Алгебраическая нормальная форма булевой функции и бинарное преобразование Мёбиуса

И.В.Агафонова
ivagafonovaspb@gmail.com

25 мая 2013 г.

Булева функция n переменных $f(x_1, x_2, \ldots, x_n)$ определена на множестве двоичных векторов длины n н принимает только два возможных значения, 0 или 1. Булева функция задана, если известны её значения при всех 2^n возможных значениях двоичного вектора $x = (x_1, x_2, \ldots, x_n)$. Таблица, в которой всем значениям аргумента сопоставлены значения булевой функции, традиционно называется *таблицей истинности*.

Например, одна из булевых функций трёх переменных задаётся следующей таблицей.

Таблица 1

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

Общее число булевых функций n переменных равно количеству различных двоичных векторов длины 2^n, то есть 2^{2^n}.

В строках таблицы истинности двоичные векторы $x = (x_1, x_2, \ldots, x_n)$ будем записывать в лексикографическом порядке по возрастанию. Пронумеруем их от 0 до $2^n - 1$ и обозначим через $x^{(i)}$ вектор, который будет i-м по порядку: $x^{(0)} = (0, \ldots, 0)$ и так далее. Заметим, что вектор $x^{(i)}$ и его номер i, записанный

в n двоичных разрядах, будут читаться одинаково. Например, в таблице 1 вектор $x^{(6)} = (1, 1, 0)$ имеет номер 110_2.

Выбранный порядок будем обозначать обычным знаком неравенства: $x^{(i-1)} < x^{(i)}$, $i = 1 : 2^n - 1$.

Если считать, что порядок записи всегда именно такой, то выписывать всю таблицу истинности нет необходимости. Для определения булевой функции достаточно задать вектор её значений $f = (f(x^{(i)})), i \in 0 : 2n - 1$, то есть последний столбец таблицы истинности. В данном примере это $f = (10010011)^T$. (Обычно записывают вектор значений без знака транспонирования, не подчёркивая различий между записью в строку или столбец.)

Для задания булевой функции не обязательно приводить полный список её значений, достаточно указать правило или формулу, по которой этот список однозначно восстанавливается.

Мы будем получать выражения для булевых функций, использующие операции в конечном поле Z_2, состоящем из элементов 0 и 1, а именно:

1) операцию $\oplus$ — сложение (по модулю 2), определяемую правилами

$$0 \oplus 0 = 0,\ 0 \oplus 1 = 1,\ 1 \oplus 0 = 1,\ 1 \oplus 1 = 0;$$

2) операцию $\cdot$ (точка) — умножение, определяемую правилами

$$0 \cdot 0 = 0,\ 0 \cdot 1 = 0,\ 1 \cdot 0 = 0,\ 1 \cdot 1 = 1.$$

Знак умножения часто опускают: xy — то же, что $x \cdot y$.

Обозначая для краткости $V_n = Z_2^n$, мы можем определить булеву функция n переменных как отображение V_n в Z_2. Это отображение мы будем строить в виде многочлена.

Многочлен от n переменных над полем Z_2 представляет собой сумму одночленов (мономов), взятых с коэффициентами 0 или 1. Из определения операций в Z_2 вытекает, что для любого $x \in Z_2$ всегда $x \oplus x = 0$, $x \cdot x = x$ и вообще $x^k = x$ для любого натурального k, так что моном не содержит степеней выше первой ни для какой переменной x_i.

Таким образом, всякий моном записывается как

$$x_1^{u_1} x_2^{u_2} \dots x_n^{u_n},$$

где $u = (u_1, u_2, \dots, u_n) \in V_n$. При $u_i = 1$ переменная x_i входит в моном, при $u_i = 0$ не входит. Мы часто будем использовать компактную запись монома

$$x^u = x_1^{u_1} x_2^{u_2} \dots x_n^{u_n}.$$

Число различных мономов от n переменных равно числу векторов $u \in V_n$, то есть 2^n, и из них можно, умножая каждый моном на коэффициент 0 или 1, составить 2^{2^n} полиномов — столько же, сколько существует булевых функций. Взаимно однозначное соответствие между булевыми функциями и полиномами устанавливает следующая теорема [1].

ТЕОРЕМА. *Каждая булева функция n переменных имеет единственное (с точностью до порядка слагаемых и сомножителей) представление в виде полинома от n переменных над полем Z_2, называемого полиномом Жегалкина или алгебраической нормальной формой (АНФ) данной функции.*

Доказательств этой теоремы известно несколько, и большинство из них даёт тот или иной способ построения АНФ. Рассмотрим один из таких способов.

Пусть булева функция n переменных задана своей таблицей значений.

Введём обозначение

$$\mathrm{supp}(x) = \{i \in 1 : n \mid x_i = 1\}$$

(носитель вектора x) и построим по каждому номеру $k \in 0 : 2^n - 1$ базисный полином

$$b_k(x) = \prod_{i \in 1:n} (x_i \oplus \delta_k(i) \oplus 1), \tag{1}$$

где

$$\delta_k(i) = \begin{cases} 1, & \text{если } i \in \mathrm{supp}(x^{(k)}), \\ 0, & \text{если } i \notin \mathrm{supp}(x^{(k)}). \end{cases}$$

Базисный полином (1) равен 1 тогда и только тогда, когда $x_i = \delta_k(i)$ при всех i, то есть в единственной точке $x = x^{(k)}$. Тогда сумма

$$\bigoplus_{k \in \mathrm{supp}(f)} b_k(x),$$

где обозначено

$$\mathrm{supp}(f) = \{k \in 0 : 2^n - 1 \mid f(x^{(k)}) = 1\},$$

принимает значение 1 в точках $x^{(k)}$ и только в них. Следовательно, имеет место представление

$$f(x) = \bigoplus_{k \in \mathrm{supp}(f)} b_k(x). \tag{2}$$

Для примера построим полином Жегалкина по таблице 1, добавив к ней столбец базисных полиномов, входящих в сумму (2) для данной функции. Получим таблицу 2.

Таблица 2

k	x_1	x_2	x_3	$f(x_1,x_2,x_3)$	$b_k(x)$
0	0	0	0	1	$(x_1 \oplus 1)(x_2 \oplus 1)(x_3 \oplus 1)$
1	0	0	1	0	
2	0	1	0	0	
3	0	1	1	1	$(x_1 \oplus 1)x_2x_3$
4	1	0	0	0	
5	1	0	1	0	
6	1	1	0	1	$x_1x_2(x_3 \oplus 1)$
7	1	1	1	1	$x_1x_2x_3$

Отсюда сразу можно записать, согласно (2),

$$f(x) = (x_1 \oplus 1)(x_2 \oplus 1)(x_3 \oplus 1) \oplus (x_1 \oplus 1)x_2x_3 \oplus x_1x_2(x_3 \oplus 1) \oplus x_1x_2x_3.$$

После раскрытия скобок и приведения подобных членов получим

$$f(x) = 1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_1x_3.$$

Формула (2) показывает, что каждую булеву функцию можно представить полиномом Жегалкина (АНФ). В свою очередь и полином можно вычислить в каждой точке и получить вектор его значений, то есть булеву функцию. При этом число булевых функций и полиномов одинаково, так что имеет место единственность АНФ для данной функции.

Булеву функцию как многочлен от n переменных будем записывать в виде

$$f(x) = \bigoplus_{u \in V_n} g(u)x^u,\ g(u) \in Z_2. \tag{3}$$

Для описания быстрого алгоритма построения АНФ нам понадобится ввести определённый порядок на множестве мономов $\{x^u\},\ x \in V_n, u \in V_n$. Мы сделаем это, используя уже введённое на V_n лексикографическое упорядочение и положив, что $x^u < x^v$ тогда и только тогда, когда $u < v$.

Теперь мы можем присвоить моному x^u тот же номер, что и вектору $u \in V_n$ при лексикографическом упорядочении. Полином (3) будет однозначно определяться вектором коэффициентов $g = (g(u^{(i)}))$, $i \in 0 : 2^n - 1$. В качестве иллюстрации в таблице 3 приводится порядок и нумерация мономов от трёх переменных. Как мы видим, встречавшийся выше многочлен $f(x) = 1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_1x_3$ задаётся вектором $g = (11101100)$.

Таблица 3

№	x_1	x_2	x_3	моном
0	0	0	0	1
1	0	0	1	x_3
2	0	1	0	x_2
3	0	1	1	x_2x_3
4	1	0	0	x_1
5	1	0	1	x_1x_3
6	1	1	0	x_1x_2
7	1	1	1	$x_1x_2x_3$

Далее будем через $u \subseteq x$ кратко обозначать отношение $\mathrm{supp}(u) \subseteq \mathrm{supp}(x)$ на V_n. Это включение означает, что из $u_j = 1$ следует $x_j = 1$, или, что то же самое, из $x_j = 0$ следует $u_j = 0$. Поэтому

$$x^u = \begin{cases} 1, & \text{если } u \subseteq x, \\ 0, & \text{в противном случае.} \end{cases} \tag{4}$$

Действительно,

$$x^u = x_1^{u_1} x_2^{u_2} \dots x_n^{u_n} = (\text{оставляем только } u_j = 1) = \prod_{u_j=1} x_j,$$

откуда и следует (4).

Вычисляя в точке x значение булевой функции, заданной полиномом (3), получаем с учётом (4), что

$$f(x) = \bigoplus_{u \in V_n,\, u \subseteq x} g(u). \tag{5}$$

Пусть булева функция n переменных $f(x)$, заданная вектором значений $f \in V_{2^n}$, является полиномом (3) с вектором коэффициентов $g \in V_{2^n}$. Отображение $\mu : V_{2^n} \to V_{2^n}$, ставящее в соответствие вектору f вектор g и тем самым функции $f(x)$ — функцию с вектором значений $g(u)$, называют *бинарным преобразованием Мёбиуса*:

$$g = \mu(f).$$

Замечательно, что это преобразование может осуществляться по формуле, аналогичной (5):

$$g(u) = \bigoplus_{x \in V_n,\, x \subseteq u} f(x). \tag{6}$$

Докажем формулу (6). Обозначим правую часть (6) через $G(u)$:

$$G(u) = \bigoplus_{x \in V_n,\, x \subseteq u} f(x). \tag{7}$$

Согласно (5), вычислим функцию

$$F(x) = \bigoplus_{u \in V_n,\, u \subseteq x} G(u).$$

Подставляя выражение (7), получаем

$$F(x) = \bigoplus_{\substack{u \in V_n,\, y \in V_n, \\ u \subseteq x \quad y \subseteq u}} f(y) = \bigoplus_{y \in V_n} f(y) \bigoplus_{\substack{u \in V_n, \\ y \subseteq u,\, u \subseteq x}} 1.$$

В последней сумме складываются просто единицы. Выделив особо слагаемое $y = x$, имеем

$$F(x) = f(x) \oplus \bigoplus_{\substack{y \in V_n, \\ y \neq x}} f(y) \bigoplus_{\substack{u \in V_n, \\ y \subseteq u,\, u \subseteq x}} 1. \tag{8}$$

Рассмотрим включение $y \subseteq u \subseteq x$ при фиксированных y и x, $y \neq x$. В силу указанного включения для $i \in 1 : n$ возможны случаи

1) $x_i = y_i = 1$, тогда $u_i = 1$;

2) $x_i = y_i = 0$, тогда $u_i = 0$;

3) $x_i = 1$, $y_i = 0$, тогда $u_i = 0$ или $u_i = 1$.

Перебор векторов u в правой сумме в (8) сводится к перебору нулей или единиц для u_i в третьем случае. (При $y \neq x$ хотя бы при одном i этот случай будет иметь место.)

Пусть m — число координат, для которых $y_i \neq x_i$ (третий случай). Тогда слагаемых в сумме ровно 2^m — чётное число, и эта сумма обратится в 0.

Получаем $F(x) = f(x)$. В таком случае $G(u) = g(u)$ в силу единственности АНФ, что и требовалось доказать.

Формулы (5) и (6) показывают, что $\mu = \mu^{-1}$.

Покажем теперь, как получается и как работает быстрый алгоритм построения $\mu(f)$ по заданному вектору значений функции $f(x_1, x_2, \ldots, x_n)$. Этот алгоритм, следуя [2], назовём быстрым преобразованием Мёбиуса.

Применим формулу (6) при фиксированных значениях $u_1 = 0$ и $u_1 = 1$, тем самым вычисляя первую и вторую половины вектора значений функции $g(u_1, u_2, \ldots, u_n)$.

$$g(0,u_2,\dots,u_n)=\bigoplus_{x\subseteq(0,u_2,\dots,u_n)} f(x)=(\text{обязательно будет } x_1=0)$$
$$=\bigoplus_{(x_2,\dots,x_n)\subseteq(u_2,\dots,u_n)} f(0,x_2,\dots,x_n), \tag{9}$$
$$g(1,u_2,\dots,u_n)=\bigoplus_{x\subseteq(1,u_2,\dots,u_n)} f(x)=\bigoplus_{\substack{x_1\in\{0,1\}\\(x_2,\dots,x_n)\subseteq(u_2,\dots,u_n)}} f(x_1,x_2,\dots,x_n)=$$
$$=\bigoplus_{(x_2,\dots,x_n)\subseteq(u_2,\dots,u_n)} [f(0,x_2,\dots,x_n)\oplus f(1,x_2,\dots,x_n)]. \tag{10}$$

Сравнивая полученные для $g(0,u_2,\dots,u_n)$, $g(1,u_2,\dots,u_n)$ формулы с (6), видим, что

$$g(0,u_2,\dots,u_n)=\mu(f(0,x_2,\dots,x_n)),$$
$$g(1,u_2,\dots,u_n)=\mu(f(0,x_2,\dots,x_n)\oplus f(1,x_2,\dots,x_n)).$$

Кратко полученный результат можно изобразить в виде

$$\mu(f)=\begin{pmatrix}\mu(f^0)\\ \mu(f^0\oplus f^1)\end{pmatrix}, \tag{11}$$

где обозначено

$$f^0=f^0(x_2,\dots,x_n)=f(0,x_2,\dots,x_n),$$
$$f^1=f^1(x_2,\dots,x_n)=f(1,x_2,\dots,x_n).$$

В формуле (11) каждое из выражений $\mu(f^0)$ и $\mu(f^0\oplus f^1)$ представляет собой вектор-столбец длины 2^{n-1}, и столбец значений для $\mu(f)$ образован конкатенацией этих двух столбцов.

Таким образом, чтобы вычислить преобразование Мёбиуса функции f, мы сначала выделим из столбца значений функции f его верхнюю половину f^0 и нижнюю f^1 и найдём их сумму $f^0\oplus f^1$, которую можно записать прямо на место столбца f^1. Полученный при этом столбец обозначим $\varphi(f)$:

$$\begin{pmatrix}f^0\\ f^1\end{pmatrix}\xrightarrow{\varphi}\begin{pmatrix}f^0\\ f^0\oplus f^1\end{pmatrix}.$$

Если $n=1$, то имеем константы $f^0=f(0)$, $f^1=f(1)$. По (9),(10) в этом случае имеем $g(0)=f(0)$, $g(1)=f(0)\oplus f(1)$, что можно записать как $g=\varphi(f)$.

Пусть $n>1$.

Уменьшим на единицу индексы переменных, а затем и n:

$$x_{i-1} := x_i,\ i \in 2:n,$$
$$n := n - 1.$$

Теперь можно работать с каждой из функций f^0, $f^0 \oplus f^1$ так же, как с f, то есть применять к ним преобразование φ и оперировать с их подвекторами. На последнем шаге, при $n = 1$, вектор $g = \mu(f)$ будет найден.

Итак, для быстрого вычисления $\mu(f)$ по заданному лексикографически упорядоченному столбцу значений функции $f = f(x_1, x_2, \ldots, x_n)$ вызывается рекурсивная процедура, которую обозначим $FastMT(n, f)$. Её псевдокод:

$FastMT(n, f)$
1. if $n = 0$ return f
2. $f := \varphi(f)$
3. $FastMT(n-1, f^0)$
4. $FastMT(n-1, f^1)$

После завершения этой процедуры на месте вектора f будет находиться вектор $g = \mu(f)$.

Приведём пример работы быстрого алгоритма для функции, заданной таблицей 1.

Таблица 4

x_1	x_2	x_3	f	$n=3$	$n=2$	$n=1,\ g=\mu(f)$
0	0	0	1	1	1	1
0	0	1	0	0	0	1
0	1	0	0	0	1	1
0	1	1	1	1	1	0
1	0	0	0	1	1	1
1	0	1	0	0	0	1
1	1	0	1	1	0	0
1	1	1	1	0	0	0

Получена функция g. Трактуя столбец g как набор коэффициентов при лексикографически упорядоченных мономах (см.таблицу 3), записываем f в алгебраической нормальной форме:

$$f = 1 \oplus x_3 \oplus x_2 \oplus x_1 \oplus x_1 x_3.$$

В заключение приведём таблицу 5, которая показывает, как этот же алгоритм по столбцу значений коэффициентов g восстанавливает столбец значений функции f.

Таблица 5

u_1	u_2	u_3	g	$n=3$	$n=2$	$n=1,\ f=\mu(g)$
0	0	0	1	1	1	1
0	0	1	1	1	1	0
0	1	0	1	1	0	0
0	1	1	0	0	1	1
1	0	0	1	0	0	0
1	0	1	1	0	0	0
1	1	0	0	1	1	1
1	1	1	0	0	0	1

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 University Press. Y. Crama and P. L. Hammer (eds.). 2010. P. 257-397.