ИТОГИ НАУКИ И ТЕХНИКИ.
Современная математика и ее приложения.
Тематические обзоры.
Том 224 (2023). С. 71–79
DOI: 10.36535/0233-6723-2023-224-71-79

УДК 519.714.24

О СИММЕТРИЧЕСКИХ БУЛЕВЫХ ФУНКЦИЯХ, ИНВАРИАНТНЫХ ОТНОСИТЕЛЬНО ПРЕОБРАЗОВАНИЯ МЁБИУСА

© 2023 г. **О. В. ЗУБКОВ**

Аннотация. Работа посвящена изучению класса инвариантных относительно преобразования Мёбиуса булевых функций. В первой части статьи систематизирована общая информация по преобразованию Мёбиуса и его неподвижным точкам. Во второй части статьи рассмотрен класс симметрических булевых функций, инвариантных относительно преобразования Мёбиуса. Показана взаимосвязь этих функций со столбцами треугольника Серпинского. Приведен метод получения масок всех таких функций в виде суммы столбцов треугольника Серпинского. Для случая $n = 2^m - 1$ доказано, что симметрическая функция инвариантна тогда и только тогда, когда инвариантна её маска.

***Ключевые слова*:** полином Жегалкина, преобразование Мёбиуса, инварианты преобразования Мёбиуса, стационарные функции, симметрические булевы функции, вес двоичного набора.

ON SYMMETRIC BOOLEAN FUNCTIONS INVARIANT UNDER THE MÖBIUS TRANSFORM

© 2023 **O. V. ZUBKOV**

Abstract. The work is devoted to the study of the class of Boolean functions that are invariant under the Möbius transform. In the first part of the paper, we systematize general information on the Möbius transform and its fixed points. In the second part, we consider a class of symmetric Boolean functions that are invariant under the Möbius transform. The relationship of these functions with columns of the Sierpinski triangle is shown. We propose a method for obtaining masks of all such functions as sums of columns of the Sierpinski triangle. For the case $n = 2^m - 1$, we proved that a symmetric function is invariant if and only if its mask is invariant.

***Keywords and phrases*:** algebraic normal form, Möbius transform, coincident functions, symmetric Boolean functions, weight of a binary set.

***AMS Subject Classification*:** 93B50

1. Необходимые определения. Будем использовать следующие обозначения. Множество из двух элементов $\{0, 1\}$ будем обозначать через E_2, а множество двоичных наборов длины n — через E_2^n. Все 2^n таких наборов будем считать упорядоченными натуральным образом от $(0, \ldots, 0)$ до $(1, \ldots, 1)$; каждому набору поставим в соответствие число от 0 до $2^n - 1$, двоичным представлением которого является этот набор. Далее двоичные наборы будем обозначать малыми греческими буквами со знаком $\widetilde{\ }$ над ними, например $\widetilde{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. Весом Хэмминга (или просто весом) двоичного набора называется число единиц в нем. Будем писать $\widetilde{\alpha} \leqslant \widetilde{\beta}$, если $\alpha_i \leqslant \beta_i$ для любого $1 \leqslant i \leqslant n$.

Булевой функцией f от n переменных $x_1, \ldots, x_n$ называется отображение $f : E_2^n \to E_2$. Множество всех булевых функций от n переменных обозначим через $P_2(n)$. Каждой булевой функции f от n переменных поставим в соответствие вектор её значений длины 2^n, который перечисляет для

всех натурально упорядоченных наборов значения функции f на этих наборах. Вектор значений функции f будем обозначать через $\widetilde{f}$ в матричных преобразованиях.

Нулевой остаточной по i-й переменной для функции $f(x_1,\dots,x_n)$ называется функция от $n-1$ переменных $f^0_{x_i} = f(x_1,\dots,x_{i-1},0,x_{i+1},\dots,x_n)$. Аналогично определим единичную остаточную $f^1_{x_i} = f(x_1,\dots,x_{i-1},1,x_{i+1},\dots,x_n)$. Верно разложение вида $f = \overline{x}_i \cdot f^0_{x_i} \oplus x_i \cdot f^1_{x_i}$.

Булева функция называется симметрической, если при произвольной перестановке переменных вектор её значений не изменяется. Данное свойство эквивалентно следующему: значения функции f на любых двух наборах одинакового веса всегда совпадают.

Любая ненулевая булева функция может быть представлена единственным образом в виде полинома Жегалкина (алгебраической нормальной формы) следующего вида:

$$f(x_1,\dots,x_n) = \bigoplus_{(\alpha_1,\dots,\alpha_n)\in E_2^n} g(\alpha_1,\dots,\alpha_n) x_1^{\alpha_1}\cdots x_n^{\alpha_n},$$

где g — вектор коэффициентов её полинома Жегалкина, а выражение $x_i^{\alpha_i}$ равно x_i, если $\alpha_i = 1$, и 1 в противном случае. Далее этот вектор коэффициентов g длины 2^n будем также рассматривать как булеву функцию от n переменных $g(x_1,\dots,x_n)$.

2. Преобразование Мёбиуса для булевых функций и треугольник Серпинского. Упомянутое выше отображение функции f в вектор коэффициентов g её полинома назвается преобразованием Мёбиуса для булевых функций. Далее будем обозначать это преобразование через $\mu(f)$. Если g — вектор коэффициентов полинома для функции f, то $\mu(f) = g$. Для вычисления $\mu(f)$ по вектору функции f будем использовать матрицу преобразования Мёбиуса T_n, которая определяется следующим образом:

$$T_0 = 1, T_n = \begin{bmatrix} T_{n-1} & 0_{2^{n-1}} \\ T_{n-1} & T_{n-1} \end{bmatrix}, \tag{1}$$

где $0_{2^{n-1}}$ — нулевая матрица размера $2^{n-1}\times 2^{n-1}$. Отметим следующие полезные для дальнейших рассуждений свойства матрицы преобразования Мёбиуса:

(i) i-й столбец матрицы, при нумерации с 0, образует вектор значений монома $x_1^{\alpha_1}\cdots x_n^{\alpha_n}$, где $(\alpha_1,\alpha_2,\dots,\alpha_n)$ — двоичное представление числа i;

(ii) матрица T_n содержит в точности остатки от деления соответствующих биномиальных коэффициентов треугольника Паскаля по модулю 2; этот треугольник называется треугольником Серпинского (см. [8]).

Матрица T_3 представлена в таблице 1.

Таблица 1

	0	1	2	3	4	5	6	7
0:	1	0	0	0	0	0	0	0
1:	1	1	0	0	0	0	0	0
2:	1	0	1	0	0	0	0	0
3:	1	1	1	1	0	0	0	0
4:	1	0	0	0	1	0	0	0
5:	1	1	0	0	1	1	0	0
6:	1	0	1	0	1	0	1	0
7:	1	1	1	1	1	1	1	1

Сведения о преобразовании Мёбиуса подробно систематизированы в [7]. В частности, там показано, что

$$\mu(f) = T_n \times \widetilde{f}, \tag{2}$$

где n — число переменных функции f. Там же показано, что матрица T_n является обратной к самой себе, т.е. $T_n^2 = E_n$, где E_n — единичная матрица размера n. Этот факт влечет инволютивность преобразования Мёбиуса; иными словами верно соотношение

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

Для вычисления вектора коэффициентов полинома $g = \mu(f)$ имеется и другой способ, указанный в [4, с.Ё69] и в [6, с. 372]. Для того, чтобы вычислить значение $g(\widetilde{\alpha})$, нужно просуммировать значения функции f на всех наборах, меньших либо равных $\widetilde{\alpha}$:

$$\mu(f)(\widetilde{\alpha}) = \bigoplus_{\widetilde{\beta} \leqslant \widetilde{\alpha}} f(\widetilde{\beta}). \tag{3}$$

Помимо упомянутых выше свойств преобразования Мёбиуса, дополнительно отметим еще ряд свойств, приведенных в [7]:

(iii) $\mu(f_1 \oplus f_2) = \mu(f_1) \oplus \mu(f_2)$;

(iv) если $x_{i_1}, \ldots, x_{i_n}$ — некоторая перестановка переменных, то

$$\mu(f(x_{i_1}, \ldots, x_{i_n})) = \mu(f)(x_{i_1}, \ldots, x_{i_n});$$

(v) если $f^0_{x_i}$ и $f^1_{x_i}$ — соответственно нулевая и единичная остаточные по аргументу x_i функции f, то

$$\mu(f) = \overline{x}_i \cdot \mu(f^0_{x_i}) \oplus x_i \cdot \left(\mu(f^0_{x_i} \oplus f^1_{x_i})\right)$$

для любой переменной x_i;

(vi) если $f_1 \otimes f_2$ — кронекерово произведение функций f_1 и f_2 (в векторе f_1 все единицы заменяются на вектор f_2, а все нули на вектор из нулей такой же длины, как и вектор f_2), то

$$\mu(f_1 \otimes f_2) = \mu(f_1) \otimes \mu(f_2).$$

3. Инвариантные относительно преобразования Мёбиуса функции и их свойства. Далее нас будет интересовать класс булевых функций, являющихся неподвижными точками оператора μ. Основные результаты по этому классу функций приводятся в [7], где они называются «coincident Boolean functions». В данной работе будем называть эти функции «инвариантными относительно преобразования Мёбиуса» или <инвариантными» (см. [1], где рассмотрена связь этого класса функций с множеством чётных функций).

Определение 1. Булеву функцию f будем называть инвариантной относительно преобразования Мёбиуса, если $\mu(f) = f$.

Из свойств преобразования Мёбиуса имеется ряд важных следствий для инвариантных относительно этого преобразования функций (см. [7]):

(a) если функция $f(x_1, \ldots, x_n)$ инвариантна относительно преобразования Мёбиуса, то $T_n \times \widetilde{f} = \widetilde{f}$;

(b) если функции f_1 и f_2 инвариантны, то $f_1 \oplus f_2$ также является инвариантной;

(c) если $x_{i_1}, \ldots, x_{i_n}$ — некоторая перестановка переменных и $f(x_1, \ldots, x_n)$ — инвариантная функция, то $f(x_{i_1}, \ldots, x_{i_n})$ также инвариантна относительно преобразования Мёбиуса;

(d) если $f_1(\widetilde{x_1})$ и $f_2(\widetilde{x_2})$ — две инвариантные функции с непересекающимися множествами переменных $\widetilde{x_1}$ и $\widetilde{x_2}$, объединение которых есть множество всех переменных $x_1, \ldots, x_n$, то их кронекерово произведение $f_1 \otimes f_2$ и, в частности, конъюнкция $f_1 \cdot f_2$, также являются инвариантными функциями. Как следствие, можно заметить, что бесповторная конъюнкция дизъюнкций вида

$$\left(\bigvee_{x_i \in X_1} x_i\right) \cdot \left(\bigvee_{x_i \in X_2} x_i\right) \cdots \left(\bigvee_{x_i \in X_m} x_i\right)$$

инвариантна относительно преобразования Мёбиуса, где $X_1, \ldots, X_m$ — разбиение множества всех переменных $x_1, \ldots, x_n$ на непересекающиеся классы (см. [2]);

(e) функция $f(x_1,\dots,x_n)$ является инвариантной тогда и только тогда, когда

$$f(\alpha_1,\dots,\alpha_n)=\bigoplus_{\widetilde{\beta}\leqslant\widetilde{\alpha}} f(\widetilde{\beta})$$

для любого набора $\alpha_1,\dots,\alpha_n$;

(f) функция $f\oplus\mu(f)$ инвариантна относительно преобразования Мёбиуса.

4. Центральные функции и разбиение всех булевых функций на классы. Согласно свойству (f) для любой функции f функция $f\oplus\mu(f)$ инвариантна относительно преобразования Мёбиуса.

Определение 2. Пусть $h=f\oplus\mu(f)$. Инвариантную функцию h будем называть центральной для функции f. Будем говорить, что f принадлежит классу функции h.

Таким образом, для функции f определено еще одно преобразование Ψ, ставящее в соответсвие этой функции её центральную функцию: $\Psi(f)=f\oplus\mu(f)=h$. Определим матрицу

$$T_n^*=T_n\oplus E_{2^n}, \tag{4}$$

где E_{2^n} — единичная матрица размера $2^n\times 2^n$. Тогда $\Psi(f)=T_n^*\times\widetilde{f}$, т.е. оператор Ψ линеен: $\Psi(f\oplus g)=\Psi(f)\oplus\Psi(g)$.

Имеют место следующие свойства (см. [7]):

(I) инвариантная функция f принадлежит классу тождественно нулевой функции; иными словами, f инвариантна тогда и только тогда, когда $\Psi(f)=\widetilde{0}$. Как следствие, можно получить следующий важный факт: $f(x_1,\dots,x_n)$ инвариантна тогда и только тогда, когда

$$T_n^*\times\widetilde{f}=\widetilde{0}; \tag{5}$$

(II) две функции f_1 и f_2 принадлежат классу одной и той же инвариантной функции h тогда и только тогда, когда функция $f_1\oplus f_2$ инвариантна относительно преобразования Мёбиуса. Отсюда следует, что множество $P_2(n)$ всех булевых функций от n переменных разбивается на смежные классы по множеству инвариантных функций от n переменных;

(III) если f — инвариантная функция и $f^1_{x_i}$ — единичная остаточная f по произвольному аргументу x_i, то

$$f=\overline{x}_i\cdot\Psi(f^1_{x_i})\oplus x_i\cdot f^1_{x_i}. \tag{6}$$

Иными словами, у инвариантной функции нулевая остаточная по любой переменной является центральной для её единичной остаточной по этой переменной;

(IV) обратно, для любой функции $g(x_1,\dots,x_{i-1},x_{i+1},\dots,x_n)$, не зависящей от переменной x_i, функция $\overline{x}_i\cdot\Psi(g)\oplus x_i\cdot g$ инвариантна относительно преобразования Мёбиуса;

(V) нулевая остаточная по любому множеству из нескольких переменных у инвариантной функции также является инвариантной;

(VI) число различных функций от n переменных, инвариантных относительно преобразования Мёбиуса, равно числу всех булевых функций от $n-1$ переменных, т.е. $2^{2^{n-1}}$.

5. Симметрические булевы функции, инвариантные относительно преобразования Мёбиуса. Основное содержание данной работы составляет исследование свойств симметрических инвариантных функций и их описание. Напомним, что f является симметрической, если $f(\widetilde{\alpha})=f(\widetilde{\beta})$ для любых двух наборов $\widetilde{\alpha}$ и $\widetilde{\beta}$ с равными весами.

Лемма 1. *Если функция f является симметрической, то $\mu(f)$ и $\Psi(f)$ также являются симметрическими функциями.*

Доказательство. Применим формулу (3) для вычисления функции $\mu(f)$ на двух наборах одинакового веса $\widetilde{\alpha}_1$ и $\widetilde{\alpha}_2$. Согласно этой формуле для нахождения $\mu(f)(\widetilde{\alpha}_1)$ нужно просуммировать значения $f(\widetilde{\beta})$ по всем наборам $\widetilde{\beta}$, не превосходящим $\widetilde{\alpha}_1$, а для нахождения $\mu(f)(\widetilde{\alpha}_2)$ нужно просуммировать значения $f(\widetilde{\gamma})$ по всем наборам $\widetilde{\gamma}$, не превосходящим $\widetilde{\alpha}_2$. Пусть w не превосходит веса наборов $\widetilde{\alpha}_1$ и $\widetilde{\alpha}_2$. Тогда число таких наборов $\widetilde{\beta}$ веса w, что $\widetilde{\beta}\leqslant\widetilde{\alpha}_1$, равно числу таких наборов

$\widetilde{\gamma}$ веса w, что $\widetilde{\gamma} \leqslant \widetilde{\alpha}_2$. Так как функция f симметрическая, то для любого веса все её значения на наборах этого веса будут одинаковы. Складывая одинаковые значения одинаковое количество раз, получим, что $\mu(f)(\widetilde{\alpha}_1)$ и $\mu(f)(\widetilde{\alpha}_2)$ получат одну и ту же добавку из наборов веса w. Так как это верно для любого w, меньшего либо равного весу этих наборов, то значения $\mu(f)(\widetilde{\alpha}_1)$ и $\mu(f)(\widetilde{\alpha}_2)$ совпадут на наборах одинакового веса $\widetilde{\alpha}_1$ и $\widetilde{\alpha}_2$, что влечет симметричность функции $\mu(f)$. Так как $\Psi(f) = f \oplus \mu(f)$ и оба слагаемых являются симметрическими функциями, то и $\Psi(f)$ будет симметрической. □

Симметрические функции удобно представлять в специальном виде при помощи перечисления множества весов (рабочих чисел) двоичных наборов, на которых они принимают значение 1 (см. [5, с. 367]. Далее, через $S(n, w_1, \ldots, w_k)$ обозначим симметрическую функцию от n переменных $x_1, \ldots, x_n$, равную 1 на наборах веса $w_1, \ldots, w_k$ и равную 0 на остальных наборах. Любой симметрической функции $S(n, w_1, \ldots, w_k)$ можно поставить в соответствие двоичный набор $\mathrm{mask}(S(n, w_1, \ldots, w_k))$ длины $n + 1$, нумерация элементов которого начинается с 0. В наборе $\mathrm{mask}(S(n, w_1, \ldots, w_k))$ единицы стоят в позициях $w_1, \ldots, w_k$, а в остальных позициях этого набора стоят нули. Этот набор будем называть маской для $S(n, w_1, \ldots, w_k)$.

Далее симметрическую функцию $S(n, w)$ с одним рабочим числом w будем называть элементарной.

Предложение 1 (см. [3]). *Пусть число $w + 1$ делится на 2^k и не делится на 2^{k+1}. Тогда все элементарные функции $S(i, w)$ для i от 0 до $w + 2^k - 1$ включительно будут инвариантными, а $S(w + 2^k, w)$ и все последующие таковыми не будут.*

Для более систематического описания функций $\mu(S(n, w))$ полезно рассмотреть треугольник Серпинского (см. [8]), в котором и строки и столбцы пронумеруем с 0. Первые строки этого треугольника представлены в таблице 2. Элемент этого треугольника, расположенный в i-й строке и j-м столбце, обозначим через $TS(i, j)$. Элементы на позициях, в которых номер строки меньше номера столбца (область выше главной диагонали), будем считать равными 0. В таблице 3 представлен аналогичный треугольник, у которого на главной диагонали находятся нули. Легко видеть, что первые 2^n строк таблицы 2 образуют матрицу T_n (см. (1)), а первые 2^n строк таблицы 3 образуют матрицу $T_n + E_n = T_n^*$ (см. (4)).

Матрицу, содержащуюся в строках таблицы 2 от 0-й до n-й обозначим через TS_n, а матрицу, содержащуюся в строках таблицы 3 от 0-й до n-й, обозначим через TS_n^*.

Таблица 2

	0	1	2	3	4	5	6	7	8	9	10
0:	1										
1:	1	1									
2:	1	0	1								
3:	1	1	1	1							
4:	1	0	0	0	1						
5:	1	1	0	0	1	1					
6:	1	0	1	0	1	0	1				
7:	1	1	1	1	1	1	1	1			
8:	1	0	0	0	0	0	0	0	1		
9:	1	1	0	0	0	0	0	0	1	1	
10:	1	0	1	0	0	0	0	0	1	0	1
11:	.	.	.	.	.	.	.	.	.	.	.

Таблица 3

	0	1	2	3	4	5	6	7	8	9	10
0:	0										
1:	1	0									
2:	1	0	0								
3:	1	1	1	0							
4:	1	0	0	0	0						
5:	1	1	0	0	1	0					
6:	1	0	1	0	1	0	0				
7:	1	1	1	1	1	1	1	0			
8:	1	0	0	0	0	0	0	0	0		
9:	1	1	0	0	0	0	0	0	1	0	
10:	1	0	1	0	0	0	0	0	1	0	0
11:	.	.	.	.	.	.	.	.	.	.	.

Лемма 2. *Для того чтобы получить $\mu(S(n,w))$, нужно просуммировать ровно те функции $S(n,i), i \leqslant n$, для которых $TS(i,w)$ равно* 1. *Иными словами,*

$$\mu(S(n,w)) = \bigoplus_{i=0}^{n} TS(i,w) \cdot S(n,i).$$

Доказательство. Найдем зачения $\mu(S(n,w))$ по формуле (3). Чтобы получить значение $\mu(S(n,w))$ на наборе $\widetilde{\alpha}$ веса i, нужно просуммировать все значения функции $S(n,w)$ на всех наборах, меньших либо равных набору $\widetilde{\alpha}$. Среди этих наборов только на наборах веса w функция $S(n,w)$ равна 1. Отсюда получим, что значение функции $\mu(S(n,w))$ на наборе $\widetilde{\alpha}$ веса i вычисляется как остаток от деления на 2 биномиального коэффициента $\binom{i}{w}$. Согласно лемме 1, для симметрической функции $S(n,w)$ функция $\mu(S(n,w))$ также является симметрической. Таким образом, для веса i все значения $\mu(S(n,w))$ на наборе $\widetilde{\alpha}$ веса i равны $TS(i,w)$. Если сгруппировать эти наборы по их весам, то получим лемму 2. □

Следствие 1. *Сумма по всем i от $w+1$ до n всех функций $S(n,i)$, для которых $TS(i,w)$ равно* 1, *является симметрической инвариантной функцией. Эта функция равна $\Psi(S(n,w))$.*

Доказательство. По определению $\Psi(f) = f \oplus \mu(f)$. Согласно лемме 2,

$$\mu(S(n,w)) = \bigoplus_{i=0}^{n} TS(i,w) \cdot S(n,i).$$

Функция $S(n,w)$ соответствует элементу $TS(w,w)$, который всегда равен 1, т.е. слагаемое $S(n,w)$ всегда входит в эту сумму. Прибавив к этой сумме $TS(w,w) \cdot S(n,w)$ (что равносильно удалению из этой суммы данного слагаемого), получим

$$\Psi(S(n,w)) = \bigoplus_{i=w+1}^{n} TS(i,w) \cdot S(n,i),$$

что и требовалось. □

Переходя к матричной форме записи результатов леммы 2 и следствия 1, получим:

$$\operatorname{mask}(\mu(S(n,w))) = TS_n \times \operatorname{mask}(S(n,w)), \tag{7}$$

$$\operatorname{mask}(\Psi(S(n,w))) = TS_n^* \times \operatorname{mask}(S(n,w)). \tag{8}$$

Так как оператор Мёбиуса μ и оператор Ψ линейны, а также линейно произведение матрицы на вектор, формулы (7) и (8) можно легко обобщить на случай произвольных симметрических функций:

$$\operatorname{mask}(\mu(S(n,w_1,\ldots,w_k))) = TS_n \times \operatorname{mask}(S(n,w_1,\ldots,w_k)), \tag{9}$$

$$\operatorname{mask}(\Psi(S(n,w_1,\ldots,w_k))) = TS_n^* \times \operatorname{mask}(S(n,w_1,\ldots,w_k)). \tag{10}$$

Из формулы (10) и свойства (5) вытекает теорема.

Теорема 1. *Симметрическая функция $S(n,w_1,\ldots,w_k)$ инвариантна относительно преобразования Мёбиуса тогда и только тогда, когда*

$$TS_n^* \times \operatorname{mask}(S(n,w_1,\ldots,w_k)) = \widetilde{0}. \tag{11}$$

Пример 1. Рассмотрим симметрическую инвариантную функцию $S(5,1,2,4)$. Её маска имеет вид (011010), а вектор равен

(0111 1110 1110 1001 1110 1001 1001 0110).

Если умножить матрицу TS_5^* на вектор-столбец маски (011010), то в итоге просуммируются первый, второй и четвертый столбцы матрицы TS_5^* (отсчет с нуля). Эти столбцы имеют соответственно вид (000101) $\oplus$ (000100) $\oplus$ (000001) и в сумме дают нулевой вектор-столбец.

6. Описание класса симметрических инвариантных относительно преобразования Мёбиуса булевых функций. В этом разделе опишем методы, при помощи которых можно получить все симметрические булевы функции, инвариантные относительно преобразования Мёбиуса.

Согласно формуле (8) любой столбец матрицы TS_n^* является маской для некоторой симметрической инвариантной функции, а значит, произвольная сумма таких столбцов также образует маску для инвариантной функции. Из формулы (10) видно, что маску для некоторой инвариантной функции $S'(n, z_1, \ldots, z_p) = \Psi(S(n, w_1, \ldots, w_k))$ можно получить в виде суммы столбцов матрицы TS_n^*, соответствующих единицам маски симметрической функции $S(n, w_1, \ldots, w_k)$, для которой S' является центральной. Очевидно, что такое представление не обязательно единственно, так как одна и та же функция S' может быть центральной для нескольких различных симметрических функций. С другой стороны, явного метода получения маски произвольной инвариантной функции $S'(n, z_1, \ldots, z_p)$ при помощи суммы столбцов матрицы TS_n^* пока нет.

Следующая теорема дает метод получения маски произвольной инвариантной относительно преобразования Мёбиуса функции $S'(n, z_1, \ldots, z_p)$ при помощи суммы столбцов матрицы TS_n^* с точностью до значения этой функции на последнем единичном наборе.

Теорема 2. *Маска любой симметрической инвариантной относительно преобразования Мёбиуса функции $S'(n, z_1, \ldots, z_p)$ может быть получена как сумма столбцов матрицы TS_n^* с номерами $z_i - 1$ и, возможно, маски многоместной конъюнкции $S(n, n)$.*

Доказательство. Для функции $S'(n, z_1, \ldots, z_p)$ возьмем единичную остаточную по любому аргументу (в силу симметричности все единичные остаточные будут между собой равны). Эта единичная остаточная будет равна $S''(n-1, z_1-1, \ldots, z_p-1)$, так как веса всех наборов уменьшатся на 1 и число переменных так же будет на 1 меньшим. Согласно (10), $\Psi(S'') = TS_{n-1}^* \times \mathrm{mask}(S'')$.

С другой стороны, $\Psi(S'')$ равна нулевой остаточной для исходной $S'(n, z_1, \ldots, z_p)$ согласно (6). Добавив к матрице TS_{n-1}^* n-ю строку, получим матрицу T_n^*. Добавив к вектору $\mathrm{mask}(S'')$ еще один бит, равный 0, в позицию n, получим вектор $\mathrm{mask}(S'') + 0$; здесь знак «+» означает конкатенацию. Тогда $TS_n^* \times (\mathrm{mask}(S'') + 0)$ определит некоторую симметрическую инвариантную функцию от n переменных, у которой нулевая остаточная совпадет с нулевой остаточной для исходной функции $S'(n, z_1, \ldots, z_p)$. В силу симметричности последней, по ее нулевой остаточной однозначно восстанавливается единичная остаточная, за исключением значения на последнем наборе веса n.

Таким образом, формула $TS_n^* \times (\mathrm{mask}(S'') + 0)$ определяет либо маску самой функциии $S'(n, z_1, \ldots, z_p)$, либо маску функциии $S'(n, z_1, \ldots, z_p) \oplus S(n, n)$. □

Пример 2. При четном n возможны оба случая относительно необходимости корректировки при помощи функции $S(n, n)$. Например для симметрической инвариантной функции $S'(4, 1, 2)$, маска которой имеет вид (01100), а вектор самой этой функции имеет вид (0111 1110 1110 1000), единичная остаточная S'' имеет вид (1110 1000), и маска для неё имеет вид (1100). Просуммировав нулевой и первый столбцы матрицы TS_4^*, получим маску (01101), т.е. в данном случае $TS_4^* \times (\mathrm{mask}(S'') + 0)$ соответствует маске функции $S(4, 1, 2, 4)$ или $S'(4, 1, 2) \oplus S(4, 4)$.

Если же изначально взять в качестве целевой функцию $S'(4, 1, 2, 4)$ с маской (01101) и вектором (0111 1110 1110 1001), то, повторяя рассуждения, получим маску для единичной остаточной (1101); просуммировав нулевой, первый и третий столбцы TS_4^*, опять получим (01101), что и является маской для исходной S'.

Такая неопределенность при четном n связана с тем, что в этом случае $(n-1)$-й столбец матрицы TS_n^* полностью нулевой, и скорректировать при помощи него последний элемент маски не получится.

При нечетном n метод работает без коррекции. Например рассмотрим инвариантную функцию $S'(5, 1, 2, 4)$. Её маска имеет вид (011010), а вектор равен (0111 1110 1110 1001 1110 1001 1001 0110). Единичная остаточная имеет маску (11010); суммируя нулевой, первый и третий столбцы TS_5^*, получим (011010), т.е. маску для исходной $S'(5, 1, 2, 4)$. Если же исходно взять стационарную функцию $S'(5, 1, 2, 4, 5)$ с маской (011011), то в итоге получим маску для её единичной остаточной

(11011); суммируя нулевой, первый, третий и четвертый столбцы TS_5^*, получим на этот раз маску (011001), что опять является маской для исходной $S'(5,1,2,4,5)$.

Полученное в теореме 2 представление для произвольной симметрической инвариантной функции является в некотором смысле каноническим. В то же время оно не позволяет, например, ответить на вопрос о количестве симметрических инвариантных функций от n переменных. Метод, позволяющий перечислить все такие функции, и полностью описывающий их множество для случая $n = 2^m - 1$ представлен в следующей теореме.

Теорема 3. *Пусть $n = 2^m - 1$, где m — натуральное число, и симметрическая функция $S(n, w_1, \ldots, w_k)$ имеет маску* $\mathrm{mask}(S)$*, которая имеет длину 2^m и является вектором для некоторой функции $f(x_1, \ldots, x_m)$. Тогда верны следующие утверждения*:

(A) $\mathrm{mask}(\mu(S)) = \mu(\mathrm{mask}(S))$;

(B) *симметрическая функция S инвариантна относительно преобразования Мёбиуса тогда и только тогда, когда её маска* $\mathrm{mask}(S)$ *является вектором инвариантной относительно преобразования Мёбиуса функции f.*

Доказательство. Ранее уже отмечалось, что матрица треугольника Серпинского TS_{2^m-1} совпадает с матрицей преобразования Мёбиуса T_m. Согласно (9) имеем $\mathrm{mask}(\mu(S)) = TS_n \times \mathrm{mask}(S)$. Так как TS_n совпадает с T_m и верно (2), имеем $TS_n \times \mathrm{mask}(S) = \mu(\mathrm{mask}(S))$. Из этих двух равенств следует утверждение (A) теоремы.

Для доказательства утверждения (B) воспользуемся утверждением (A). Если функция S инвариантна, то $\mathrm{mask}(S) = \mathrm{mask}(\mu(S)) = \mu(\mathrm{mask}(S))$, т.е. функция $f = \mathrm{mask}(S)$ является инвариантной. Обратно, пусть функция $f = \mathrm{mask}(S)$ является инвариантной; тогда $\mathrm{mask}(\mu(S)) = \mu(\mathrm{mask}(S)) = \mathrm{mask}(S)$. Если совпадают маски для $\mu(S)$ и S, то совпадают и сами эти функции, т.е. S является инвариантной. □

Пример 3. Пусть $\mathrm{mask}(S) = (1011)$. Тогда $S = (1001\ 0111)$, $\mu(S) = (1110\ 1001)$. В итоге $\mu(\mathrm{mask}(S)) = (1101)$ и $\mathrm{mask}(\mu(S)) = (1101)$, что согласуется с утверждением (A) теоремы 3.

Пример 4. Пусть $m = 2$. Запишем все инвариантные функции от двух переменных: (0000), (0001), (0110), (0111). Рассматривая их как маски для симметрических функций от трёх переменных ($3 = 2^2 - 1$) получим описание всех таких инвариантов преобразования Мёбиуса: (0000 0000), $S(3,3) = (0000\ 0001)$, $S(3,1,2) = (0111\ 1110)$, $S(3,1,2,3) = (0111\ 1111)$.

Пример 5. Для $m = 3$ имеется 16 инвариантных функций от трех переменных. Соответственно, имеется 16 симметрических инвариантов преобразования Мёбиуса от семи переменных. Далее приведем соответствующие пары $\mathrm{mask}(S) \leftrightarrow S$:

$(0000\ 0000) \leftrightarrow 0_{2^7}$,
$(0000\ 0001) \leftrightarrow S(7,7)$,
$(0000\ 0110) \leftrightarrow S(7,5,6)$,
$(0000\ 0111) \leftrightarrow S(7,5,6,,7)$
$(0001\ 0010) \leftrightarrow S(7,3,6)$,
$(0001\ 0011) \leftrightarrow S(7,3,6,7)$,
$(0001\ 0100) \leftrightarrow S(7,3,5)$,
$(0001\ 0101) \leftrightarrow S(7,3,5,7)$,
$(0110\ 1010) \leftrightarrow S(7,1,2,4,6)$,
$(0110\ 1011) \leftrightarrow S(7,1,2,4,6,7)$,
$(0110\ 1100) \leftrightarrow S(7,1,2,4,5)$,
$(0110\ 1101) \leftrightarrow S(7,1,2,4,5,7)$,
$(0111\ 1000) \leftrightarrow S(7,1,2,3,4)$,
$(0111\ 1001) \leftrightarrow S(7,1,2,3,4,7)$,
$(0111\ 1110) \leftrightarrow S(7,1,2,3,4,5,6)$,
$(0111\ 1111) \leftrightarrow S(7,1,2,3,4,5,6,7)$.

Следствие 2. *Для $n = 2^m - 1$, где $m \in \mathbb{N}$, число симметрических функций от n переменных, инвариантных относительно преобразования Мёбиуса, равно числу всех инвариантных функций от m переменных и равно $2^{2^{m-1}}$.*

СПИСОК ЛИТЕРАТУРЫ

1. *Бухман А. В.* О распознавании функций, инвариантных относительно преобразования Мёбиуса, и чётных функций, заданных в форме полиномов// в кн.: Прикладная математика и информатика / Тр. ф-та ВМК МГУ им. М. В. Ломоносова. — М.: МАКС Пресс, 2012. — С. 105–112.
2. *Зубков О. В.* Представление полиномиально устойчивых функций суммами бесповторных в элементарном базисе слагаемых// Мат. 6 Междунар. школы-семинара «Синтаксис и семантика логических систем» (Монголия, Ханх, 11-16 августа 2019 г.). — Иркутск: Изд-во ИГУ, 2019. — С. 48–52.
3. *Зубков О. В.* О классе полиномиально устойчивых булевых функций// Итоги науки техн. Совр. мат. прилож. Темат. обзоры. — 2022. — *214*. — С. 37–43.
4. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004.
5. *Яблонский С. В.* Введение в дискретную математику. — М.: Высшая школа, 2001.
6. *MacWilliams F. J., Sloane N. J. A.* The theory of Error-Correcting Codes. — Amsterdam–New York–Oxford: Noth-Holland, 1978.
7. *Pieprzyk J., Zhang X.-M.* Computing Möbius transform of boolean functions and characterising coincident boolean functions// in: Boolean Functions: Cryptography and Applications. — Rouen, France: Publications des Univercites de Rouen et du Havre, 2007. — P. 135–151.
8. *Sloane N. J. A.* Rows of Sierpinski's triangle// `http://oeis.org/A006943/b006943.txt`.

Зубков Олег Владимирович
Иркутский государственный университет
E-mail: `oleg.zubkov@mail.ru`