УДК 519.7

А. А. Мазуров

О КОЛИЧЕСТВЕ ЧАСТИЧНО СТАЦИОНАРНЫХ ФУНКЦИЙ ТРЕХЗНАЧНОЙ ЛОГИКИ

Аннотация.

Актуальность и цели. Булевы и многозначные функции – основной объект изучения дискретной математики. Они представляют собой зависимости между величинами, принимающими конечный набор значений. Существует несколько способов описания таких зависимостей, и на практике часто встречается табличное задание функции и задание в виде полинома. Оба эти представления функций можно выразить в виде векторов. В случае табличного задания функции это вектор ее значений, в случае полиномиального задания – вектор коэффициентов полинома. Преобразование вектора значений функции в вектор коэффициентов ее полинома в булевом случае является преобразованием Мёбиуса. Неподвижные точки такого преобразования мы будем называть стационарными функциями. Пусть α – вектор, состоящий из *n* элементов поля E_3. α-преобразованием функции *f* будем называть такую функцию $g = \nu_{\tilde{\alpha}}(f)$, что $g(x_1,\ldots,x_n) = f(x_1+\alpha_1,\ldots,x_n+\alpha_n)$. Если $\nu_{\tilde{\alpha}}(f) = f$, то такую функцию будем называть частично стационарной относительно вектора α. Целью данной работы является нахождение количества частично стационарных функций в трехзначной логике для любого вектора α.

Материалы и методы. Нахождение количества частично стационарных функций основано на знании некоторых свойств таких функций, полученных в ходе исследования преобразования. Доказано, что количество частично стационарных функций зависит только от количества нулей, единиц и двоек в векторе α, и не зависит от их порядка в нем.

Выводы и результаты. Найдено точное количество частично стационарных относительно вектора α функций трехзначной логики для любого вектора α.

Ключевые слова: многозначные функции, преобразование Мёбиуса, частично стационарная функция, трехзначная логика.

A. A. Mazurov

ON THE QUANTITY OF PARTIALLY STATIONARY FUNCTIONS OF TERNARY LOGIC

Abstract.

Background. Boolean and multi-valued functions are the main research object of discrete mathematics. They represent dependences between values admitting the final value set. There several ways to describe such dependencies, and in practice one often encounters a tabular function set and a set in the form of a polynomial. Both these representations of functions may be expressed as vectors. In case of a tabular function set it is a vector of its values, in case of a polynomial set – a vector of polynomial coefficients. Transformation of a function value vector into a vector of coefficients of its polynomials in the Boolean case is the Mobius transformation. The fixed points of such transformation the author has suggested to call stationary functions. Let α be a vector consisting of *n* elements of E_3 field. α-transformation of *f* function shall be called such $g = \nu_{\tilde{\alpha}}(f)$ function that $g(x_1,\ldots,x_n) = f(x_1+\alpha_1,\ldots,x_n+\alpha_n)$. If $\nu_{\tilde{\alpha}}(f) = f$, then such function shall be called a partially stationary one relative to

α vector. The aim of the study is to find the quantity of partially stationary functions in ternary logic for any α vector.

Materials and methods. Finding the quantity of partially stationary functions is based on some features of such functions, obtained in the course of transformation research. It is proved that the quantity of partially stationary functions depends only on the number of zeros, ones and twos in α vector, and doesn't depend on their order in the vector.

Conclusion and results. The author found the precise quantity of partially stationary functions, relative to α vector, of ternary logic for any α vector.

Key words: multi-valued functions, Mobius transformation, partially stationary function, ternary logic.

Введение

Булевы и k-значные функции широко применяются в кибернетике и криптографии. Они выражают зависимости между величинами, принимающими только конечный набор значений. В связи с этим самый простой способ задания таких функций – табличный, когда выписываются все значения функции на всех наборах. Однако на практике из-за громоздкости он почти не применяется.

Более удобным является представление в виде полиномов. Известно, что для каждой функции существует единственное ее представление в виде полинома в том и только в том случае, когда k – простое число. Данный способ задания функций во многих случаях оказывается более удобным благодаря краткости и наглядности.

В работах [1–3] подробно рассмотрены свойства преобразования, которое по вектору значений функции строит вектор, состоящий из коэффициентов полинома. Были найдены и охарактеризованы с точки зрения некоторых алгебраических и криптографических свойств функции, являющиеся неподвижными точками такого преобразования. В работе [4] такие функции названы 1-инвариантными. Мы далее будем называть их стационарными. Свойства таких функций и их количество в трехзначной логике были установлены в работах [5–7].

Далее в основном будет рассматриваться случай трехзначной логики. Некоторые исследования, относящиеся к трехзначной логике, можно найти в [8, 9].

Здесь мы рассмотрим функции трехзначной логики, аналоги которых в булевой логике названы в работах [1–3] частично стационарными.

1. Основные понятия

Пусть k – натуральное число, $k \geq 2$. Множество всех натуральных чисел от 0 до $k-1$ обозначается через E_k : $E_k = \{0,\ldots,k-1\}$. Функцией k-значной логики от n переменных называется отображение $f : E_k^n \to E_k$. Множество всех функций k-значной логики от n переменных обозначается $P_k(n)$. Множество всех функций k-значной логики (от любого количества переменных) обозначается P_k.

Существуют различные способы задания функций k-значной логики, одними из наиболее часто встречающихся являются задания в виде вектора

значений функции или в виде ее полинома в случае, когда k – простое число. Рассмотрим эти способы.

Вектором значений функции f, зависящей от переменных $x_1,..., x_n$, называется вектор, элементами которого являются значения функции на всех наборах от $(0,\ldots,0)$ до $(k-1,\ldots,k-1)$ в лексикографическом порядке, т.е. на наборах, обозначающих числа от 0 до k^n-1 в k-чной системе счисления в порядке возрастания. Длина этого вектора равна k^n.

Везде далее будем отождествлять вектор значений функции f с самой этой функцией. Обозначать его будем либо также символом f, либо в некоторых случаях символом $\mathbf{f}$. Таким образом, функции-константы от различного числа переменных будем считать различными, так как у них различные векторы значений.

Также здесь и далее сложение и умножение элементов из E_k (а именно значений переменных и значений функций, коэффициентов полинома) ведется по модулю k.

Полиномом в k-значной логике называется формула вида

$$\sum_{\tilde{\alpha}\in E_k^n} c_{\tilde{\alpha}} x_1^{\alpha_1}\cdots x_n^{\alpha_n},$$

где $x^{\alpha}=\begin{cases}1, & \alpha=0,\\ \underbrace{x\cdot x\cdot\ldots\cdot x}_{\alpha}, & \alpha\neq 0.\end{cases}$

Числа $c_{\tilde{\alpha}}$ называются коэффициентами полинома.

Для любого простого числа k и любой функции $f\in P_k$ существует единственное представление этой функции в виде полинома с точностью до перестановки слагаемых [10]. Всюду далее будем считать k простым числом. Вектором коэффициентов полинома функции называется вектор

$$(c_{(0,\ldots,0)},\ \ldots\ , c_{(k-1,\ldots,k-1)}),$$

где индексы расположены в лексикографическом порядке.

Основной объект исследования в этой работе – это преобразование вектора значений функции в вектор коэффициентов соответствующего ей полинома. Называть его будем преобразованием Мёбиуса. Обозначать его будем так: $\mu(f)$ – преобразование Мёбиуса, примененное к вектору значений функции f. Таким образом, запись $g = \mu(f)$ означает, что вектор значений функции g совпадает с вектором коэффициентов полинома функции f. Это преобразование является линейным преобразованием над векторами из E_k^n. Матрицу этого преобразования для функций n переменных будем обозначать T_n. Будем также обозначать $\mu^2(f)$ результат двукратного применения преобразования Мёбиуса к вектору значений функции f.

Если для какой-то функции f оказывается, что $\mu(f) = f$, то это означает, что вектор значений функции совпадает с вектором коэффициентов ее полинома, поэтому такие функции представляют особый интерес.

Функцию $f\in P_k(n)$ назовем стационарной функцией относительно μ^p, $p\geq 1$, с константой m, если $\mu^p(f)=m\cdot f$, где $m\in E_k\setminus\{0\}$.

Стационарным классом $Q_m^p(n)$ (функций *n* переменных) с константой *m* относительно μ^p назовем множество всех стационарных функций *k*-значной логики (зависящих от *n* переменных) с константой *m* относительно μ^p: $Q_m^p(n) = \{f : \mu^p(f) = m \cdot p\}$.

Пусть $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$, где $\alpha_1, \ldots, \alpha_n \in E_3$, и пусть π – произвольная перестановка на множестве *n* элементов. Введем следующие обозначения: $\nu_{\tilde{\alpha}}(f) = f(x_1 + \alpha_1, \ldots, x_n + \alpha_n)$, $\rho_\pi(f) = f(\pi(x_1), \ldots, \pi(x_n))$. $\nu_{\tilde{\alpha}}(f)$ – иногда будем далее называть $\tilde{\alpha}$-преобразованием функции *f*. Преобразования $\nu_{\tilde{\alpha}}(f)$ и $\rho_\pi(f)$, как и $\mu(f)$, являются линейными преобразованиями векторов из E_k^n.

Частично стационарной по отношению к вектору $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ с константой *l* функцией будем называть такую функцию *f*, что $\mu(f) = l \cdot \nu_{\tilde{\alpha}}(f)$. Множество частично стационарных функций от *n* переменных по отношению к вектору $\tilde{\alpha}$ будем обозначать $V_{\tilde{\alpha}}(n)$.

2. Количество частично стационарных функций

Лемма 1. Пусть $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$, π – перестановка на множестве *n* элементов. Тогда $\rho_\pi(\nu_{\tilde{\alpha}}(f)) = \nu_{\pi^{-1}(\tilde{\alpha})}(\rho_\pi(f))$.

Доказательство. По определению, $\rho_\pi(\nu_{\tilde{\alpha}}(f(x))) = f(\pi(x) + \tilde{\alpha})$. Заметим, что перестановка индексов переменных – линейное преобразование в пространстве векторов значений функций. Поэтому $\pi(x) + \tilde{\alpha} = \pi(x + \pi^{-1}(\tilde{\alpha}))$ и, следовательно, $f(\pi(x) + \tilde{\alpha}) = f\left(\pi\left(x + \pi^{-1}(\tilde{\alpha})\right)\right)$. По определению, это означает, что $\rho_\pi(\nu_{\tilde{\alpha}}(f)) = \nu_{\pi^{-1}(\tilde{\alpha})}(\rho_\pi(f))$.

Теорема 1. Пусть π – произвольная перестановка на множестве *n* элементов. Количество частично стационарных функций по отношению к вектору $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ совпадает с количеством частично стационарных функций по отношению к вектору $\pi(\tilde{\alpha})$.

Доказательство. Заметим, что $\rho_\pi(\mu(f)) = \mu(\rho_\pi(f))$. Если *f* – частично стационарная функция по отношению к вектору $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$, то с учетом леммы 1 $(f_\pi)_\mu = (f_\pi)_{\pi^{-1}(\tilde{\alpha})}$. Если взять $g = \mu(f)$, то $g_\mu = g_{\pi^{-1}(\tilde{\alpha})}$. Обратное соответствие следует из только что доказанного путем замены $\pi(\tilde{\alpha})$ на $\pi^{-1}(\tilde{\alpha})$ и наоборот. Теорема доказана.

Из этой теоремы следует, что количество частично стационарных функций по отношению к вектору $\tilde{\alpha}$ зависит только от количества нулей, единиц и двоек в нем. Следовательно, достаточно рассматривать только векторы вида $\tilde{\alpha} = (1, \ldots, 1, 2, \ldots, 2, 0, \ldots, 0)$, в которых *m* нулей, *p* единиц и *q* двоек. Такой порядок удобно выбрать с точки зрения дальнейших рассуждений.

Теорема 2. Матрица преобразования $\nu_{\tilde{\alpha}}(f)$, где $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$, строится следующим образом:

$$\text{если } \alpha_1 = 0, \text{ то } \mathbf{P}_{\tilde{\alpha}} = \begin{bmatrix} \mathbf{P}_{\tilde{\beta}} & 0 & 0 \\ 0 & \mathbf{P}_{\tilde{\beta}} & 0 \\ 0 & 0 & \mathbf{P}_{\tilde{\beta}} \end{bmatrix};$$

$$\text{если } \alpha_1 = 1, \text{ то } \mathbf{P}_{\tilde{\alpha}} = \begin{bmatrix} 0 & \mathbf{P}_{\tilde{\beta}} & 0 \\ 0 & 0 & \mathbf{P}_{\tilde{\beta}} \\ \mathbf{P}_{\tilde{\beta}} & 0 & 0 \end{bmatrix};$$

$$\text{если } \alpha_1 = 2, \text{ то } \mathbf{P}_{\tilde{\alpha}} = \begin{bmatrix} 0 & 0 & \mathbf{P}_{\tilde{\beta}} \\ \mathbf{P}_{\tilde{\beta}} & 0 & 0 \\ 0 & \mathbf{P}_{\tilde{\beta}} & 0 \end{bmatrix},$$

где $\tilde{\beta} = (\alpha_2, \ldots, \alpha_n)$.

Доказательство. Пусть $\mathbf{P}_{\tilde{\beta}}$ – матрица этого преобразования для вектора $\tilde{\beta} = (\alpha_2, \ldots, \alpha_n)$. Тогда вектор значений $\nu_{\tilde{\alpha}}(f)$ можно представить следующим образом:

$$\nu_{\tilde{\alpha}}(f) = (\mathbf{f}(\alpha_1, x_2, \ldots, x_n), \mathbf{f}(\alpha_1 + 1, x_2, \ldots, x_n), \mathbf{f}(\alpha_1 + 2, x_2, \ldots, x_n)) = \mathbf{P}_{\tilde{\alpha}}\mathbf{f}.$$

Теорема доказана.

Заметим, что для любого вектора $\tilde{\alpha}$ выполняются равенства $\mathbf{P}_{\tilde{\alpha}}^3 = \mathbf{I}$ и $\mathbf{P}_{\tilde{\alpha}}^2 = \mathbf{P}_{2\tilde{\alpha}}$, где $2\tilde{\alpha} = (2\alpha_1, \ldots, 2\alpha_n)$, а $\mathbf{I}$ – единичная матрица соответствующего размера и умножение происходит в E_3, т.е. все действия выполняются по модулю 3.

Для того чтобы функция n переменных была частично стационарной по отношению к вектору $2\tilde{\alpha}$, т.е. $\mu(f) = \nu_{2\tilde{\alpha}}(f)$, необходимо, чтобы $\mathbf{T}_n\mathbf{f} = \mathbf{P}_{2\tilde{\alpha}}\mathbf{f} = \mathbf{P}_{\tilde{\alpha}}^2\mathbf{f}$, где $\mathbf{P}_{\tilde{\alpha}}$ – это матрица преобразования $\nu_{\tilde{\alpha}}(f)$. Домножим обе части этого равенства слева на $\mathbf{P}_{\tilde{\alpha}}$. Тогда $\mathbf{P}_{\tilde{\alpha}}\mathbf{T}_n\mathbf{f} = \mathbf{f}$. По теореме 1 для нахождения количества таких функций достаточно рассмотреть векторы $\tilde{\alpha}$ вида (2,...,2,1,...,1,0,...,0), в которых m нулей, p единиц и q двоек. Рассмотрим случаи, когда вектор состоит только из нулей, когда он состоит из нулей и единиц и когда он состоит из нулей, единиц и двоек.

Если вектор состоит из одних нулей (т.е. $m = n$), то получаем условие $\mathbf{T}_n\mathbf{f} = \mathbf{f}$, где $\mathbf{T}_n$ – матрица преобразования μ, и f – обычная стационарная функция. Как показано в [7], множество таких функций n переменных является линейным подпространством пространства всех функций трехзначной логики n переменных, и его размерность равна

$$\frac{3^n + (-1)^n + 2 + 4 \cdot 3^{\frac{n}{2}} \arccos\left(n \cdot \cos\frac{1}{\sqrt{3}}\right)}{8}.$$

Пусть теперь вектор $\tilde{\alpha}$ имеет вид $\tilde{\alpha}=(1,\ldots,1,0,\ldots,0)$, где m нулей и p единиц. Найдем количество частично стационарных по отношению к нему функций. Для этого потребуется следующий результат.

Теорема 3. Количество функций f таких, что $\left(\mathbf{P}_{\tilde{\alpha}}\mathbf{T}_n\right)^2\mathbf{f}=\mathbf{f}$, где $\tilde{\alpha}=(\underbrace{1,\ldots,1}_{p},\underbrace{0,\ldots,0}_{m})$, равно

$$3^{\frac{\left(3^p-1\right)\left(3^m+(-1)^m\right)}{4}+\frac{3^m+2(-1)^p+(-1)^m}{4}}.$$

Количество функций f таких, что $\left(\mathbf{P}_{\tilde{\alpha}}\mathbf{T}_n\right)^2\mathbf{f}=2\mathbf{f}$, равно

$$3^{\frac{\left(3^p-1\right)\left(3^m+(-1)^m\right)}{4}+\frac{3^m-2(-1)^p+(-1)^m}{4}}.$$

Доказательство. Матрица преобразования и условия на вектор значений функции имеют следующий вид:

$$(\mathbf{P}_{2\tilde{\alpha}}\mathbf{T}_n)^2=\begin{bmatrix}2(\mathbf{P}_{\tilde{\beta}}\mathbf{T}_n)^2 & (\mathbf{P}_{\tilde{\beta}}\mathbf{T}_n)^2 & (\mathbf{P}_{\tilde{\beta}}\mathbf{T}_n)^2\\ 0 & 2(\mathbf{P}_{\tilde{\beta}}\mathbf{T}_n)^2 & 0\\ 0 & 2(\mathbf{P}_{\tilde{\beta}}\mathbf{T}_n)^2 & (\mathbf{P}_{\tilde{\beta}}\mathbf{T}_n)^2\end{bmatrix},$$

$$\begin{cases}2(\mathbf{P}_{\tilde{\beta}}\mathbf{T}_n)^2\mathbf{f}_0+(\mathbf{P}_{\tilde{\beta}}\mathbf{T}_n)^2\mathbf{f}_1+(\mathbf{P}_{\tilde{\beta}}\mathbf{T}_n)^2\mathbf{f}_2=\mathbf{f}_0,\\ 2(\mathbf{P}_{\tilde{\beta}}\mathbf{T}_n)^2\mathbf{f}_1=\mathbf{f}_1,\\ 2(\mathbf{P}_{\tilde{\beta}}\mathbf{T}_n)^2\mathbf{f}_1+(\mathbf{P}_{\tilde{\beta}}\mathbf{T}_n)^2\mathbf{f}_2=\mathbf{f}_2.\end{cases}$$

Рассматривая второе уравнение, складывая второе и третье уравнения, а также все три уравнения, видим, что

$$\left(\mathbf{P}_{\tilde{\alpha}}\mathbf{T}_n\right)^2\mathbf{f}_1=2\mathbf{f}_1,\ \left(\mathbf{P}_{\tilde{\alpha}}\mathbf{T}_n\right)^2\left(\mathbf{f}_1+\mathbf{f}_2\right)=\mathbf{f}_1+\mathbf{f}_2,$$

$$\left(\mathbf{P}_{\tilde{\alpha}}\mathbf{T}_n\right)^2\left(\mathbf{f}_0+\mathbf{f}_1+\mathbf{f}_2\right)=2\left(\mathbf{f}_0+\mathbf{f}_1+\mathbf{f}_2\right).$$

С другой стороны, выбрав указанным способом f_0, f_1 и f_2, получаем необходимые равенства. Следовательно, если обозначить $z_l^{(2)}(p)=\left|\left\{f:(\mathbf{P}_{\tilde{\alpha}}\mathbf{T}_n)^2\mathbf{f}=l\cdot\mathbf{f}\right\}\right|$, то $z_1^{(2)}(p)=z_1^{(2)}(p-1)+2z_2^{(2)}(p-1)$.

Рассматривая точно так же $z_2(p)$, получаем $z_2(p)=2z_1(p-1)+z_2(p-1)$. С учетом того, что

$$z_1^{(2)}(0)=q_1^{(2)}(m)=\frac{3^m+(-1)^m+2}{4}\ \text{и}\ z_2^{(2)}(0)=q_2^{(2)}(m)=\frac{3^m+(-1)^m-2}{4},$$

получаем систему двух рекуррентных уравнений. Решить ее довольно просто, зная, что $z_1^{(2)}(p)+z_2^{(2)}(p)=3\left(z_1^{(2)}(p-1)+z_2^{(2)}(p-1)\right)=3^p\cdot\dfrac{\left(3^m+(-1)^m\right)}{2}$. Решением является

$$z_1^{(2)}(p)=\frac{\left(3^p-1\right)\left(3^m+(-1)^m\right)}{4}+\frac{3^m+2(-1)^p+(-1)^m}{4},$$

$$z_2^{(2)}(p)=\frac{\left(3^p-1\right)\left(3^m+(-1)^m\right)}{4}+\frac{3^m-2(-1)^p+(-1)^m}{4},$$

откуда получаем утверждение теоремы.

Теорема 4. Количество функций f таких, что $\mathbf{P}_{\tilde{\alpha}}\mathbf{T}_n\mathbf{f}=l\cdot\mathbf{f}$, где $\tilde{\alpha}=(\underbrace{1,\ldots,1}_{p},\underbrace{0,\ldots,0}_{m})$, $l\in\{1,2\}$, равно $3^{z_l(p)}$, где

$$z_l(p)=\frac{\left(3^m+(-1)^m\right)\left(\dfrac{3^p-1}{2}\right)-1-(-1)^p}{4}+$$

$$+\frac{3^m+2+(-1)^m}{8}+\frac{(-1)^{p+l+1}\cdot 3^{\frac{m}{2}}\cos\left(m\cdot\arccos\left(\dfrac{1}{\sqrt{(3)}}\right)\right)}{2},$$

Доказательство. Заметим, что множества $\left\{f:\mathbf{P}_{\tilde{\alpha}}\mathbf{T}_n\mathbf{f}=l\cdot\mathbf{f},l=1,2\right\}$ являются линейными подпространствам пространства всех функций. Обозначим $z_l(p)=\dim\left\{f:\mathbf{P}_{\tilde{\alpha}}\mathbf{T}_n\mathbf{f}=l\cdot\mathbf{f}\right\}$, где $\tilde{\alpha}=(\underbrace{1,\ldots,1}_{p},\underbrace{0,\ldots 0}_{m})$. Фиксируем произвольный вектор $\tilde{\alpha}$ указанного вида.

Как следует из теоремы 2, матрица преобразования в этом случае имеет вид

$$\mathbf{P}_{2\tilde{\alpha}}\mathbf{T}_n=\begin{bmatrix}0 & 2\mathbf{P}_{2\tilde{\beta}}\mathbf{T}_{n-1} & \mathbf{P}_{2\tilde{\beta}}\mathbf{T}_{n-1}\\ 2\mathbf{P}_{2\tilde{\beta}}\mathbf{T}_{n-1} & 2\mathbf{P}_{2\tilde{\beta}}\mathbf{T}_{n-1} & 2\mathbf{P}_{2\tilde{\beta}}\mathbf{T}_{n-1}\\ \mathbf{P}_{2\tilde{\beta}}\mathbf{T}_{n-1} & 0 & 0\end{bmatrix},$$

где $\tilde{\beta}=(\alpha_2,\ldots,\alpha_n)$. Выпишем уравнения для вектора значений функции f:

$$\begin{cases}2\mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1}\mathbf{f}_1+\mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1}\mathbf{f}_2=\mathbf{f}_0,\\ 2\mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1}\mathbf{f}_0+2\mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1}\mathbf{f}_1+2\mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1}\mathbf{f}_2=\mathbf{f}_1,\\ \mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1}\mathbf{f}_0=\mathbf{f}_2.\end{cases}$$

Сложив второе уравнение с третьим, получаем $2\mathbf{P}_{\tilde{\beta}}\mathbf{T}_{\mathbf{n-1}}(\mathbf{f}_1+\mathbf{f}_2)=\mathbf{f}_1+\mathbf{f}_2$. Сложив все три уравнения и применив к ним преобразование $\mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1}$, имеем $\left(\mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1}\right)^2\mathbf{f}_1=2\mathbf{f}_1$. Выбирая подходящие f_1 и f_2 по этим условиям, можно найти f_0 однозначно при помощи первого уравнения.

Таким образом, показано, что $z_1(p)=z_2(p-1)+z_2^{(2)}(p-1)$. Аналогичными рассуждениями легко доказывается, что $z_2(p)=z_1(p-1)+z_2^{(2)}(p-1)$. Подставляя одно выражение в другое, с учетом результатов предыдущей теоремы получаем

$$z_1(p)=\begin{cases}\sum z^{(2)}(j)+q_1(m), & p=2k,\\ \sum z^{(2)}(j)+q_2(m), & p=2k+1,\end{cases}$$

$$z_2(p)=\begin{cases}\sum z^{(2)}(j)+q_1(m), & p=2k+1,\\ \sum z^{(2)}(j)+q_2(m), & p=2k.\end{cases}$$

Вычисляя сумму и приводя выражение к общему виду, получаем выражение, указанное в утверждении теоремы.

Теорема доказана.

Рассмотрим теперь вектор $\tilde{\alpha}$ вида $\tilde{\alpha}=(2,\ldots,2,1,\ldots,1,0,\ldots,0)$. Как и в предыдущем случае, сначала докажем предварительный результат.

Теорема 5. Количество функций f таких, что $(\mathbf{P}_{\tilde{\alpha}}\mathbf{T}_n)^3\mathbf{f}=2\mathbf{f}$, где $\tilde{\alpha}=(\underbrace{2,\ldots 2}_{q},\underbrace{1,\ldots 1}_{p},\underbrace{0,\ldots 0}_{m})$, равно $3^{l(q,p,m)}$,

$$l(q,p,m)=3^q\cdot\left[\frac{\left(3^m+(-1)^m\right)\left(\frac{3^p-1}{2}\right)-1-(-1)^p}{4}+\right.$$

$$\left.+\frac{3^m+2+(-1)^m}{8}+\frac{(-1)^{q+p+1}\cdot 3^{\frac{m}{2}}\cos\left(m\cdot\arccos\left(\frac{1}{\sqrt{3}}\right)\right)}{2}\right].$$

Доказательство. Рассмотрим матрицу $\mathbf{P}_{\tilde{\alpha}}\mathbf{T}_n$, где $n=m+p+q$. Так как $\left(\mathbf{P}_1\mathbf{T}_1\right)^3=2\mathbf{I}$, где $\mathbf{I}$ – единичная матрица соответствующего размера, то $(\mathbf{P}_{\tilde{\alpha}}\mathbf{T}_n)^3$ – диагональная блочная матрица размера $3^q\times 3^q$ с блоками вида $2(\mathbf{P}_{\tilde{\gamma}}\mathbf{T}_{m+p})^3$, если q нечетное, или $(\mathbf{P}_{\tilde{\gamma}}\mathbf{T}_{m+p})^3$, если q четное, где $\tilde{\gamma}=(\underbrace{1,\ldots,1}_{p},\underbrace{0,\ldots,0}_{m})$. При этом несложно проверить, что если $(\mathbf{P}_{\tilde{\gamma}}\mathbf{T}_{m+p})^3\mathbf{f}=2\mathbf{f}$,

то $(\mathbf{P}_{\tilde{\gamma}}\mathbf{T}_{m+p})\mathbf{f} = 2\mathbf{f}$, и если $(P_{\tilde{\gamma}}T_{m+p})^3 f = f$, то $(\mathbf{P}_{\tilde{\gamma}}\mathbf{T}_{m+p})\mathbf{f} = \mathbf{f}$. Следовательно, размерность пространства функций таких, что $\left(\mathbf{P}_1\mathbf{T}_1\right)^3 \mathbf{f} = l \cdot \mathbf{f}$, равна $3^q \times X$, где X – результат теоремы 4. Отсюда получаем утверждение теоремы.

Теорема 6. Количество функций $f \in V_{2\tilde{\alpha}}(n)$, где $\tilde{\alpha} = (\underbrace{2,\ldots 2}_{q},\underbrace{1,\ldots 1}_{p},\underbrace{0,\ldots 0}_{m})$, $q \geq 1$, равно $3^{l(q,p,m)}$, где

$$l(q,p,m) = 3^{q-1} \cdot \left[\frac{\left(3^m + (-1)^m\right)\left(\frac{3^p - 1}{2}\right) - 1 - (-1)^p}{4} + \right.$$

$$\left. + \frac{3^m + 2 + (-1)^m}{8} + \frac{(-1)^{q+p} \cdot 3^{\frac{m}{2}} \cos\left(m \cdot \arccos\left(\frac{1}{\sqrt{3}}\right)\right)}{2} \right].$$

Доказательство. Как следует из теоремы 2, матрица преобразования в этом случае имеет вид

$$\mathbf{P}_{\tilde{\alpha}}\mathbf{T}_n = \begin{bmatrix} 2\mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1} & 2P_{\tilde{\beta}}T_{n-1} & 2\mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1} \\ \mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1} & 0 & 0 \\ 0 & 2\mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1} & \mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1} \end{bmatrix},$$

где $\tilde{\beta} = (\alpha_2,\ldots,\alpha_n)$. Выпишем уравнения для вектора значений функции f:

$$\begin{cases} 2\mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1}\mathbf{f}_0 + 2\mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1}\mathbf{f}_1 + 2\mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1}\mathbf{f}_2 = \mathbf{f}_0, \\ \mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1}\mathbf{f}_0 = \mathbf{f}_1, \\ 2\mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1}\mathbf{f}_1 + \mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1}\mathbf{f}_2 = \mathbf{f}_2. \end{cases}$$

Сложим все три уравнения:

$$\mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1}\mathbf{f}_1 = \mathbf{f}_0 + \mathbf{f}_1 + \mathbf{f}_2.$$

Применим теперь к обеим частям $\mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1}$, тогда с учетом первого и второго уравнений исходной системы имеем

$$\begin{cases} 2(\mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1})^2\mathbf{f}_1 = \mathbf{f}_0, \\ \mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1}\mathbf{f}_0 = \mathbf{f}_1. \end{cases}$$

Из этих уравнений следует, что $2(\mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1})^3\mathbf{f}_1 = \mathbf{f}_1$. Таким образом, если известна такая функция f_1, то по ней подходящие f_0 и f_2 находятся единственным образом.

Из этих рассуждений и теоремы 3 следует, что количество таких функций совпадает с количеством функций $(\mathbf{P}_{\tilde{\beta}}\mathbf{T}_{n-1})^3\mathbf{g} = 2\mathbf{g}$ от $(n-1)$ переменной, поэтому утверждение теоремы следует из предыдущего результата.

Заключение

В работе были подробно рассмотрены классы частично стационарных функций. Приведено точное количество таких функций в зависимости от параметра, указан способ построения таких функций.

Список литературы

1. **Pieprzyk, J.** Computing mobius transforms of Boolean functions and characterising coincident boolean functions / J. Pieprzyk, X.-M. Zhang // Boolean Functions: Cryptography and Applications. – France, Rouen : Publications des Universites de Rouen et du Havre, 2007. – P. 135–151.
2. **Pieprzyk, J.** Mobius-α commutative functions and partially coincident functions / J. Pieprzyk, H. Wang, X.-M. Zhang // Boolean Functions: Cryptography and Applications. – France, Rouen: Publications des Universites de Rouen et du Havre, 2008. – P. 135–150.
3. **Pieprzyk, J.** Mobius transforms, coincident Boolean functions and non-coincidence property of Boolean functions / J. Pieprzyk, H. Wang, X.-M. Zhang // International Journal of Computer Mathematics. – 2011. – Vol. 88, № 7. – P. 1398–1416.
4. **Леонтьев, В. К.** О некоторых задачах, связанных с булевыми полиномами / В. К. Леонтьев // Журнал вычислительной математики и математической физики. – 1999. – Т. 39, № 6. – Р.1045–1054.
5. **Мазуров, А. А.** Структура стационарных классов функций трехзначной логики / А. А. Мазуров // Вестник Московского университета. Сер. 15. Вычислительная математика и кибернетика. – 2013. – С. 33–38.
6. **Мазуров, А. А.** О стационарных классах функций трехзначной логики / А. А. Мазуров // Проблемы теоретической кибернетики : материалы 16 Междунар. конф.. – Н. Новгород : Изд-во Нижегород. гос. ун-та, 2011. – С. 286–289.
7. **Мазуров, А. А.** О числе стационарных точек преобразования Мебиуса в трехзначной логике / А. А. Мазуров // Ломоносов-2013 : материалы молодежного научного форума [Электронный ресурс]. – М. : МАКС Пресс, 2013.
8. **Алехина, М. А.** О надежности схем, реализующих функции из P_3 / М. А. Алехина, О. Ю. Барсукова // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. – 2012. – № 1 (21). – С. 57–65.
9. **Алехина, М. А.** Оценки ненадежности схем в базисе Россера – Туркетта / М. А. Алехина, О. Ю. Барсукова // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. – 2014. – № 1 (29). – С. 5–19.
10. **Яблонский, С. В.** Введение в дискретную математику / С. В. Яблонский. – М. : Наука, 1986.

References

1. Pieprzyk J., Zhang X.-M. *Boolean Functions: Cryptography and Applications*. France, Rouen: Publications des Universites de Rouen et du Havre, 2007, pp. 135–151.
2. Pieprzyk J., Wang H., Zhang X.-M. *Boolean Functions: Cryptography and Applications*. France, Rouen: Publications des Universites de Rouen et du Havre, 2008, pp. 135–150.
3. Pieprzyk J., Wang H., Zhang X.-M. *International Journal of Computer Mathematics*. 2011, vol. 88, no. 7, pp. 1398–1416.

4. Leont'ev V. K. *Zhurnal vychislitel'noy matematiki i matematicheskoy fiziki* [Journal of calculus mathematics and mathematical physics]. 1999, vol. 39, no. 6, pp.1045–1054.
5. Mazurov A. A. *Vestnik Moskovskogo universiteta. Seriya 15: Vychislitel'naya matematika i kibernetika* [Bulletin of Moscow University. Series 15: Calculus mathematics and cybernetics]. 2013, pp. 33–38.
6. Mazurov A. A. *Problemy teoreticheskoy kibernetiki: materialy 16 Mezhdunar. konf.* [Problem of theoretical cybernetics: proceedings of 16 International conference]. Nizhny Novgorod: Izd-vo Nizhegorod. gos. un-ta, 2011, pp. 286–289.
7. Mazurov A. A. *Lomonosov-2013: materialy molodezhnogo nauchnogo foruma* [Lomonosov-2013: proceedings of the youth scientific forum (electronic resource)]. Moscow: MAKS Press, 2013.
8. Alekhina M. A., Barsukova O. Yu. *Izvestiya vysshikh uchebnykh zavedeniy. Povolzhskiy region. Fiziko-matematicheskie nauki* [University proceedings. Volga region. Physical and mathematical sciences]. 2012, no. 1 (21), pp. 57–65.
9. Alekhina M. A., Barsukova O. Yu. *Izvestiya vysshikh uchebnykh zavedeniy. Povolzhskiy region. Fiziko-matematicheskie nauki* [University proceedings. Volga region. Physical and mathematical sciences]. 2014, no. 1 (29), pp. 5–19.
10. Yablonskiy S. V. *Vvedenie v diskretnuyu matematiku* [Introduction into discrete mathematics]. Moscow: Nauka, 1986.

Мазуров Анатолий Алексеевич
инженер, фирма «Инфокрипт»
(Россия, г. Москва, пр-т Вернадского, 78, стр. 7)

Mazurov Anatoliy Alekseevich
Engineer, Firm “Infocrypt” (building 7, 78 Vernadskogo avenue, Moscow, Russia)

E-mail: anat-mazurov@mail.ru

УДК 519.7

Мазуров, А. А.

О количестве частично стационарных функций трехзначной логики / А. А. Мазуров // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. – 2014. – № 3 (31). – С. 67–77.