1. *Гаврилов Г. П., Сапоженко А. А. Сборник задач по дискретной математике.* — М.: Наука, 1977.

2. *Алексеев В. Б. Дискретная математика.* — М., 2002.

3. *Белоусов А. И., Ткачев С. Б. Дискретная математика.* — М.: Изд-во МГТУ им. Н. Э. Баумана, 2004.

4. *Грэхем Р., Кнут Д., Паташник О. Конкретная математика.* — М.: Мир, 1998.

5. *Макоха А. Н., Сахнюк П. А., Червяков Н. И. Дискретная математика.* — М.: Физматлит, 2005.

6. *Судоплатов С. В., Овчинникова Е. В. Элементы дискретной математики.* — М.: ИНФРА-М, Новосибирск: Изд-во НГТУ, 2002.

7. *Фомичев В. М. Дискретная математика и криптология.* — М.: ДИАЛОГ-МИФИ, 2003.

8. *Чашкин А. В. Лекции по дискретной математике.* — М.: Изд-во МГУ, 2007.

9. *Логачев О. А., Сальников А. А., Ященко В. В. Булевы фукнции в теории кодирования и криптологии.* — М.: МЦНМОб, 2004

10. *Яблонский С. В. Введение в дискретную математику.* — 3-е изд. — М.: Высш. школа, 2001.

11. *Коршунов А. Д. Монотонные булевы функции* // Успехи математических наук, 58:5(353) (2003), 89–162

12. *Vollmer H., Wagner K. W. Recursion Theoretic Characterizations of Complexity Classes of Counting Functions* // Theoretical Computer Science, 163 1996, 245 — 258.

13. *Crama Y., Hammer L. P. Boolean Functions. Theory, Algorithms, and Applications.* — Cambridge: University Press, 2011.

Рагимханов Вадим Римиханович

Дискретная математика.
Часть IV.
Булевы функции

Учебное пособие

Издательство ДГУ
г. Махачкала, ул. М. Ярагского, 59^{e}

Email автора для отзывов и замечаний:
Отзывы и замечания

Сайт ДГУ

Тиульный лист

Оглавление

Назад

Полный экран

Закрыть

Выход