АЛГЕБРАИЧЕСКАЯ НОРМАЛЬНАЯ ФОРМА БУЛЕВЫХ ФУНКЦИЙ И ЕЕ БЫСТРОЕ ВЫЧИСЛЕНИЕ*

И. В. Агафонова — iivagafonovaspb@gmail.com

В. Н. Малозёмов — malv@math.spbu.ru

25 мая 2013 г.

1°. Функция n переменных $f(x_1, \dots, x_n)$ называется *булевой*, если её аргументы и сама она могут принимать только два значения, 0 или 1.

Вектор булевых переменных $x = (x_1, \dots, x_n)$ имеет $N = 2^n$ различных значений $x^{(0)}, x^{(1)}, \dots, x^{(N-1)}$. Их можно перечислить. Например, при $n = 1$ и $n = 2$ таблицы аргументов выглядят так:

№	x_1
0	0
1	1

№	x_1	x_2
0	0	0
1	1	0
2	0	1
3	1	1

Переход от таблицы с n аргументами к таблице с $n + 1$ аргументом осуществляется по следующей схеме:

№	$x_1 \quad \dots \quad x_n$
0	
1	A
$\vdots$	
$2^n - 1$	

$\longrightarrow$

№	$x_1 \quad \dots \quad x_n$	x_{n+1}
0		0
1	A	$\vdots$
$\vdots$		
$2^n - 1$		0
2^n		1
$2^n + 1$	A	$\vdots$
$\vdots$		
$2^{n+1} - 1$		1

*Семинар по дискретному гармоническому анализу и геометрическому моделированию «DHA & CAGD»: `http://www.dha.spb.ru/`

Каждому вектору аргументов $x^{(k)}$ сопоставляется значение булевой функции $f[k] = f(x^{(k)})$. Ниже приводится полная таблица булевой функции при $n = 3$.

№	x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	0	$f[0]$
1	1	0	0	$f[1]$
2	0	1	0	$f[2]$
3	1	1	0	$f[3]$
4	0	0	1	$f[4]$
5	1	0	1	$f[5]$
6	0	1	1	$f[6]$
7	1	1	1	$f[7]$

Общее количество булевых функций n переменных равно количеству различных двоичных векторов $f[0 : N-1]$ длины $N = 2^n$, то есть 2^{2^n}.

2°. Принципиальный факт заключается в том, что любую булеву функцию можно составить из её аргументов и константы 1 с помощью двух операций — сложения по модулю 2 и умножения. Эти операции определяются так:

$$\begin{array}{cccc} 0 \oplus 0 = 0, & 0 \oplus 1 = 1, & 1 \oplus 0 = 1, & 1 \oplus 1 = 0; \\ 0 \cdot 0 = 0, & 0 \cdot 1 = 0, & 1 \cdot 0 = 0, & 1 \cdot 1 = 1. \end{array}$$

Знак умножения (точку) часто опускают: вместо $x_1 \cdot x_2$ пишут $x_1 x_2$.

Отметим, что для булевой переменной a справедливо равенство

$$a \oplus a = 0. \tag{1}$$

Рассмотрим булеву функцию одной переменной $f(x_1)$. С учётом (1) имеем

$$f(x_1) = f(0) \oplus [f(0) \oplus f(1)]x_1 = a_0^1 \oplus a_1^1 x_1.$$

Это равенство верно как при $x_1 = 0$, так и при $x_1 = 1$. Аналогично для булевой функции двух переменных получаем

$$\begin{aligned} f(x_1, x_2) &= f(x_1, 0) \oplus [f(x_1, 0) \oplus f(x_1, 1)]x_2 = a_0^2 \oplus a_1^2 x_1 \oplus [a_2^2 \oplus a_{12}^2 x_1]x_2 = \\ &= a_0^2 \oplus a_1^2 x_1 \oplus a_2^2 x_2 \oplus a_{12}^2 x_1 x_2. \end{aligned}$$

В общем случае

$$\begin{gathered} f(x_1, \ldots, x_{n-1}, x_n) = \\ = f(x_1, \ldots, x_{n-1}, 0) \oplus [f(x_1, \ldots, x_{n-1}, 0) \oplus f(x_1, \ldots, x_{n-1}, 1)]x_n = \\ = a_0^n \oplus \bigoplus_{\substack{1 \leqslant i_1 < \cdots < i_k \leqslant n, \\ k \in 1:n}} a^n_{i_1, \ldots, i_k} x_{i_1} \cdots x_{i_k}, \end{gathered} \tag{2}$$

где коэффициенты принимают значения 0 или 1. Это и есть алгебраическая нормальная форма булевой функции.

Выражение, стоящее в правой части равенства (2), называется *полиномом Жегалкина* [1]. Верхний индекс n у коэффициентов полинома Жегалкина обычно опускают.

Подведём итог.

ТЕОРЕМА. *Любая булева функция может быть представлена в виде полинома Жегалкина.*

3°. Количество коэффициентов у полинома Жегалкина равно

$$1 + C_n^1 + \cdots + C_n^n = 2^n.$$

Оно совпадает с количеством значений вектора аргументов булевой функции. По значениям $f[0], f[1], \ldots, f[N-1]$ булевой функции нетрудно вычислить коэффициенты соответствующего полинома Жегалкина. Программа вычислений выглядит так:

$$\begin{aligned}
&\text{for } k := 0 \text{ to } 2^n - 1 \text{ do}\\
&\quad a[k] := f[k];\\
&\text{for } i := 1 \text{ to } n \text{ do}\\
&\text{for } s := 0 \text{ to } 2^{n-i} - 1 \text{ do}\\
&\text{for } l := 0 \text{ to } 2^{i-1} - 1 \text{ do}\\
&\quad a[2^i s + 2^{i-1} + l] := a[2^i s + l] \oplus a[2^i s + 2^{i-1} + l]
\end{aligned} \tag{3}$$

После работы программы в массиве $a[0 : 2^n - 1]$ будут находиться коэффициенты полинома Жегалкина.

Разберёмся в схеме (3) более детально. При $i = 1$ $(l = 0)$ вычисляем

$$\begin{aligned}
&\text{for } s := 0 \text{ to } 2^{n-1} - 1 \text{ do}\\
&\quad a[2s+1] := a[2s] \oplus a[2s+1]
\end{aligned}$$

При $i = 2$

$$\begin{aligned}
&\text{for } s := 0 \text{ to } 2^{n-2} - 1 \text{ do}\\
&\text{for } l := 0 \text{ to } 1 \text{ do}\\
&\quad a[4s + 2 + l] := a[4s + l] \oplus a[4s + 2 + l]
\end{aligned}$$

и так далее. При $i = n$ $(s = 0)$

$$\begin{aligned}
&\text{for } l := 0 \text{ to } 2^{n-1} - 1 \text{ do}\\
&\quad a[2^{n-1} + l] := a[l] \oplus a[2^{n-1} + l]
\end{aligned}$$

Схема (3) называется *быстрым алгоритмом вычисления коэффициентов полинома Жегалкина*. В ней используется только операция сложения по модулю 2 в количестве

$$\sum_{i=1}^{n} 2^{n-i}2^{i-1} = n2^{n-1} = \frac{1}{2}N\log_2 N \text{ операций.}$$

В табл. 1 приведены результаты вычислений по схеме (3) для конкретной булевой функции трёх переменных. В последнем столбце перечислены все мономы от трёх переменных, а в предпоследнем — найденные значения коэффициентов при этих мономах.

Таблица 1

№	x_1	x_2	x_3	f	$i=1$	$i=2$	$i=3$	мономы
0	0	0	0	1	1	1	1	1
1	1	0	0	0	1	1	1	x_1
2	0	1	0	1	1	0	0	x_2
3	1	1	0	0	1	0	0	x_1x_2
4	0	0	1	0	0	0	1	x_3
5	1	0	1	1	1	1	0	x_1x_3
6	0	1	1	1	1	1	1	x_2x_3
7	1	1	1	0	1	0	0	$x_1x_2x_3$

Получаем представление

$$f(x_1, x_2, x_3) = 1 \oplus x_1 \oplus x_3 \oplus x_2x_3. \qquad (4)$$

Отметим, что индексы переменных, входящих в мономы, согласованы со значениями аргументов булевой функции.

4°. Рассмотрим обратную задачу — вычисление значений полинома Жегалкина (2). Она решается просто, так как соотношения (3) обратимы. Удивительным является тот факт, что значения полинома Жегалкина будут найдены, если воспользоваться самой схемой (3), поменяв в ней местами идентификаторы f и a (см. [2]).

В табл. 2 приведены результаты вычисления значений полинома (4) по схеме (3).

В последнем столбце указаны значения полинома (4).

Таблица 2

№	x_1	x_2	x_3	a	$i=1$	$i=2$	$i=3$
0	0	0	0	1	1	1	1
1	1	0	0	1	0	0	0
2	0	1	0	0	0	1	1
3	1	1	0	0	0	0	0
4	0	0	1	1	1	1	0
5	1	0	1	0	1	1	1
6	0	1	1	1	1	0	1
7	1	1	1	0	1	0	0

ЛИТЕРАТУРА

1. Жегалкин И. И. *Арифметизация символической логики.* //Матем. сб. 1928. Т. 35. С. 311—377.

2. Carlet C. *Boolean functions for cryptography and error correcting codes* // In: Boolean Models and Methods in Mathematics, Computer Science and Engineering. Cambridge Univ. Press. Y. Crama and P. L. Hammer (eds.). 2010. P. 257–397.