# МЛ и ТА (ИУ7), занятие 2

# **Полные системы булевых функций**

Д. А. Степанов

Напомним, что *булев куб* $\mathbb{B}^n$ размерности $n$ — это множество всех наборов длины $n$ из нулей и единиц:

$$\mathbb{B}^n = \{\tilde{\alpha} = (\alpha_1, \dots, \alpha_n) \,|\, \alpha_i = 0, 1,\ i = 1, \dots, n\}.$$

Элемент $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$ булева куба называется его *вершиной*, *булевым набором* или *булевым вектором*. Заметим, что булев куб $\mathbb{B}^m$ размерности $m$ можно многими способами отобразить в булев куб $\mathbb{B}^n$ размерности $n$. В качестве стандартного отображения $\mathbb{B}^m$ в $\mathbb{B}^n$ будем рассматривать любое из отображений вида

$$\mathbb{B}^m \ni \tilde{\alpha} = (\alpha_1, \dots, \alpha_m) \mapsto (\alpha_{i_1}, \dots, \alpha_{i_n}) \in \mathbb{B}^n,$$

где $(i_1, \dots, i_n)$ — некоторый фиксированный кортеж длины $n$ из чисел $1, \dots, m$. Например, существует лишь одно отображение такого вида булева куба $\mathbb{B}^1$ в булев куб $\mathbb{B}^n$ для любого $n$: оно определяется формулой

$$\mathbb{B}^1 \ni x \mapsto (\underbrace{x, x, \dots, x}_{n}) \in \mathbb{B}^n,$$

в то время как имеется $n$ отображений в обратную сторону:

$$\mathbb{B}^n \ni (x_1, x_2, \dots, x_n) \mapsto x_i \in \mathbb{B}^1, \quad i = 1, 2, \dots, n.$$

*Булева функция* от $n$ переменных — это отображение $f\colon \mathbb{B}^n \to \mathbb{B}$ из булева куба $\mathbb{B}^n$ в множество $\mathbb{B} = \{0, 1\}$. Система булевых функций $f_1, \dots, f_k$ называется *полной*, если любая булева функция $f$ допускает представление в виде суперпозиции функций системы $f_1, \dots, f_k$ и стандартных отображений, описанных выше. Проще говоря, для выражения функции $f$ разрешается подставлять функции $f_1, \dots, f_k$ друг в друга и подставлять в них любые переменные. Эквивалентным образом понятие полной системы может быть определено через понятие *формулы над системой* $f_1, \dots, f_k$, см. [БТ, п. 6.7].

*Задача* 1. Докажите (или найдите соответствующее место в [БТ]), не используя теоремы Поста, что система $\{\cdot, \vee, ^-\}$ ($\cdot$ — конъюнкция, $\vee$ — дизъюнкция, $^-$ — отрицание) полна. Она называется *стандартным базисом* в множестве булевых функций. Покажите затем, что полными будут и меньшие системы $\{\cdot, ^-\}$ и $\{\vee, ^-\}$.

Для исследования систем булевых функций на полноту используются специальные множества булевых функций, называемые *классами Поста*. Булева функция $f\colon \mathbb{B}^n \to \mathbb{B}$ называется

- *сохраняющей нуль*, если $f(0,0,\ldots,0)=0$; класс всех булевых функций, сохраняющих нуль, обозначается $T_0$;
- *сохраняющей единицу*, если $f(1,1,\ldots,1)=1$; класс функций, сохраняющих единицу, обозначается $T_1$;
- *самодвойственной*, если

  $$\forall \tilde{\alpha} \in \mathbb{B}^n \; f(\bar{\tilde{\alpha}}) = \overline{f(\tilde{\alpha})},$$

  где $\bar{\tilde{\alpha}}$ обозначает противоположную вершину, т. е.

  $$\text{если } \tilde{\alpha} = (\alpha_1,\ldots,\alpha_n), \text{ то } \bar{\tilde{\alpha}} = (\bar{\alpha}_1,\ldots,\bar{\alpha}_n);$$

  класс самодвойственных функций обозначается $S$;
- *монотонной*, если она монотонно не убывает относительно *булева порядка*, т. е. если $\tilde{\alpha} \leqslant \tilde{\beta}$, то $f(\tilde{\alpha}) \leqslant f(\tilde{\beta})$; булев порядок предполагает, что $0 \leqslant 1$ и

  $$\tilde{\alpha} \leqslant \tilde{\beta} \Leftrightarrow \alpha_i \leqslant \beta_i, \quad i = 1,\ldots,n;$$

  класс монотонных функций обозначается $M$;
- *линейной*, если она представляется полиномом Жегалкина степени 1; *полином Жегалкина* — это формула над базисом $\{\oplus,\cdot,1\}$, где $\oplus$ — плюс по модулю 2 а 1 — функция, тождественно равная 1; эквивалентно, полином Жегалкина — это выражение вида

  $$\sum_{\{i_1,\ldots,i_m\}\subseteq\{1,\ldots,n\}} a_{i_1\ldots i_m} x_{i_1}\ldots x_{i_n} =$$

  $$= a_0 \oplus a_1x_1 \oplus \cdots \oplus a_nx_n \oplus a_{12}x_1x_2 \oplus a_{13}x_1x_3 \oplus \cdots \oplus a_{n-1,n}x_{n-1}x_n \oplus$$

  $$\oplus \cdots \oplus a_{12\ldots n}x_1x_2\ldots x_n,$$

  $a_{i_1\ldots i_m} \in \mathbb{B}$; полином Жегалкина степени 1 — выражение вида

  $$a_0 \oplus a_1x_1 \oplus \cdots \oplus a_nx_n;$$

  класс линейных функций обозначается $L$.

Можно показать (см. [БТ, Пример 6.17]), что базис Жегалкина $\{\oplus,\cdot,1\}$ также представляет собой полную систему булевых функций. В дальнейшем плюс по модулю 2 будем обозначать просто $+$.

*Пример* 1. Проверим, принадлежит ли к каким-то из классов Поста булева функция $f(x_1, x_2, x_3)$, заданная таблицей

| $N$ | $x_1$ | $x_2$ | $x_3$ | $f$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 1 | 1 |
| 2 | 0 | 1 | 0 | 1 |
| 3 | 0 | 1 | 1 | 0 |
| 4 | 1 | 0 | 0 | 1 |
| 5 | 1 | 0 | 1 | 0 |
| 6 | 1 | 1 | 0 | 0 |
| 7 | 1 | 1 | 1 | 0 |

Непосредственно из таблицы мы видим, что $f(0,0,0) = 0$, $f(1,1,1) = 0$, следовательно $f \in T_0$, но $f \notin T_1$. Булевы векторы $(0,0,0)$ и $(1,1,1)$ противоположны, но $f(0,0,0) = f(1,1,1) = 0$, значит $f$ не является самодвойственной, $f \notin S$. Набор $(0,0,1)$ меньше относительно булева порядка набора $(0,1,1)$, но $f(0,0,1) = 1 > 0 = f(0,1,1)$, следовательно, $f$ и не монотонна, $f \notin M$.

Проверка линейности наиболее трудоёмка и требует построения полинома Жегалкина для функции $f$. Общий полином Жегалкина от трёх переменных выглядит следующим образом.

$$Z = a_0 + a_1x_1 + a_2x_2 + a_3x_3 + a_{12}x_1x_2 + a_{13}x_1x_3 + a_{23}x_2x_3 + a_{123}x_1x_2x_3 \quad (1)$$

Подберём коэффициенты $a$ таким образом, чтобы при всех значениях переменных значения функции $f$ и данного полинома Жегалкина совпадали. Коэффициенты легко подбираются, если следовать непосредственно таблице значений функции. Имеем

$$\begin{aligned}
&x_1 = x_2 = x_3 = 0\colon && f = 0,\ Z = a_0 \Rightarrow \underline{a_0 = 0};\\
&x_1 = x_2 = 0, x_3 = 1\colon && f = 1,\ Z = a_0 + a_3 = a_3 \Rightarrow \underline{a_3 = 1};\\
&x_1 = 0, x_2 = 1, x_3 = 0\colon && f = 1,\ Z = a_0 + a_2 = a_2 \Rightarrow \underline{a_2 = 1};\\
&x_1 = 0, x_2 = x_3 = 1\colon && f = 0,\ Z = a_0 + a_2 + a_3 + a_{23} = a_{23} \Rightarrow \underline{a_{23} = 0};\\
&x_1 = 1, x_2 = x_3 = 0\colon && f = 1,\ Z = a_0 + a_1 = a_1 \Rightarrow \underline{a_1 = 1};\\
&x_1 = 1, x_2 = 0, x_3 = 1\colon && f = 0,\ Z = a_0 + a_1 + a_3 + a_{13} = a_{13} \Rightarrow \underline{a_{13} = 0};\\
&x_1 = x_2 = 1, x_3 = 0\colon && f = 0,\ Z = a_0 + a_1 + a_2 + a_{12} = a_{12} \Rightarrow \underline{a_{12} = 0};\\
&x_1 = x_2 = x_3 = 1\colon && f = 0,\ Z = a_0 + a_1 + a_2 + a_3 + a_{12} + a_{13} + a_{23} + a_{123} =\\
& && \qquad = 1 + a_{123} \Rightarrow \underline{a_{123} = 1}.
\end{aligned}$$

Отсюда следует, что

$$f(x_1, x_2, x_3) = x_1 + x_2 + x_3 + x_1x_2x_3.$$

Поскольку в полиноме Жегалкина присутствует член третьей степени $x_1x_2x_3$, функция $f$ не линейна, $f \notin L$. Таким образом, булева функция $f$ содержится лишь в одном из классов Поста — $T_0$. †

Критерием полноты системы булевых функций служит следующая теорема Поста.

**Теорема 1.** *Система булевых функций полна тогда и только тогда, когда она не содержится ни в одном из пяти классов Поста $T_0$, $T_1$, $S$, $M$, $L$.*

Следующий пример можно использовать как образец для решения задачи о полных системах булевых функций из стендового домашнего задания.

*Пример* 2. Выясним, полна ли система булевых функций $\{f, w\}$, где $f$ задана формулой

$$f(x_1, x_2, x_3) = \overline{x}_1 \to \big((x_1 \vee x_2 \vee x_3)(x_2 \to x_3)\big),$$

в которой $\to$ обозначает импликацию, а $w$ задана вектором значений

$$w = (10010110).$$

Если система полна, выразим через неё функции $\cdot$ и $\bar{\ }$ стандартного базиса и реализуем их схемами из функциональных элементов.

Для начала построим таблицу функций $f$ и $w$. Для вычисления значений функции $f$ удобно представить её как суперпозицию $f = f_3 \to f_4$, $f_3 = \overline{x}_1$, $f_4 = f_1 \cdot f_2$, $f_1 = x_1 \vee x_2 \vee x_3$, $f_2 = x_2 \to x_3$.

| $N$ | $x_1$ | $x_2$ | $x_3$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f$ | $w$ |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |
| 2 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 |
| 3 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 4 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 |
| 5 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 |
| 6 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |
| 7 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 |

Непосредственно из таблицы видно, что $f \in T_0$, $f \in T_1$, $w \notin T_0$, $w \notin T_1$. Булев вектор $(0,0,1)$ противоположен вектору $(1,1,0)$, но в то же время $f(0,0,1) = f(1,1,0) = 1$. Это показывает, что функция $f$ не является самодвойственной, $f \notin S$. Рассматривая все пары противоположных наборов, убеждаемся, что функция $w$ на всех таких парах принимает противоположные значения: $w(0,0,0) = 1$, но $w(1,1,1) = 0$, $w(0,0,1) = 0$, но $w(1,1,0) = 1$ и т. д. Таким образом, $w \in S$.

Проверка монотонности также несложно осуществляется по таблице. Скажем, $(0,0,0) < (0,0,1)$, но $w(0,0,0) = 1 > 0 = w(0,0,1)$, следовательно, функция $w$ не монотонна, $w \notin M$. Функция $f$, однако, оказывается монотонной. Для наглядности можно построить диаграмму Хассе булева порядка на булевом кубе $\mathbb{B}^3$, отметив на ней также значения функции $f$ (рис. 1).

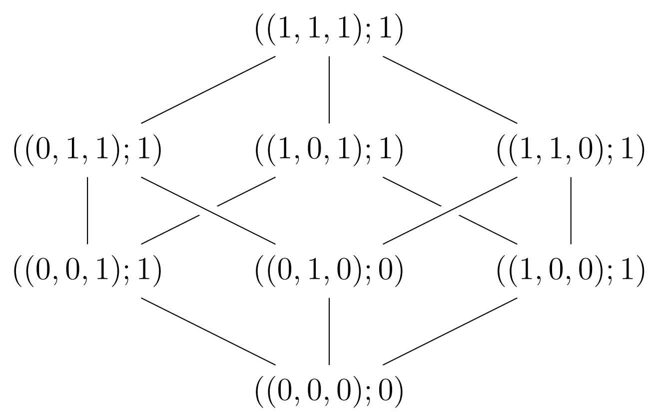


Рис. 1: Диаграмма Хассе булева порядка на $\mathbb{B}^3$; число при вершине — значение функции $f$

Из рис. 1 видно, что условие монотонности функции $f$ выполнено на любой паре сравнимых наборов. Значит, $f \in M$.

Перейдём к построению полиномов Жегалкина, которые представляют функции $f$ и $w$. Так как и $f$, и $w$ зависят от трёх переменных, полиномы Жегалкина ищем снова в виде (1) Для функции $f$ имеем:

$$
\begin{array}{ll}
x_1 = x_2 = x_3 = 0\colon & f = 0,\ Z = a_0 \Rightarrow \underline{a_0 = 0};\\
x_1 = x_2 = 0, x_3 = 1\colon & f = 1,\ Z = a_0 + a_3 = a_3 \Rightarrow \underline{a_3 = 1};\\
x_1 = 0, x_2 = 1, x_3 = 0\colon & f = 0,\ Z = a_0 + a_2 = a_2 \Rightarrow \underline{a_2 = 0};\\
x_1 = 0, x_2 = x_3 = 1\colon & f = 1,\ Z = a_0 + a_2 + a_3 + a_{23} = 1 + a_{23} \Rightarrow \underline{a_{23} = 0};
\end{array}
$$

$$
\begin{aligned}
&x_1 = 1, x_2 = x_3 = 0\colon && f = 1,\ Z = a_0 + a_1 = a_1 \Rightarrow \underline{a_1 = 1};\\
&x_1 = 1, x_2 = 0, x_3 = 1\colon && f = 1,\ Z = a_0 + a_1 + a_3 + a_{13} = a_{13} \Rightarrow \underline{a_{13} = 1};\\
&x_1 = x_2 = 1, x_3 = 0\colon && f = 1,\ Z = a_0 + a_1 + a_2 + a_{12} = 1 + a_{12} \Rightarrow \underline{a_{12} = 0};\\
&x_1 = x_2 = x_3 = 1\colon && f = 1,\ Z = a_0 + a_1 + a_2 + a_3 + a_{12} + a_{13} + a_{23} + a_{123} =\\
& && \qquad = 1 + a_{123} \Rightarrow \underline{a_{123} = 0}.
\end{aligned}
$$

Отсюда следует, что

$$
f(x_1, x_2, x_3) = x_1 + x_3 + x_1x_3, \tag{2}
$$

и функция $f$, таким образом, не линейна, $f \notin L$.

Для функции $w$ получаем:

$$
\begin{aligned}
&x_1 = x_2 = x_3 = 0\colon && w = 1,\ Z = a_0 \Rightarrow \underline{a_0 = 1};\\
&x_1 = x_2 = 0, x_3 = 1\colon && w = 0,\ Z = a_0 + a_3 = 1 + a_3 \Rightarrow \underline{a_3 = 1};\\
&x_1 = 0, x_2 = 1, x_3 = 0\colon && w = 0,\ Z = a_0 + a_2 = 1 + a_2 \Rightarrow \underline{a_2 = 1};\\
&x_1 = 0, x_2 = x_3 = 1\colon && w = 1,\ Z = a_0 + a_2 + a_3 + a_{23} = 1 + a_{23} \Rightarrow \underline{a_{23} = 0};\\
&x_1 = 1, x_2 = x_3 = 0\colon && w = 0,\ Z = a_0 + a_1 = 1 + a_1 \Rightarrow \underline{a_1 = 1};\\
&x_1 = 1, x_2 = 0, x_3 = 1\colon && w = 1,\ Z = a_0 + a_1 + a_3 + a_{13} = 1 + a_{13} \Rightarrow \underline{a_{13} = 0};\\
&x_1 = x_2 = 1, x_3 = 0\colon && w = 1,\ Z = a_0 + a_1 + a_2 + a_{12} = 1 + a_{12} \Rightarrow \underline{a_{12} = 0};\\
&x_1 = x_2 = x_3 = 1\colon && w = 0,\ Z = a_0 + a_1 + a_2 + a_3 + a_{12} + a_{13} + a_{23} + a_{123} =\\
& && \qquad = a_{123} \Rightarrow \underline{a_{123} = 0}.
\end{aligned}
$$

Следовательно,

$$
w(x_1, x_2, x_3) = 1 + x_1 + x_2 + x_3,
$$

и функция $w$ оказывается линейной, $w \in L$.

Соберём полученные результаты в т. н. *критериальную таблицу*.

| | $T_0$ | $T_1$ | $S$ | $M$ | $L$ |
|---|---|---|---|---|---|
| $f$ | $+$ | $+$ | $-$ | $+$ | $-$ |
| $w$ | $-$ | $-$ | $+$ | $-$ | $+$ |

В каждом столбце критериальной таблицы есть хотя бы один минус. Это означает, что система $\{f, w\}$ не содержится ни в одном из классов Поста и по теореме 1 она полна.

Алгоритм выражения отрицания и конъюнкции через функции произвольной полной системы изложен в доказательстве теоремы Поста, см. [БТ, Теорема 6.7]. Следуя этому алгоритму, заметим, что функция $w$ не принадлежит ни классу $T_0$, ни классу $T_1$. Это позволяет сразу выразить отрицание:

$$\overline{x} = w(x, x, x). \tag{3}$$

Далее со вспомогательными целями нужно выразить константы 0 и 1 (т. е. булевы функции, которые тождественно принимают значения 0 и 1 соответственно). Добиться этого можно, используя несамодвойственную функцию $f$ и уже выраженное отрицание. Как мы уже заметили, функция $f$ на противоположных наборах $(0, 0, 1)$ и $(1, 1, 0)$ принимает одно и то же значение 1. Отсюда следует, что

$$1 = f(x, x, \overline{x}). \tag{4}$$

Константа 0 тогда легко выражается как

$$0 = \overline{1} = \overline{f(x, x, \overline{x})}. \tag{5}$$

Конъюнкция выражается с помощью нелинейной функции. Заметим, что каков бы ни был нелинейный полином Жегалкина $Z(x_1, \ldots, x_n)$, подставив вместо всех переменных, кроме некоторых двух, константы 0 и 1, его можно свести к выражению вида

$$\chi(x, y) = xy + ax + by + c.$$

В нашем случае полином Жегалкина (2) для функции $f$ уже имеет этот вид с $x = x_1$, $y = x_3$, $a = 1$. $b = 1$, $c = 0$. Согласно общему алгоритму, конъюнкция теперь может быть выражена следующим образом

$$xy = \chi(x + b, y + a) + ab + c. \tag{6}$$

Обратите внимание, что если, например, $b = 1$, то $x + 1 = \overline{x}$ (напомним, что $+$ у нас обозначает плюс по модулю 2), а если $b = 0$, то $x + b = x$. Таким образом, преобразование (6) реализуемо с помощью уже выраженного отрицания. В нашем случае получаем:

$$xy = \chi(x + 1, y + 1) + 1 = \overline{\chi(\overline{x}, \overline{y})} = \overline{f(\overline{x}, 1, \overline{y})} \tag{7}$$

(в данном случае было всё равно, подставлять вместо $x_2$ константу 0 или 1; мы выбрали 1 так как она проще выражается через $f$ и $w$).

Схемы из функциональных элементов подробно описаны в [БТ, п. 6.8]. По сути, схема из функциональных элементов — это графическое представление разложения булевой функции в суперпозицию некоторых

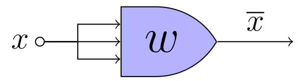


Рис. 2: Схема для отрицания

условно простейших функций. В нашем случае, простейшими считаются $f$ и $w$ и, например, отрицание выражается через них (фактически, через одну $w$) по формуле (3). Соответствующая схема из функциональных элементов показана на рис. 2.

Для полной записи конъюнкции как суперпозиции функций $f$ и $w$ нужно скомбинировать формулы (3), (4) и (7). Получим:

$$\begin{aligned} xy &= \overline{f(\overline{x}, 1, \overline{y})} = \overline{f(\overline{x}, f(x, x, \overline{x}), \overline{y})} = \\ &= w\Big(f\big(w(x,x,x), f(x,x,w(x,x,x)), w(y,y,y)\big), \\ &\qquad f\big(w(x,x,x), f(x,x,w(x,x,x)), w(y,y,y)\big), \\ &\qquad f\big(w(x,x,x), f(x,x,w(x,x,x)), w(y,y,y)\big)\Big). \end{aligned}$$

Схема из функциональных элементов:

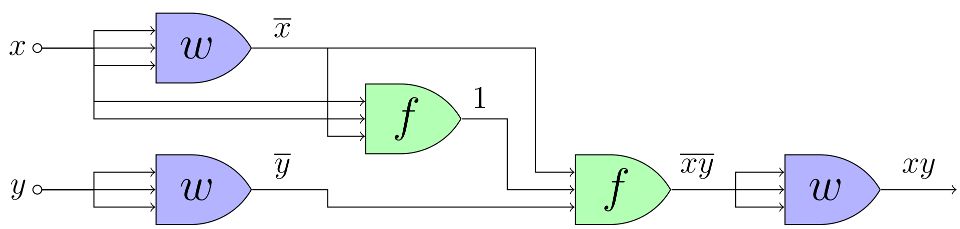


Рис. 3: Схема для конъюнкции

†

Для самостоятельного решения рекомендуется задача [БТ, 6.23, стр. 459].

# Список литературы

[БТ] А. И. Белоусов, С. Б. Ткачёв, Дискретная математика, 3-е изд., М.: Издательство МГТУ им. Н. Э. Баумана, 2004.