

О СЛОЖНОСТИ ДОКАЗАТЕЛЬСТВА ПОВТОРНОСТИ БУЛЕВЫХ ФУНКЦИЙ В БИНАРНОМ БАЗИСЕ¹

А. А. Вороненко

Московский государственный университет им. М. В. Ломоносова, г. Москва, Россия

E-mail: dm6@cs.msu.ru

Показано, что для доказательства повторности булевой функции в базисе всех функций двух переменных в худшем случае требуется линейное по числу переменных функции количество наборов.

Ключевые слова: неповторная булева функция, сложность доказательства.

Булева функция $f(x_1, \dots, x_n)$, представляемая (не представляемая) неповторной формулой в некотором базисе, называется *неповторной* (*повторной*) в этом базисе. Множество всех функций двух переменных называется *бинарным базисом*.

В настоящей работе доказываются две теоремы.

Теорема 1. Существует повторная в бинарном базисе функция n переменных, доказательство повторности которой требует предъявления не менее $n + 3$ наборов.

Теорема 2. Для любой повторной в бинарном базисе функции n переменных можно предъявить $4n$ наборов, доказывающих ее повторность.

Их следствием является

Теорема 3. Доказательство повторности булевой функции в базисе всех функций двух переменных в худшем случае требует линейного относительно числа переменных функции количества наборов.

Преобразованиями обобщенной однотипности называются замена переменной или самой функции на ее отрицание и перестановка переменных. Функции, получаемые друг из друга конечным числом преобразований обобщенной однотипности, называются *обобщенно однотипными*.

Функциями Стеценко называются функции следующих пяти семейств:

$$\begin{aligned} f_d^{(s)} &= x_1 \wedge (x_2 \vee x_3 \wedge \dots \wedge x_s) \vee x_2 \wedge \bar{x}_3 \wedge \dots \wedge \bar{x}_s, & s \geq 3, \\ f_t^{(s)} &= x_1 \wedge x_2 \wedge \dots \wedge x_s \vee \bar{x}_1 \wedge \bar{x}_2 \wedge \dots \wedge \bar{x}_s, & s \geq 2, \\ f_m^{(s)} &= x_1 \wedge (x_2 \vee \dots \vee x_s) \vee x_2 \wedge \dots \wedge x_s, & s \geq 3, \\ f_4 &= x_1 \wedge (x_2 \vee x_3) \vee x_3 \wedge x_4, \\ f_5 &= x_1 \wedge (x_3 \wedge x_4 \vee x_5) \vee x_2 \wedge (x_3 \vee x_4 \wedge x_5). \end{aligned}$$

Теорема Стеценко [1]. Из любой повторной в базисе $\{\wedge, \vee, \neg\}$ функции можно подстановкой констант получить подфункцию, однотипную с одной из функций Стеценко.

¹Работа выполнена при поддержке гранта Президента РФ МД-757.2011.9.

Функциями Перязева называются следующие четыре функции:

$$\begin{aligned} p_1 &= x_1 \wedge x_2 \wedge x_3 \oplus \bar{x}_2 \wedge \bar{x}_3, \\ p_2 &= x_1 \wedge (x_2 \vee x_3) \oplus x_2 \wedge x_3, \\ p_3 &= x_1 \wedge x_2 \wedge x_3 \wedge x_4 \oplus (x_1 \oplus \bar{x}_2) \wedge \bar{x}_3 \wedge \bar{x}_4, \\ p_4 &= x_1 \wedge (x_2 \vee x_3 \wedge x_4) \oplus (x_3 \vee x_2 \wedge x_4). \end{aligned}$$

Теорема Перязева [2]. Из любой повторной в бинарном базисе функции можно подстановкой констант получить подфункцию, однотипную с одной из функций Стеценко (для $f_t^{(s)}$ выполняется $s \geq 3$), либо одну из функций Перязева.

Рассмотрим повторную в бинарном базисе функцию $(x_1 \vee \dots \vee x_n) \wedge (\bar{x}_1 \vee \dots \vee \bar{x}_n)$, где $n \geq 3$. Оценим снизу количество наборов в доказательстве ее повторности. Для доказательства повторности этой функции требуется предъявить оба ее нуля, иначе предъявляемая частичная функция доопределима либо до $x_1 \vee \dots \vee x_n$, либо до $\bar{x}_1 \vee \dots \vee \bar{x}_n$.

Назовем 0–1-матрицу *разнозначной*, если все ее строки различны и она не имеет ни нулевых, ни единичных строк. Будем говорить, что функция φ *моделирует* разнозначную матрицу, если $\varphi(x) = 1$ для всех строк x матрицы и $\varphi(\mathbf{0}) = \varphi(\mathbf{1}) = 0$.

Лемма 1. Каковы бы ни были три (четыре) ненулевых и неединичных набора значений трех (четырех) переменных, найдется неповторная функция, равная на них единице и нулю на единичном и нулевом наборах.

Доказательство. В силу возможности замены всех переменных их отрицаниями будем считать, что средний вес наборов не превосходит половины числа столбцов матрицы, составленной из этих наборов. В силу симметричности функции $(x_1 \vee \dots \vee x_n) \wedge (\bar{x}_1 \vee \dots \vee \bar{x}_n)$ на каждом слое булева куба, начиная с первого, будем выбирать минимальные в лексикографическом порядке наборы. Для трех переменных

возникает три матрицы $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$. Первые две из них моделирует функция $x_1 \oplus (x_2 \vee x_3)$, последнюю — $x_2 \oplus x_3$.

Заметим, что часть матриц с четырьмя столбцами моделируется функцией $x_1 \oplus x_2 \oplus x_3 \oplus x_4$ либо одной из функций вида $(x_{i_1} \oplus x_{i_2}) \vee (x_{i_3} \oplus x_{i_4})$. Чтобы этого не произошло, матрица должна иметь набор веса два из каждой из трех пар противоположных наборов. Возможны четыре случая:

$$\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}.$$

Все эти матрицы моделирует функция $(\bar{x}_1 \vee \bar{x}_2) \wedge (x_3 \vee x_4)$. ■

Для ненулевых и неединичных наборов длины не менее пяти введем следующую классификацию: наборы *первого рода* — имеющие ровно один ноль или ровно одну единицу; наборы *второго рода* — имеющие ровно два нуля или ровно две единицы (эти значения — 0 и 1 соответственно — назовём *особыми*); наборы *третьего рода* — остальные.

Лемма 2. Пусть дана произвольная разнзначная 0–1-матрица размера $m \times n$, где $m \leq n$ и $n \geq 5$. Тогда либо эта матрица моделируется некоторой бесповторной функцией, либо в ней есть два столбца, удалением которых вместе со строками, имеющими в них разные значения, и удалением дублирующихся строк можно вновь получить разнзначную матрицу с числом строк, не превосходящим числа столбцов.

Доказательство. Пусть противоположных строк второго рода нет. Рассмотрим граф с n вершинами и ребрами между теми из них, для которых существует строка второго рода, имеющая особые значения в соответствующих позициях (граф *второго рода*). Если в графе второго рода есть две неизоллированные вершины, не соединенные ребром, то выбор соответствующих столбцов приводит к удалению не менее двух строк. В противной ситуации рассмотрим два случая.

1. Граф второго рода пуст. Если $m < n$, то можно взять любые два столбца так, чтобы они различались хотя бы в одной строке. Если $m = n$ и есть хотя бы две строки первого рода, то можно взять два столбца, в которых одна из них принимает уникальное значение. Наконец, при $m = n$ и наличии не более одной строки первого рода общее количество вариантов выбора пар столбцов не меньше, чем $3(n-1)(n-3) + n - 1$, что больше, чем $\binom{n}{2}$. Поэтому какая-то пара встретится не менее двух раз.

2. Граф второго рода — объединение клики размера $l \geq 2$ и изоллированных вершин. Пусть в клику входят первые l вершин. Если имеется хотя бы одна строка первого или третьего рода, то, взяв два столбца: один из первых l , а другой — из оставшихся, которые отличаются в этой строке, получим утверждение леммы. Если строк первого и третьего родов нет, то при $l \geq 5$ матрицу моделирует функция

$$(x_1 \oplus x_{l+1}) \vee (x_2 \oplus x_{l+2}) \vee \cdots \vee (x_l \oplus x_{2l}).$$

При $l = 4$ с точностью до симметрий возможны два вида матриц:

$$\begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Данные матрицы моделируются функциями $x_6 \wedge (\overline{x_1} \vee \overline{x_2} \vee \overline{x_3} \vee \overline{x_4})$ и $(x_1 \oplus x_2) \vee (x_3 \oplus x_5)$ соответственно. ■

Для доказательства теоремы 1 достаточно воспользоваться леммами 1 и 2 и тем, что если функция φ моделирует матрицу, полученную из исходной по лемме 2 удалением i -го и j -го столбцов, то функция $(x_i \oplus x_j) \vee \varphi$ моделирует исходную матрицу.

Перейдем к доказательству верхней оценки — теоремы 2.

Дерево называется *каноническим*, если оно удовлетворяет следующим условиям:

- 1) Листья помечены попарно различными переменными или отрицаниями переменных.
- 2) Внутренние вершины помечены одним из следующих символов: $\wedge$, $\vee$, $\oplus$, $\overline{\oplus}$ (вершины любой степени захода, которым соответствует конъюнкция, дизъюнкция, сумма по модулю 2 или ее отрицание).

- 3) Смежные вершины не могут быть помечены одинаковыми символами из множества $\{\wedge, \vee, \oplus, \overline{\oplus}\}$, а также символами $\oplus$ и $\overline{\oplus}$ одновременно.
- 4) Корень расположен снизу. Вершина, смежная сверху с вершиной, помеченной $\oplus$ или $\overline{\oplus}$, не может быть помечена ни отрицанием переменной, ни конъюнкцией.

В работе [3] доказывается следующий факт.

Утверждение 1. Любая бесповторная функция (зависящая хотя бы от одной переменной) в бинарном базисе представима единственным каноническим деревом.

Переменную x_i назовем *особой* для функции $f(x_1, \dots, x_n)$, если для любой другой переменной x_j подстановкой констант на места оставшихся переменных можно либо получить как линейную, так и нелинейную функции, существенно зависящие от x_i и x_j , либо получить две нелинейных функции переменных x_i и x_j , одна из которых становится константой при подстановке $x_i = 0$, другая — при подстановке $x_i = 1$.

Из утверждения 1 вытекает

Лемма 3. Бесповторная в бинарном базисе функция не имеет особых переменных.

Лемма 4. Переменная x_1 — особая для функций семейства $f_t^{(s)}$. Для доказательства этого достаточно предъявить $4s$ наборов.

Доказательство. Подстановки $x_2 = \dots = x_{j-1} = x_{j+1} = \dots = x_s = 0$ дают всевозможные подфункции вида $\overline{x_1} \wedge \overline{x_j}$, а подстановки $x_2 = \dots = x_{j-1} = x_{j+1} = \dots = x_s = 1$ — вида $x_1 \wedge x_j$. Общее число различных наборов равно $4s$. ■

Лемма 5. Переменная x_2 — особая для функций семейства $f_m^{(s)}$. Для доказательства этого достаточно предъявить $4s$ наборов.

Доказательство. Подстановки $x_1 = 1, x_3 = \dots = x_{j-1} = x_{j+1} = \dots = x_s = 0$ дают всевозможные подфункции вида $x_2 \vee x_j$ для $j \geq 3$, а подстановки $x_1 = 0, x_3 = \dots = x_{j-1} = x_{j+1} = \dots = x_s = 1$ — всевозможные подфункции вида $x_2 \wedge x_j$ для $j \geq 3$. Подстановки $x_3 = \dots = x_s = 0$ и $x_3 = \dots = x_s = 1$ дают подфункции $x_2 \wedge x_1$ и $x_2 \vee x_1$ соответственно. Общее число различных наборов равно $4s$. ■

В каноническом дереве назовем *эквивалентными* переменные или отрицания переменных, если помеченные ими вершины смежны с одной внутренней вершиной. Если вершина, помеченная x_j или $\overline{x_j}$, лежит в корневом поддереве с корнем — вершиной, смежной с вершиной, помеченной x_i или $\overline{x_i}$, то скажем, что переменная x_i *не слабее* переменной x_j .

Лемма 6. Для доказательства повторности функции семейства $f_d^{(s)}$ достаточно предъявить $4s$ наборов.

Доказательство. Подстановки $x_1 = 1, x_2 = 0, x_4 = \dots = x_{j-1} = x_{j+1} = \dots = x_s = 1$ дают всевозможные подфункции вида $x_3 \wedge x_j$ для $j \geq 4$, а подстановки $x_1 = 0, x_2 = 1, x_4 = \dots = x_{j-1} = x_{j+1} = \dots = x_s = 0$ — всевозможные подфункции вида $\overline{x_3} \wedge \overline{x_j}$ для $j \geq 4$. При этом подстановка $x_2 = 0, x_4 = \dots = x_s = 1$ дает остаточную функцию $x_3 \wedge x_1$, подстановка $x_1 = x_4 = \dots = x_s = 1$ — остаточную функцию $x_3 \vee x_2$, а подстановка $x_1 = 0, x_4 = \dots = x_s = 1$ — остаточную функцию $\overline{x_3} \wedge x_2$. В силу значений функции при этих подстановках переменная x_3 не может быть не слабее переменных $x_4, \dots, x_s$ и не может быть эквивалентна переменной x_2 . Остаются неопровергнутыми два варианта для бесповторной реализации.

1. Переменная x_3 эквивалентна x_1 . Тогда для гипотетической неповторной функции можно сделать замену $u = x_3 \wedge x_1$, что противоречит соотношению $f(1101 \dots 1) \neq f(01 \dots 1)$.

2. Переменная x_3 не слабее эквивалентных друг другу переменных x_1 и x_2 . Подстановка $x_3 = 0, x_4 = \dots = x_s = 1$ дает остаточную функцию $x_1 \wedge x_2$. Тогда для гипотетической неповторной функции можно сделать замену $u = x_1 \wedge x_2$. Противоречивым окажется соотношение $f(101 \dots 1) \neq f(01 \dots 1)$.

Общее число различных наборов не превосходит $4s$. ■

Лемма 7. Для доказательства повторности функции Стеценко f_5 достаточно предъявить 14 наборов.

Доказательство. Подстановка $x_2 = 0, x_4 = 1, x_5 = 0$ дает подфункцию $x_1 \wedge x_3$, подстановка $x_2 = 1, x_4 = 0, x_5 = 1$ — подфункцию $x_1 \vee x_3$. Таким образом, между x_1 и x_3 и нелинейной связкой в гипотетической неповторной формуле должны быть линейные связки, как и после нелинейной связки, т. е. формула имеет вид

$$((x_1 \oplus x_i^{\sigma_i}) \vee (x_3 \oplus x_j^{\sigma_j})) \oplus x_k^{\sigma_k},$$

где $\{i, j, k\} = \{2, 4, 5\}$. При этом остаточные функции переменных x_i, x_k и x_j, x_k будут линейными. Подстановка $x_1 = 1, x_2 = 0, x_3 = 1$ дает подфункцию $x_4 \vee x_5$, а подстановка $x_1 = 0, x_3 = 0, x_5 = 1$ — подфункцию $x_2 \wedge x_4$. Имеем противоречие. Получаемые при подстановках четверки имеют общие наборы. Общее количество различных наборов равно 14. ■

Доказательство теоремы 2. Выделим по теореме Перязева подфункцию $s \leq n$ переменных. При $s \leq 4$ теорема вытекает из неравенства $2^s \leq 4s$, при больших n — из лемм 4, 5, 6 и 7.

ЛИТЕРАТУРА

1. Стеценко В. А. О предплюх базисах в P_2 // Матем. вопросы кибернетики. Вып. 4. М.: Физматлит, 1992. С. 139–177.
2. Перязев Н. А. Слабоповторные булевы функции в бинарном базисе // Дискретная математика и информатика. Вып. 4. Иркутск: Изд-во Иркут. ун-та, 1998. 12 с.
3. Вороненко А. А. О проверяющих тестах для неповторных функций // Матем. вопросы кибернетики. Вып. 11. М.: Физматлит, 2002. С. 163–176.