Серия «Математика»
2016. Т. 16. С. 19—29

Онлайн-доступ к журналу:
http://isu.ru/izvestia

ИЗВЕСТИЯ
Иркутского
государственного
университета

УДК 519.714.4
MSC 68Q17

Нижняя оценка сложности функций над конечным полем порядка 4 в классе поляризованных полиномов

А. С. Балюк, А. С. Зинченко
Иркутский государственный университет

Аннотация. Представления функций над конечными полями, в том числе полиномиальные, в настоящее время активно исследуются. Одним из основных направлений этих исследований является сложность таких представлений. Вопросы полиномиальных представлений булевых функций довольно хорошо изучены. Для многих классов полиномов найдены точные значения сложности таких представлений.

В последнее время возрос интерес к полиномиальным представлениям функций над конечными полями порядка больше двух и кольцами вычетов по составному модулю. Исследование сложности таких представлений сопряжено с определенными трудностями, и даже в довольно простых классах полиномиальных форм найдены только несовпадающие верхние и нижние оценки сложности.

В настоящей работе внимание уделено поляризованным полиномам над конечным полем порядка 4. Полиномы этого класса представляют собой суммы произведений множителей определенного вида. Каждый полином реализует некоторую n-местную функцию над конечным полем. Под сложностью полинома понимается число ненулевых слагаемых в нем. Каждая функция может быть реализована несколькими различными полиномами из одного класса. Под сложностью функции в классе полиномов понимается минимально возможная сложность реализующего ее полинома из этого класса.

Ранее были известны эффективные нижние оценки сложности в классе поляризованных полиномов для случая булевых и трехзначных функций и более слабая мощностная оценка для случая функций над конечным полем простого порядка.

В настоящей статье получена эффективная нижняя оценка сложности функций над конечным полем порядка 4, аналогичная ранее известным оценкам для булевых и трехзначных функций.

Ключевые слова: конечное поле, поляризованный полином, кронекерова форма, нижняя оценка сложности.

1. Обозначения и определения

Будем использовать следующие обозначения и соглашения:

- $\#S$ — число элементов конечного множества S;
- $\mathbb{N} = \{0, 1, 2, \dots\}$ — множество натуральных чисел;
- $\min S$ обозначает наименьший, а $\max S$ — наибольший элемент конечного непустого множества $S \subset \mathbb{N}$;
- если $\alpha \geqslant 0$ — действительное число, то $\lfloor \alpha \rfloor = \max\{i \in \mathbb{N} \mid i \leqslant \alpha\}$;
- нотация Айверсона [3]: если R — некоторое утверждение, то

$$[R] = \begin{cases} 1, & \text{если } R \text{ истинно,} \\ 0, & \text{если } R \text{ ложно;} \end{cases}$$

- условимся, что если $i < j$, то биномиальный коэффициент $\binom{i}{j} = 0$;
- если M — матрица размера $m \times k$, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant k$, то $M[i, j]$ — элемент, стоящий на пересечении i-й строки и j-го столбца M;
- если M_1 — матрица размера $m_1 \times k_1$, M_2 — матрица размера $m_2 \times k_2$, то матрица $M = M_1 \otimes M_2$ размера $m_1 m_2 \times k_1 k_2$, в которой для всех i_1, i_2, j_1, j_2, $1 \leqslant i_1 \leqslant m_1$, $1 \leqslant i_2 \leqslant m_2$, $1 \leqslant j_1 \leqslant k_1$, $1 \leqslant j_2 \leqslant k_2$, выполняется $M[(i_1 - 1)m_2 + i_2, (j_1 - 1)k_2 + j_2] = M_1[i_1, j_1]M[i_2, j_2]$, называется кронекеровым произведением матриц M_1 и M_2;
- $\mathbb{F}_q$ — конечное поле порядка q, *1* — единица, а *0* — ноль поля $\mathbb{F}_q$;
- условимся, что $a^0 = 1$ для всех $a \in \mathbb{F}_q$;
- $\mathbb{M}_q[m \times k]$ — множество всех матриц размера $m \times k$ с элементами из $\mathbb{F}_q$;
- $I_m \in \mathbb{M}_q[m \times m]$ — единичная матрица, $I_m[i, j] = [i = j]$;
- $\mathbb{F}_q^m = \{v \mid v = (v_1, \dots, v_m),\ v_i \in \mathbb{F}_q,\ 1 \leqslant i \leqslant m\}$ — m-мерное векторное пространство над $\mathbb{F}_q$ с операциями покомпонентного сложения и умножения на элементы из $\mathbb{F}_q$;
- если $u \in \mathbb{F}_q^m$, $v \in \mathbb{F}_q^k$, то запись $w = (u, v)$ обозначает вектор $w \in \mathbb{F}_q^{m+k}$, где $w_i = u_i[i \leqslant m] + v_{i-m}[i > m]$ для всех $1 \leqslant i \leqslant m + k$;
- $Z(v) = \#\{i \mid v_i = 0,\ 1 \leqslant i \leqslant m\}$ — количество нулевых элементов вектора $v \in \mathbb{F}_q^m$;
- функцию $f : \mathbb{F}_q^n \to \mathbb{F}_q$ будем отождествлять с вектором $f \in \mathbb{F}_q^N$, $f = (f_1, \dots, f_N)$, полагая $f_k = f(\sigma^k)$ для всех k, $1 \leqslant k \leqslant N = q^n$, где $\sigma^1, \dots, \sigma^N$ — все векторы из $\mathbb{F}_q^n$, упорядоченные лексикографически, и вместо $f : \mathbb{F}_q^n \to \mathbb{F}_q$ будем писать $f \in \mathbb{F}_q^N$.

Далее будем считать, что q — степень простого числа, $\mathbb{F}_q$ — конечное поле порядка q, $n \in \mathbb{N}$ и $N = q^n$.

Определение 1. *Пусть $v \in \mathbb{F}_q^n$. Выражение*

$$\Phi_c^v(x_1, \dots, x_n) = \sum_{\sigma \in \mathbb{F}_q^n} c_t (x_1 + v_1)^{\sigma_1} \dots (x_n + v_n)^{\sigma_n}, \qquad (1.1)$$

где $c \in \mathbb{F}_q^N$, а все операции сложения и умножения выполняются в поле $\mathbb{F}_q$, назовем поляризованным полиномом переменных $x_1, \ldots, x_n$ над полем $\mathbb{F}_q$ с поляризацией v и вектором коэффициентов c.

Если переменным $x_1, \ldots, x_n$ придавать всевозможные значения из $\mathbb{F}_q$, то полином Φ_c^v из (1.1) задает некоторую функцию $\Phi_c^v \in \mathbb{F}_q^N$. Сложностью полинома назовем величину $L(\Phi_c^v) = \#\{c_t \mid c_t \neq 0,\ 1 \leqslant t \leqslant N\}$.

Сложностью функции $f \in \mathbb{F}_q^N$ в классе поляризованных полиномов назовем величину $L_{\mathcal{P}}(f) = \min\{L(\Phi_c^v) \mid c \in \mathbb{F}_q^N,\ v \in \mathbb{F}_q^n,\ \Phi_c^v = f\}$.

Сложностью множества функций $F \subseteq \mathbb{F}_q^N$ в классе поляризованных полиномов назовем величину $L_{\mathcal{P}}(F) = \max\{L_{\mathcal{P}}(f) \mid f \in F\}$. Для оценки сложности класса всех n-местных функций введем величину $L_{\mathcal{P}}(n) = L_{\mathcal{P}}(\mathbb{F}_q^N)$.

Понятие поляризованного полинома использовалось в работах [1; 4; 5; 6]. В работе [5] было показано, что $L_{\mathcal{P}}(n) = \left\lfloor \frac{2}{3} 2^n \right\rfloor$ для $q = 2$. В работе [4] было показано, что $L_{\mathcal{P}}(n) \geqslant \left\lfloor \frac{3}{4} 3^n \right\rfloor$ для $q = 3$. В работе [1] для простого q было показано, что $L_{\mathcal{P}}(n) \geqslant \frac{q-1}{q} q^n - o(q^n)$. В настоящей работе для случая $q = 4$ устанавливается оценка $L_{\mathcal{P}}(n) \geqslant \left\lfloor \frac{4}{5} 4^n \right\rfloor$.

Пусть $K \subseteq \mathbb{M}_q[q \times q]$ — множество невырожденных матриц. Определим множество $K^{\otimes n}$ следующим образом

$$K^{\otimes n} = \{M_1 \otimes \cdots \otimes M_n \mid M_1, \ldots, M_n \in K\}.$$

Пусть $M \in K^{\otimes n}$, $c \in \mathbb{F}_q^N$. Пару $\langle M, c \rangle$ назовем кронекеровой формой, порожденной множеством K. Кронекерова форма $\langle M, c \rangle$ задает некоторую функцию $f \in \mathbb{F}_q^N$, определяемую равенством $f = Mc$. Под сложностью кронекеровой формы будем понимать величину

$$L(\langle M, c \rangle) = \#\{c_t \mid c_t \neq 0,\ 1 \leqslant t \leqslant N\}.$$

Сложностью функции $f \in \mathbb{F}_q^N$ в классе кронекеровых форм, порожденных множеством K, назовем величину

$$L_{K^\otimes}(f) = \min\{L(\langle M, c \rangle) \mid M \in K^{\otimes n},\ c \in \mathbb{F}_q^N,\ f = Mc\}.$$

Сложностью множества функций $F \subseteq \mathbb{F}_q^N$ в классе кронекеровых форм, порожденных множеством K, назовем величину

$$L_{K^\otimes}(F) = \max\{L_{K^\otimes}(f) \mid f \in F\}.$$

Также введем обозначение $L_{K^\otimes}(n) = L_{K^\otimes}(\mathbb{F}_q^N)$.

Понятие кронекеровой формы было введено в [2]. Там же для поля $\mathbb{F}_q$ было показано, что если $T_{\mathcal{P}} = \{T_a \in \mathbb{M}_q[q \times q] \mid T_a[i,j] = \binom{j-1}{i-1} a^{|j-i|}, a \in \mathbb{F}_q\}$, то $L_{\mathcal{P}}(n) = L_{T_{\mathcal{P}}^\otimes}(n)$.

2. Основной результат

Положим $q = 4$, $n \in \mathbb{N}$, $N = 4^n$. Элементы поля $\mathbb{F}_4$ обозначим цифрами 0, 1, 2, 3, набранными курсивом. Сложение и умножение в поле $\mathbb{F}_4$ зададим следующими таблицами

$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Целое число k в контексте операций с элементами поля $\mathbb{F}_4$ будем отождествлять с 0, если k четное, и с 1, если k нечетное.

Далее будем считать, что все операции с матрицами и векторами выполняются в поле $\mathbb{F}_4$.

Определим функции $g^n \in \mathbb{F}_4^N$ и $h^n \in \mathbb{F}_4^N$ рекуррентно следующим образом:

$$\begin{aligned} g^0 &= (0), \quad h^0 = (1), \\ g^{n+1} &= (g^n,\ g^n + h^n, 3g^n + \ h^n, g^n + 3h^n), \\ h^{n+1} &= (h^n, 2g^n \qquad , 2g^n + 2h^n, g^n + 2h^n). \end{aligned} \tag{2.1}$$

Определим функции $f_t^n \in \mathbb{F}_4^N$ рекуррентно следующим образом:

$$f_0^n = g^n, \quad f_1^n = h^n, \quad f_{t+2}^n = f_{t+1}^n + 2f_t^n.$$

Обратим внимание, что $f_{t+5}^n = 2f_t^n$. Действительно,

$$f_{t+5}^n = f_{t+4}^n + 2f_{t+3}^n = 3f_{t+3}^n + 2f_{t+2}^n = f_{t+2}^n + f_{t+1}^n = 2f_t^n. \tag{2.2}$$

Выпишем несколько начальных значений f_t^n:

$$\begin{aligned} &f_0^n = g^n, && f_1^n = h^n, && f_2^n = 2g^n + h^n, \\ &f_3^n = 2g^n + 3h^n, && f_4^n = g^n + h^n, && f_5^n = 2g^n. \end{aligned} \tag{2.3}$$

Обратим внимание, что последовательность функций f_t^n является периодической с периодом 15, так как $f_{t+15}^n = 2^3 f_t^n = f_t^n$.

Лемма 1. *Пусть $n \geqslant 1$, $M_1 \in \mathbb{M}_4[N \times N]$, $M_2 \in \mathbb{M}_4[\frac{N}{4} \times \frac{N}{4}]$, и пусть $t_1, \ldots, t_4 \in \mathbb{N}$ и $a_1, \ldots, a_4 \in \mathbb{F}_4$ таковы, что выполняются векторные равенства*

$$M_1 g^{n+1} = (a_1 M_2 f_{t_1}^n, \ldots, a_4 M_2 f_{t_4}^n), \quad M_1 h^{n+1} = (a_1 M_2 f_{t_1+1}^n, \ldots, a_4 M_2 f_{t_4+1}^n).$$

Тогда для всех $t \in \mathbb{N}$ выполняется $M_1 f_t^{n+1} = (a_1 M_2 f_{t_1+t}^n, \ldots, a_4 M_2 f_{t_4+t}^n)$.

Доказательство. Доказательство индукцией по t.

Базис индукции. При $t = 0$ и $t = 1$ утверждение очевидно, поскольку $f_0^{n+1} = g^{n+1}$, а $f_1^{n+1} = h^{n+1}$.

Шаг индукции. Пусть $t \geqslant 2$. По предположению индукции

$$M_1 f_{t-2}^{n+1} = (a_1 M_2 f_{t_1+t-2}^n, \ldots, a_4 M_2 f_{t_4+t-2}^n),$$
$$M_1 f_{t-1}^{n+1} = (a_1 M_2 f_{t_1+t-1}^n, \ldots, a_4 M_2 f_{t_4+t-1}^n).$$

Пусть $M_1 f_t^{n+1} = (u_1, u_2, u_3, u_4)$. Поскольку $f_t^{n+1} = f_{t-1}^{n+1} + 2 f_{t-2}^{n+1}$, имеем:

$$u_i = a_i M_2 f_{t_i+t-1}^n + 2 a_i M_2 f_{t_i+t-2}^n = a_i M_2 (f_{t_i+t-1}^n + 2 f_{t_i+t-2}^n) = a_i M_2 f_{t_i+t}^n$$

при $1 \leqslant i \leqslant 4$. Что и требовалось доказать. □

Для каждого $a \in \mathbb{F}_4$ определим матрицу $T_a \in \mathbb{M}_4[4{\times}4]$, элементы которой определены следующим образом:

$$T_a[i,j] = \tbinom{j-1}{i-1} a^{|j-i|}, \quad 1 \leqslant i, j \leqslant 4. \tag{2.4}$$

Зададим множество $T_{\mathcal{P}} \subset \mathbb{M}_4[4{\times}4]$ как $T_{\mathcal{P}} = \{T_a \mid a \in \mathbb{F}_4\}$. Обратим внимание, что $\binom{j-1}{i-1} = 0$ при $i > j$, поэтому матрицы из множества $T_{\mathcal{P}}$ — верхние треугольные и имеют следующий вид

$$T_0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, T_1 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, T_2 = \begin{bmatrix} 1 & 2 & 3 & 1 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{bmatrix}, T_3 = \begin{bmatrix} 1 & 3 & 2 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Кроме того, выполняются следующие матричные равенства.

$$T_0 \begin{bmatrix} g^n & & & h^n \\ & h^n & 2g^n + & h^n \\ 2g^n + & h^n & 2g^n + 3h^n & \\ 2g^n + 3h^n & & g^n + & h^n \end{bmatrix} = \begin{bmatrix} g^n & & & h^n \\ & h^n & 2g^n + & h^n \\ 2g^n + & h^n & 2g^n + 3h^n & \\ 2g^n + 3h^n & & g^n + & h^n \end{bmatrix} = \begin{bmatrix} f_0^n & f_1^n \\ f_1^n & f_2^n \\ f_2^n & f_3^n \\ f_3^n & f_4^n \end{bmatrix} \tag{2.5}$$

$$T_1 \begin{bmatrix} g^n & & & h^n \\ & h^n & 2g^n + & h^n \\ 2g^n + & h^n & 2g^n + 3h^n & \\ 2g^n + 3h^n & & g^n + & h^n \end{bmatrix} = \begin{bmatrix} g^n + 3h^n & & g^n + 2h^n \\ 2g^n + 2h^n & & 3g^n \\ & 2h^n & 3g^n + 2h^n \\ 2g^n + 3h^n & & g^n + & h^n \end{bmatrix} = \begin{bmatrix} 3f_2^n & 3f_3^n \\ 2f_4^n & 2f_5^n \\ 2f_1^n & 2f_2^n \\ f_3^n & f_4^n \end{bmatrix} \tag{2.6}$$

$$T_2 \begin{bmatrix} g^n & & & h^n \\ & h^n & 2g^n + & h^n \\ 2g^n + & h^n & 2g^n + 3h^n & \\ 2g^n + 3h^n & & g^n + & h^n \end{bmatrix} = \begin{bmatrix} 2g^n + 2h^n & & 3g^n & \\ g^n + 3h^n & & g^n + 2h^n & \\ g^n & & & h^n \\ 2g^n + 3h^n & & g^n + & h^n \end{bmatrix} = \begin{bmatrix} 2f_4^n & 2f_5^n \\ 3f_2^n & 3f_3^n \\ f_0^n & f_1^n \\ f_3^n & f_4^n \end{bmatrix} \tag{2.7}$$

$$T_3 \begin{bmatrix} g^n & & & h^n \\ & h^n & 2g^n + & h^n \\ 2g^n + & h^n & 2g^n + 3h^n & \\ 2g^n + 3h^n & & g^n + & h^n \end{bmatrix} = \begin{bmatrix} & 2h^n & 3g^n + 2h^n & \\ 3g^n & & & 3h^n \\ 3g^n + 3h^n & & g^n + 3h^n & \\ 2g^n + 3h^n & & g^n + & h^n \end{bmatrix} = \begin{bmatrix} 2f_1^n & 2f_2^n \\ 3f_0^n & 3f_1^n \\ 3f_4^n & 3f_5^n \\ f_3^n & f_4^n \end{bmatrix} \tag{2.8}$$

Пусть $v \in \mathbb{F}_4^{n+1}$, $v=(u^1,u^2,u^3,u^4)$, где $u^1,\dots,u^4 \in \mathbb{F}_4^n$, $M \in \mathbb{M}_4[\frac{N}{4}\times\frac{N}{4}]$ и $M_0 \in \mathbb{M}_4[4\times4]$. Тогда по определению кронекерова произведения при $1 \leqslant i \leqslant N$ и $1 \leqslant t \leqslant 4$ имеем

$$((M_0 \otimes M)v)_{(t-1)N+i} = \sum_{k=1}^{4}\sum_{j=1}^{N} M_0[t,k]M[i,j]v_{(k-1)N+j}$$
$$= \sum_{k=1}^{4} M_0[t,k]\sum_{j=1}^{N} M[i,j]u_j^k = \sum_{k=1}^{4} M_0[t,k](Mu^k)_i,$$

что в матричном виде можно записать как

$$(M_0 \otimes M)\begin{bmatrix} u^1 \\ u^2 \\ u^3 \\ u^4 \end{bmatrix} = M_0 \begin{bmatrix} Mu^1 \\ Mu^2 \\ Mu^3 \\ Mu^4 \end{bmatrix}. \tag{2.9}$$

Лемма 2. *Пусть $M_1,\dots,M_n \in T_{\mathcal{P}}$, $M = M_1 \otimes \cdots \otimes M_n$. Тогда для любого $t \in \mathbb{N}$*

$$\sum_{i=0}^{4} Z(Mf_{t+i}^n) = 4^n.$$

Доказательство. Поскольку по (2.2)

$$\sum_{i=0}^{4} Z(Mf_{t+i}^n) = \sum_{i=0}^{4} Z(Mf_{(t+i) \bmod 5}^n) = \sum_{i=0}^{4} Z(Mf_i^n), \tag{2.10}$$

достаточно доказать, что

$$\sum_{t=0}^{4} Z(Mf_t^n) = 4^n. \tag{2.11}$$

Доказательство проведем индукцией по n.

Базис индукции. Пусть $n = 0$. Тогда M состоит из одного элемента $M[1,1] = 1$, и $Mf_t^0 = f_t^0$. Из (2.1) и (2.3) получаем $f_0^0 = (0)$, $f_1^0 = (1)$, $f_2^0 = (1)$, $f_3^0 = (3)$, $f_4^0 = (1)$. Откуда,

$$\sum_{t=0}^{4} Z(Mf_t^0) = 1 = 4^0.$$

Шаг индукции. Пусть $n \geqslant 0$, $M = M_1 \otimes \cdots \otimes M_n$, где $M_1,\dots,M_n \in T_{\mathcal{P}}$. По предположению индукции выполняется (2.11).

Пусть $M_0 \in T_{\mathcal{P}}$. Рассмотрим матрицу $M' = M_0 \otimes M$ и покажем, что

$$\sum_{t=0}^{4} Z(M'f_t^{n+1}) = 4^{n+1}.$$

По определению (2.1) имеем $g^{n+1} = (g^n, g^n + h^n, 3g^n + h^n, g^n + 3h^n)$, $h^{n+1} = (h^n, 2g^n, 2g^n + 2h^n, g^n + 2h^n)$. Тогда, учитывая (2.9) и (2.5)–(2.8), а также лемму 1, получаем

$$
\begin{aligned}
M'f_t^{n+1} &= (T_0 \otimes M)f_t^{n+1} = (Mf_t^n, Mf_{t+1}^n, Mf_{t+2}^n, Mf_{t+3}^n),\\
M'f_t^{n+1} &= (T_1 \otimes M)f_t^{n+1} = (3Mf_{t+2}^n, 2Mf_{t+4}^n, 2Mf_{t+1}^n, Mf_{t+3}^n),\\
M'f_t^{n+1} &= (T_2 \otimes M)f_t^{n+1} = (2Mf_{t+4}^n, 3Mf_{t+2}^n, Mf_t^n, Mf_{t+3}^n),\\
M'f_t^{n+1} &= (T_3 \otimes M)f_t^{n+1} = (2Mf_{t+1}^n, 3Mf_t^n, 3Mf_{t+4}^n, Mf_{t+3}^n)
\end{aligned}
$$

в случаях $M_0 = T_0$, $M_0 = T_1$, $M_0 = T_2$, $M_0 = T_3$ соответственно. Учитывая (2.10) и предположение индукции, во всех случаях получаем

$$\sum_{t=0}^{4} Z(M'f_t^{n+1}) = 4\sum_{t=0}^{4} Z(Mf_t^n) = 4 \cdot 4^n = 4^{n+1}. \qquad \square$$

Лемма 3. *Пусть $M_1, \ldots, M_n \in T_{\mathcal{P}}$, $M = M_1 \otimes \cdots \otimes M_n$. Тогда для любого $t \in \mathbb{N}$*

$$Z(Mf_t^n) = \frac{4^n}{5} + (-1)^n \left(\frac{4}{5} - [t + b \not\equiv 0 \pmod 5] \right), \tag{2.12}$$

где $b = -b_0 + b_2 + 2b_3$, $b_a = \#\{i \mid 1 \leqslant i \leqslant n,\ M_i = T_a\}$, $a \in \mathbb{F}_4$.

Доказательство. Доказательство проведем индукцией по n.

Базис индукции. Пусть $n = 0$. $f_{5k}^0 = 2^k g^0 = (0)$ для всех $k \in \mathbb{N}$. Если же $t = 5k + i$, где $k \in \mathbb{N}$ и $1 \leqslant i \leqslant 4$, то, поскольку $2^k \neq 0$ и $(0) \notin \{f_i^0 \mid 1 \leqslant i \leqslant 4\} = \{(1), (3)\}$, имеем $f_t^0 = 2^k f_i^0 \neq (0)$. Матрица M состоит из единственного элемента $M[1,1] = 1$, и поэтому $Mv = v$ для всех $v \in \mathbb{F}_4^1$, а значит, $Z(Mf_t^0) = [t \equiv 0 \pmod 5]$.

Пусть $\beta_t^n = \frac{4^n}{5} + (-1)^n \left(\frac{4}{5} - [t + b \not\equiv 0 \pmod 5] \right)$. Поскольку $n = 0$, то $b_a = 0$, для всех $a \in \mathbb{F}_4$, а следовательно, $b = 0$. Тогда

$$\beta_t^0 = \frac{1}{5} + \frac{4}{5} - [t \not\equiv 0 \pmod 5] = [t \equiv 0 \pmod 5].$$

Значит, $\beta_t^0 = [t \equiv 0 \pmod 5] = Z(Mf_t^0)$, и базис индукции выполнен.

Шаг индукции. Пусть $n \geqslant 0$, $M_1, \ldots, M_n \in T_{\mathcal{P}}$, $M = M_1 \otimes \cdots \otimes M_n$. По предположению индукции для всех $t \in \mathbb{N}$ выполняется равенство (2.12).

Пусть $M_0 \in T_{\mathcal{P}}$. Рассмотрим матрицу $M' = M_0 \otimes M$ и покажем, что утверждение леммы выполняется для M', то есть, для всех $t \in \mathbb{N}$

$$Z(M'f_t^{n+1}) = \frac{4^{n+1}}{5} + (-1)^{n+1} \left(\frac{4}{5} - [t + b' \not\equiv 0 \pmod 5] \right), \tag{2.13}$$

где $b' = -b'_0 + b'_2 + 2b'_3$, $b'_a = b_a + [M_0 = T_a]$, $a \in \mathbb{F}_4$.

Если $g^{n+1} = (u_1, \dots, u_4)$, $h^{n+1} = (v_1, \dots, v_4)$ и векторы $M'g^{n+1}$ и $M'h^{n+1}$ представимы в виде

$$\begin{aligned}(M'g^{n+1})_i &= \sum_{j=1}^{4} M_0[i,j]Mu_j = M\sum_{j=1}^{4} M_0[i,j]u_j = a_{t_i}Mf_{t_i}^n,\\ (M'h^{n+1})_i &= \sum_{j=1}^{4} M_0[i,j]Mv_j = M\sum_{j=1}^{4} M_0[i,j]v_j = a_{t_i}Mf_{t_i+1}^n,\end{aligned} \tag{2.14}$$

то по лемме 1 выполняется

$$M'f_t^{n+1} = (a_{t_1}Mf_{t+t_1}^n, \dots, a_{t_4}Mf_{t+t_4}^n). \tag{2.15}$$

В свою очередь, равенства (2.14) выполняются, если справедливо следующее матричное равенство

$$\begin{bmatrix} M_0[1,1] & \dots & M_0[1,4] \\ \vdots & \ddots & \vdots \\ M_0[4,1] & \dots & M_0[4,4] \end{bmatrix} \begin{bmatrix} u_1 & v_1 \\ \vdots & \vdots \\ u_4 & v_4 \end{bmatrix} = \begin{bmatrix} a_{t_1}f_{t_1}^n & a_{t_1}f_{t_1+1}^n \\ \vdots & \vdots \\ a_{t_4}f_{t_4}^n & a_{t_4}f_{t_4+1}^n \end{bmatrix}. \tag{2.16}$$

Из (2.5)–(2.8) следует, что (2.16) выполняется для любой $M_0 \in T_{\mathcal{P}}$.

Учитывая конкретные значения $t_1, \dots, t_4$ из (2.5)–(2.8), получаем

$$\begin{aligned}Z((T_0 \otimes M)f_t^{n+1}) &= Z(Mf_t^n\ \ ) + Z(Mf_{t+1}^n) + Z(Mf_{t+2}^n) + Z(Mf_{t+3}^n),\\ Z((T_1 \otimes M)f_t^{n+1}) &= Z(Mf_{t+2}^n) + Z(Mf_{t+4}^n) + Z(Mf_{t+1}^n) + Z(Mf_{t+3}^n),\\ Z((T_2 \otimes M)f_t^{n+1}) &= Z(Mf_{t+4}^n) + Z(Mf_{t+2}^n) + Z(Mf_t^n\ \ ) + Z(Mf_{t+3}^n),\\ Z((T_3 \otimes M)f_t^{n+1}) &= Z(Mf_{t+1}^n) + Z(Mf_t^n\ \ ) + Z(Mf_{t+4}^n) + Z(Mf_{t+3}^n).\end{aligned}$$

Применяя лемму 2 и предположение индукции, имеем

$$\begin{aligned}Z((T_0 \otimes M)f_t^{n+1}) &= 4^n - Z(Mf_{t+4}^n) = 4^n - \tfrac{4^n}{5} - (-1)^n(\tfrac{4}{5} - [t+b \not\equiv 1 \pmod 5]),\\ Z((T_1 \otimes M)f_t^{n+1}) &= 4^n - Z(Mf_t^n\ \ ) = 4^n - \tfrac{4^n}{5} - (-1)^n(\tfrac{4}{5} - [t+b \not\equiv 0 \pmod 5]),\\ Z((T_2 \otimes M)f_t^{n+1}) &= 4^n - Z(Mf_{t+1}^n) = 4^n - \tfrac{4^n}{5} - (-1)^n(\tfrac{4}{5} - [t+b \not\equiv 4 \pmod 5]),\\ Z((T_3 \otimes M)f_t^{n+1}) &= 4^n - Z(Mf_{t+2}^n) = 4^n - \tfrac{4^n}{5} - (-1)^n(\tfrac{4}{5} - [t+b \not\equiv 3 \pmod 5]).\end{aligned}$$

Как легко проверить, $b = b' + [M_0 = T_0] - [M_0 = T_2] - 2[M_0 = T_3]$. Поэтому,

$$\begin{aligned}Z((T_0 \otimes M)f_t^{n+1}) &= \tfrac{4^{n+1}}{5} + (-1)^{n+1}\left(\tfrac{4}{5} - [t+b' \not\equiv 0 \pmod 5]\right),\\ Z((T_1 \otimes M)f_t^{n+1}) &= \tfrac{4^{n+1}}{5} + (-1)^{n+1}\left(\tfrac{4}{5} - [t+b' \not\equiv 0 \pmod 5]\right),\\ Z((T_2 \otimes M)f_t^{n+1}) &= \tfrac{4^{n+1}}{5} + (-1)^{n+1}\left(\tfrac{4}{5} - [t+b' \not\equiv 0 \pmod 5]\right),\\ Z((T_3 \otimes M)f_t^{n+1}) &= \tfrac{4^{n+1}}{5} + (-1)^{n+1}\left(\tfrac{4}{5} - [t+b' \not\equiv 0 \pmod 5]\right).\end{aligned}$$

Таким образом, для любого $M_0 \in T_{\mathcal{P}}$ выполняется (2.13). Лемма доказана. □

Теорема 1. *В поле $\mathbb{F}_4$ справедлива оценка $L_{T_{\mathcal{P}}^{\otimes}}(n) \geqslant \left\lfloor \frac{4}{5}4^n \right\rfloor$.*

Доказательство. Для начала заметим, что $T_a^{-1} = T_{-a}$. Действительно, при $1 \leqslant i \leqslant j \leqslant q$ выполняется (см., например, таблицу 199 в [3])

$$(T_{-a}T_a)[i,j] = \sum_{k=1}^{q} \tbinom{k-1}{i-1}(-a)^{|k-i|}\tbinom{j-1}{k-1}a^{|j-k|} = \sum_{k=i}^{j} \tbinom{k-1}{i-1}(-a)^{k-i}\tbinom{j-1}{k-1}a^{j-k} =$$
$$= a^{j-i}\tbinom{j-1}{i-1}\sum_{k=i}^{j}(-1)^{k-i}\tbinom{j-i}{k-i} = a^{j-i}\tbinom{j-1}{i-1}(1-1)^{j-i} = [i=j].$$

Таким образом, $T_{-a}T_a = I_q$, в силу верхней треугольности матриц T_a и T_{-a}. Тогда, $T_{\mathcal{P}} = \{M^{-1} \mid M \in T_{\mathcal{P}}\}$ и $T_{\mathcal{P}}^{\otimes} = \{M^{-1} \mid M \in T_{\mathcal{P}}^{\otimes}\}$.

По лемме 3, учитывая целочисленность функции $Z(v)$, $v \in \mathbb{F}_4^n$, имеем $\max\{Z(Mg^n) \mid M \in T_{\mathcal{P}}^{\otimes}\} \leqslant \frac{4^n}{5} + \frac{1}{5} + \frac{3}{5}[n \equiv 0 \pmod 2]$. Поскольку $L(\langle M, c\rangle) = 4^n - Z(c)$, имеем

$$L_{T_{\mathcal{P}}^{\otimes}}(g^n) = \min\{L(\langle M,c\rangle) \mid M \in T_{\mathcal{P}}^{\otimes},\, c \in \mathbb{F}_4^N,\, Mc = g^n\}$$
$$= \min\{4^n - Z(M^{-1}g^n) \mid M \in T_{\mathcal{P}}^{\otimes}\} = 4^n - \max\{Z(Mg^n) \mid M \in T_{\mathcal{P}}^{\otimes}\}$$
$$\geqslant 4^n - \left(\tfrac{4^n}{5} + \tfrac{1}{5} + \tfrac{3}{5}[n \equiv 0 \pmod 2]\right) = \tfrac{4}{5}4^n - \tfrac{1}{5} - \tfrac{3}{5}[n \equiv 0 \pmod 2] = \left\lfloor \tfrac{4}{5}4^n \right\rfloor.$$

Следовательно, $L_{T_{\mathcal{P}}^{\otimes}}(n) = \max\{L_{T_{\mathcal{P}}^{\otimes}}(f) \mid f \in \mathbb{F}_4^N\} \geqslant \left\lfloor \frac{4}{5}4^n \right\rfloor$. □

Следствие 1. *В поле $\mathbb{F}_4$ справедлива оценка $L_{\mathcal{P}}(n) \geqslant \left\lfloor \frac{4}{5}4^n \right\rfloor$.*

Доказательство. Из лемм 1 и 4 работы [2] следует, что $L_{\mathcal{P}}(n) = L_{T_{\mathcal{P}}^{\otimes}}(n)$. Значит требуемая оценка следует из теоремы 1. □

Список литературы

1. Алексеев В. Б. О сложности реализации функций k-значной логики поляризованными полиномами / В. Б. Алексеев, А. А. Вороненко, С. Н. Селезнева // Дискретные модели в теории управляющих систем : тр. V Междунар. конф., Ратмино, 26-29 мая 2003 г. – М. : МАКС Пресс, 2003. – С. 8–9.
2. Балюк А. С. Верхние оценки сложности функций над конечными полями в некоторых классах кронекеровых форм / А. С. Балюк, Г. В. Янушковский // Изв. Иркут. гос. ун-та. Сер. Математика. – 2015. – Т. 14. – С. 3–17.
3. Грэхем Р. Конкретная математика. Основание информатики : пер. с англ. / Р. Грэхем, Д. Кнут, О. Паташник. – М. : Мир, 1998. – 703 с.
4. Маркелов Н. К. Нижняя оценка сложности функций трехзначной логики в классе поляризованных полиномов / Н. К. Маркелов // Вестн. Моск. ун-та. Сер. 15. Вычисл. математика и кибернетика. – 2012. – № 3. – С. 40–45.
5. Перязев Н. А. Сложность булевых функций в классе полиномиальных поляризованных форм / Н. А. Перязев // Алгебра и логика. – 1995. – Т. 34, № 3. – С. 323–326.

6. Селезнева С. Н. О сложности представления функций многозначных логик поляризованными полиномами / С. Н. Селезнева // Дискрет. математика. – 2002. – Т. 14, № 2. – С. 48–53.

Балюк Александр Сергеевич, кандидат физико-математических наук, доцент, Институт математики, экономики и информатики, Иркутский государственный университет, 664003, Иркутск, ул. К. Маркса, 1, тел.: (3952)242210 (e-mail: sacha@hotmail.ru)

Зинченко Анна Сергеевна, кандидат физико-математических наук, доцент, Институт математики, экономики и информатики, Иркутский государственный университет, 664003, Иркутск, ул. К. Маркса, 1, тел.: (3952)242210 (e-mail: azinchenko@gmail.com)

A. S. Baliuk, A. S. Zinchenko

Lower Bound of the Complexity of Functions over Finite Field of Order 4 in the Class of Polarized Polynomials

Abstract. The representations, including polynomial, of functions over final fields have been actively investigated. The complexity of such representations is the main stream of research. Polynomial representations of Boolean functions have been studied well enough. The exact values of the complexity have been found for a lot of polynomial classes.

Recently, the interest to polynomial representations of functions over finite fields and over finite rings is being increased. There are a lot of difficulties in studying of the complexity of these representations. Only not equal upper and lower bounds has been obtained, even for sagnificantly simple classes of polynomials.

This paper is about polarized polynomials over finite field of order 4. Such a polynomial is a finite sum of products. Every polynomial represents an n-variable function over finite field. A complexity of a polynomial is a number of nonzero summands in it. Every function can be represented by several polynomials, which are belongs to the same class. A complexity of a function in a class of polynomials is the minimal complexity of polynomials in the class, which represent this function.

Previously, the constructive lower bounds in the class of polarized polynomials have been known only for the case of Boolean and three-valued functions. Also, the weaker, non-constructive lower bound has been known for the case of functions over arbitrary prime finite field.

In this paper the constructive lower bound has been obtained for functions over finite field of order 4 in the class of polarized polynomials. The lower bound is equivalent to previously known lower bound for Boolean and three-valued functions.

Keywords: finite field, polarized polynomial, Kroneker form, complexity, lower bounds.

References

1. Alekseev V.B., Voronenko A.A., Selezneva S.N. On the complexity of representations of k-valued functions by polarized polynomials (in Russian). *In proceedings of V International conference «Discrete models in theory of control systems», Ratmino, May 26-29 2003*, 2003, pp. 8–9.

2. Baliuk A.S., Yanushkovsky G.V. Upper bounds of the complexity of functions over finite fields in some classes of Kroneker forms (in Russian). *IIGU Ser. Matematika*, 2015, vol. 14, pp. 3–17.
3. Graham R., Knuth D., Patashnik O. Concrete Mathematics. A Foundation for Computer Science. Addison Wesley, 1994. 672 p.
4. Markelov N.K. A lower estimate of the complexity of three-valued logic functions in the class of polarized polynomials. *Moscow University Computational Mathematics and Cybernetics*, 2012, vol. 36, issue 3, pp. 150–154.
5. Peryazev N.A. Complexity of Boolean functions in the class of polarized polynomial forms. *Algebra and Logic*, 1995, vol. 34, issue 3, pp. 177–179.
6. Selezneva S.N. On the complexity of the representation of functions of many-valued logics by polarized polynomials. *Discrete Mathematics and Applications*, 2002, vol. 12, no 3, pp. 229–234.

Baliuk Aleksandr Sergeevich, Candidate of Sciences (Physics and Mathematics), Irkutsk State University, 1, K. Marx st., Irkutsk, 664003 tel.: (3952)242210 (e-mail: `sacha@hotmail.ru`).

Zinchenko Anna Sergeevna, Candidate of Sciences (Physics and Mathematics), Irkutsk State University, 1, K. Marx st., Irkutsk, 664003 tel.: (3952)242210 (e-mail: `azinchenko@gmail.com`).