Серия «Математика»
2017. Т. 22. С. 18—30

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

ИЗВЕСТИЯ
Иркутского
государственного
университета

УДК 519.714.4
MSC 68Q17
DOI https://doi.org/10.26516/1997-7670.2017.22.18

Нижняя оценка сложности поляризованных полиномов семизначных функций

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

Аннотация. Одним из направлений исследования функций над конечными полями является исследование их представлений, в том числе полиномиальных. При изучении полиномиальных представлений функций можно выделить задачу оценки сложности таких представлений.

Под сложностью реализующего функцию полинома понимается число его ненулевых слагаемых. При этом каждая функция может быть представлена несколькими различными полиномами из одного класса. Под сложностью функции в классе полиномов понимается минимально возможная сложность реализующего ее полинома из этого класса. Под сложностью множества функций в классе полиномов понимается максимально возможная сложность функции из данного множества в классе полиномов.

В случае функций над конечным полем порядка 2 (булевых функций) для многих классов полиномиальных форм известны точные значения сложности таких представлений, а для функций над конечными полями порядка больше двух даже в довольно простых классах полиномов найдены только несовпадающие верхние и нижние оценки сложности.

Данная работа посвящена исследованию представления семизначных функций поляризованными полиномами. Полиномы этого класса имеют вид суммы конечного числа произведений определенного вида.

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

В предыдущих работах авторами были получены эффективные нижние оценки сложности для случая функций над конечными полями порядка 4 и 5.

В настоящей работе получена эффективная нижняя оценка сложности семизначных функций в классе поляризованных полиномов.

Ключевые слова: k-значная функция, конечное поле, поляризованный полином, кронекерова форма, нижняя оценка сложности.

1. Обозначения и определения

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

Будем использовать терминологию и обозначения из [2], а также условимся, что

- в выражениях приоритет операции кронекерова произведения является наивысшим;
- функция $\ell : \mathbb{F}_q \to \mathbb{N}$, где $\ell(a) = 1+(1+\min\{k \in \mathbb{N} \mid \xi^k = a\})[a\neq 0]$ для всех $a \in \mathbb{F}_q$, а ξ — примитивный элемент поля $\mathbb{F}_q$, задает линейный порядок на $\mathbb{F}_q$;
- если $v \in \mathbb{F}_q^n$, то положим $\ell(v) = 1 + \sum_{i=1}^n (\ell(v_i) - 1)\, q^{n-i}$, так что ℓ задает лексикографический порядок на $\mathbb{F}_q^n$;
- зафиксируем $\sigma^1, \ldots, \sigma^N \in \mathbb{F}_q^n$ так, что $\ell(\sigma^k) = k$ для всех k, $1 \leqslant k \leqslant N$;
- функцию $f : \mathbb{F}_q^n \to \mathbb{F}_q$ будем отождествлять с вектором $f \in \mathbb{F}_q^N$, $f = (f_1, \ldots, f_N)$, полагая $f_k = f(\sigma^k)$ для всех k, $1 \leqslant k \leqslant N = q^n$, и вместо $f : \mathbb{F}_q^n \to \mathbb{F}_q$ будем писать $f \in \mathbb{F}_q^N$;
- выражение $\sum_{t\in\tau} \varphi(t)$, в котором $\tau = (\tau_1, \ldots, \tau_k)$, $\tau_i \in \mathbb{N}$, $1 \leqslant i \leqslant k$ и $\varphi : \mathbb{N} \to \mathbb{R}$, будем отождествлять с $\sum_{i=1}^k \varphi(\tau_i)$.

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

$$\Phi_c^v(x_1, \ldots, x_n) = \sum_{t=1}^{N} c_t (x_1 + v_1)^{\ell(\sigma_1^t)-1} \ldots (x_n + v_n)^{\ell(\sigma_n^t)-1}, \qquad (1.1)$$

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; 6–9]. В работе [8] было показано, что $L_{\mathcal{P}}(n) = \left\lfloor \frac{2}{3} 2^n \right\rfloor$ для $q = 2$. В работе [7] 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 работе [2] для случая $q = 4$ была найдена оценка $L_{\mathcal{P}}(n) \geqslant \left\lfloor \frac{4}{5} 4^n \right\rfloor$, а в работе [3] для

случая $q = 5$ — оценка $L_{\mathcal{P}}(n) \geqslant \left\lfloor \frac{5}{6}5^n - \frac{2}{3}2^n \right\rfloor$. В настоящей работе для случа $q = 7$ устанавливается оценка $L_{\mathcal{P}}(n) \geqslant \left\lfloor \frac{7}{8}7^n - \frac{7}{8}(1+\sqrt{2})^n \right\rfloor$.

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

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

Определение 2. *Пару $\langle M, c\rangle$, где $M \in K^{\otimes n}$, $c \in \mathbb{F}_q^N$, 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 [4], где 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 $q = 7$, $n \in \mathbb{N}$, $N = 7^n$. Тогда $\mathbb{F}_q = \{0, 1, 2, 3, 4, 5, 6\}$. Далее будем считать, что все операции с матрицами и векторами выполняются по модулю 7.

Определим функции $g^n \in \mathbb{F}_7^N$ и $h^n \in \mathbb{F}_7^N$ рекуррентно следующим образом:

$$g^0 = (0), h^0 = (1),$$
$$g^{n+1} = (5g^n{+}4h^n, 5g^n{+}6h^n, 6g^n{+}6h^n, 4g^n{+}\ h^n, 4g^n{+}\ h^n, 4g^n{+}5h^n, g^n),$$
$$h^{n+1} = (\ g^n{+}6h^n, 5g^n{+}3g^n, 5g^n{+}4h^n, 2g^n{+}6h^n, 2g^n{+}6h^n, 3g^n, \qquad h^n).$$

Определим функции $f_t^n \in \mathbb{F}_7^N$ рекуррентно следующим образом:

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

Обратим внимание, что $f^n_{t+8} = 5f^n_t$. Действительно,

$$f^n_{t+4} = 2f^n_{t+3} + 2f^n_{t+2} = 6f^n_{t+2} + 4f^n_{t+1} = 2f^n_{t+1} + 5f^n_t$$
$$f^n_{t+8} = 2f^n_{t+5} + 5f^n_{t+4} = 4f^n_{t+2} + 6f^n_{t+1} + 4f^n_t = 5f^n_t.$$

Из этого, в частности, следует, что $f^n_{8k+i} = 5^k f^n_i$ для всех $k, i \in \mathbb{N}$.

Выпишем несколько начальных значений f^n_t:

$$\begin{array}{c} f^n_0 = g^n, f^n_1 = h^n, f^n_2 = 2g^n{+}2h^n, f^n_3 = 4g^n{+}6h^n, f^n_4 = 5g^n{+}2h^n, \\ f^n_5 = 4g^n{+}2h^n, f^n_6 = 4g^n{+}h^n, \;\; f^n_7 = 2g^n{+}6h^n, f^n_8 = 5g^n. \end{array} \tag{2.1}$$

Лемма 1. *Пусть $n \in \mathbb{N}$, $M_1 \in \mathbb{M}_7[7N{\times}7N]$, $M_2 \in \mathbb{M}_7[N{\times}N]$, и пусть $t_1, \ldots, t_7 \in \mathbb{N}$ и $a_1, \ldots, a_7 \in \mathbb{F}_7$ таковы, что выполняются векторные равенства*

$$M_1 g^{n+1} = (a_1 M_2 f^n_{t_1}, \ldots, a_7 M_2 f^n_{t_7}), \;\; M_1 h^{n+1} = (a_1 M_2 f^n_{t_1+1}, \ldots, a_7 M_2 f^n_{t_7+1}).$$

Тогда для всех $t \in \mathbb{N}$ выполняется $M_1 f^{n+1}_t = (a_1 M_2 f^n_{t_1+t}, \ldots, a_7 M_2 f^n_{t_7+t})$.

Доказательство аналогично доказательству леммы 1 в работе [3].

Для каждого $a \in \mathbb{F}_q$ определим матрицу $T_a \in \mathbb{M}_7[7{\times}7]$, элементы которой определены следующим образом: $T_a[i,j] = \binom{j-1}{i-1} a^{|j-i|}$, $1 \leqslant i, j \leqslant 7$. Зададим множество $T_{\mathcal{P}} \subset \mathbb{M}_7[7{\times}7]$ как $T_{\mathcal{P}} = \{T_a \mid a \in \mathbb{F}_7\}$. Обратим внимание, что $\binom{j-1}{i-1} = 0$ при $i > j$, поэтому матрицы из множества $T_{\mathcal{P}}$ — верхние треугольные, T_0 — единичная матрица, а остальные имеют следующий вид:

$$T_1 = \begin{bmatrix} 1&1&1&1&1&1&1 \\ 0&1&2&3&4&5&6 \\ 0&0&1&3&6&3&1 \\ 0&0&0&1&4&3&6 \\ 0&0&0&0&1&5&1 \\ 0&0&0&0&0&1&6 \\ 0&0&0&0&0&0&1 \end{bmatrix}, \quad T_2 = \begin{bmatrix} 1&2&4&1&2&4&1 \\ 0&1&4&5&4&3&3 \\ 0&0&1&6&3&3&2 \\ 0&0&0&1&1&5&6 \\ 0&0&0&0&1&3&4 \\ 0&0&0&0&0&1&5 \\ 0&0&0&0&0&0&1 \end{bmatrix}, \quad T_3 = \begin{bmatrix} 1&3&2&6&4&5&1 \\ 0&1&6&6&3&6&2 \\ 0&0&1&2&5&4&4 \\ 0&0&0&1&5&6&1 \\ 0&0&0&0&1&1&2 \\ 0&0&0&0&0&1&4 \\ 0&0&0&0&0&0&1 \end{bmatrix},$$

$$T_4 = \begin{bmatrix} 1&4&2&1&4&2&1 \\ 0&1&1&6&4&6&5 \\ 0&0&1&5&5&3&4 \\ 0&0&0&1&2&6&6 \\ 0&0&0&0&1&6&2 \\ 0&0&0&0&0&1&3 \\ 0&0&0&0&0&0&1 \end{bmatrix}, \quad T_5 = \begin{bmatrix} 1&5&4&6&2&3&1 \\ 0&1&3&5&3&3&4 \\ 0&0&1&1&3&4&2 \\ 0&0&0&1&6&5&1 \\ 0&0&0&0&1&4&4 \\ 0&0&0&0&0&1&2 \\ 0&0&0&0&0&0&1 \end{bmatrix}, \quad T_6 = \begin{bmatrix} 1&6&1&6&1&6&1 \\ 0&1&5&3&3&5&1 \\ 0&0&1&4&6&4&1 \\ 0&0&0&1&3&3&1 \\ 0&0&0&0&1&2&1 \\ 0&0&0&0&0&1&1 \\ 0&0&0&0&0&0&1 \end{bmatrix}.$$

Заметим, что $T_a^{-1} = T_{-a}$. Действительно, при $1 \leqslant i \leqslant j \leqslant 7$ выполняется (см., например, таблицу 199 в [5])

$$(T_{-a}T_a)[i,j] = \sum_{k=1}^{7} \tbinom{k-1}{i-1}(-a)^{|k-i|}\tbinom{j-1}{k-1}a^{|j-k|} = \sum_{k=i}^{j} \tbinom{k-1}{i-1}(-a)^{k-i}\tbinom{j-1}{k-1}a^{j-k}$$
$$= a^{j-i}\tbinom{j-1}{i-1}\sum_{k=i}^{j}(-1)^{k-i}\tbinom{j-i}{k-i} = a^{j-i}\tbinom{j-1}{i-1}(1-1)^{j-i} = [i{=}j].$$

Значит, $T_{-a}T_a = I_7$, в силу верхней треугольности матриц T_a и T_{-a}. Из этого следует, что $T_{\mathcal{P}} = \{M^{-1} \mid M \in T_{\mathcal{P}}\}$ и $T_{\mathcal{P}}^{\otimes n} = \{M^{-1} \mid M \in T_{\mathcal{P}}^{\otimes n}\}$.

Обратим внимание, что выполняются следующие матричные равенства, в которых элементы матриц, на которые умножаются матрицы $T_0, \ldots, T_6$, — это векторы из пространства $\mathbb{F}_7^N$, а столбцы представляют собой функции g^{n+1} и h^{n+1}.

$$T_0\begin{bmatrix} 5g^n{+}4h^n & g^n{+}6h^n \\ 5g^n{+}6h^n & 5g^n{+}3h^n \\ 6g^n{+}6h^n & 5g^n{+}4h^n \\ 4g^n{+}\ h^n & 2g^n{+}6h^n \\ 4g^n{+}\ h^n & 2g^n{+}6h^n \\ 4g^n{+}5h^n & 3g^n \\ g^n & h^n \end{bmatrix} = \begin{bmatrix} 5g^n{+}4h^n & g^n{+}6h^n \\ 5g^n{+}6h^n & 5g^n{+}3h^n \\ 6g^n{+}6h^n & 5g^n{+}4h^n \\ 4g^n{+}\ h^n & 2g^n{+}6h^n \\ 4g^n{+}\ h^n & 2g^n{+}6h^n \\ 4g^n{+}5h^n & 3g^n \\ g^n & h^n \end{bmatrix} = \begin{bmatrix} 3f_3^n & 3f_4^n \\ 3f_5^n & 3f_6^n \\ 3f_2^n & 3f_3^n \\ f_6^n & f_7^n \\ f_6^n & f_7^n \\ 2f_7^n & 2f_8^n \\ f_0^n & f_1^n \end{bmatrix} \tag{2.2}$$

$$T_1\begin{bmatrix} 5g^n{+}4h^n & g^n{+}6h^n \\ 5g^n{+}6h^n & 5g^n{+}3h^n \\ 6g^n{+}6h^n & 5g^n{+}4h^n \\ 4g^n{+}\ h^n & 2g^n{+}6h^n \\ 4g^n{+}\ h^n & 2g^n{+}6h^n \\ 4g^n{+}5h^n & 3g^n \\ g^n & h^n \end{bmatrix} = \begin{bmatrix} g^n{+}2h^n & 4g^n{+}5h^n \\ g^n{+}\ h^n & 2g^n{+}3h^n \\ 6g^n{+}2h^n & 4g^n{+}3h^n \\ 3g^n{+}6h^n & 5g^n{+}\ h^n \\ 4g^n{+}5h^n & 3g^n \\ 3g^n{+}5h^n & 3g^n{+}6h^n \\ g^n & h^n \end{bmatrix} = \begin{bmatrix} 2f_6^n & 2f_7^n \\ 4f_2^n & 4f_3^n \\ 5f_3^n & 5f_4^n \\ 6f_6^n & 6f_7^n \\ 2f_7^n & 2f_8^n \\ 6f_5^n & 6f_6^n \\ f_0^n & f_1^n \end{bmatrix} \tag{2.3}$$

$$T_2\begin{bmatrix} 5g^n{+}4h^n & g^n{+}6h^n \\ 5g^n{+}6h^n & 5g^n{+}3h^n \\ 6g^n{+}6h^n & 5g^n{+}4h^n \\ 4g^n{+}\ h^n & 2g^n{+}6h^n \\ 4g^n{+}\ h^n & 2g^n{+}6h^n \\ 4g^n{+}5h^n & 3g^n \\ g^n & h^n \end{bmatrix} = \begin{bmatrix} 5g^n & 5h^n \\ 3g^n{+}5h^n & 3g^n{+}6h^n \\ 2h^n & 4g^n{+}4h^n \\ 6g^n{+}6h^n & 5g^n{+}4h^n \\ 6g^n{+}2h^n & 4g^n{+}3h^n \\ 2g^n{+}5h^n & 3g^n{+}5h^n \\ g^n & h^n \end{bmatrix} = \begin{bmatrix} 5f_0^n & 5f_1^n \\ 6f_5^n & 6f_6^n \\ 2f_1^n & 2f_2^n \\ 3f_2^n & 3f_3^n \\ 5f_3^n & 5f_4^n \\ 6f_4^n & 6f_5^n \\ f_0^n & f_1^n \end{bmatrix} \tag{2.4}$$

$$T_3\begin{bmatrix} 5g^n{+}4h^n & g^n{+}6h^n \\ 5g^n{+}6h^n & 5g^n{+}3h^n \\ 6g^n{+}6h^n & 5g^n{+}4h^n \\ 4g^n{+}\ h^n & 2g^n{+}6h^n \\ 4g^n{+}\ h^n & 2g^n{+}6h^n \\ 4g^n{+}5h^n & 3g^n \\ g^n & h^n \end{bmatrix} = \begin{bmatrix} 2g^n{+}6h^n & 5g^n \\ 5g^n{+}4h^n & g^n{+}6h^n \\ 5g^n{+}5h^n & 3g^n{+}\ h^n \\ h^n & 2g^n{+}2h^n \\ 3g^n{+}6h^n & 5g^n{+}\ h^n \\ g^n{+}5h^n & 3g^n{+}4h^n \\ g^n & h^n \end{bmatrix} = \begin{bmatrix} f_7^n & f_8^n \\ 3f_3^n & 3f_4^n \\ 6f_2^n & 6f_3^n \\ f_1^n & f_2^n \\ 6f_6^n & 6f_7^n \\ 2f_3^n & 2f_4^n \\ f_0^n & f_1^n \end{bmatrix} \tag{2.5}$$

$$T_4\begin{bmatrix}5g^n{+}4h^n & g^n{+}6h^n\\ 5g^n{+}6h^n & 5g^n{+}3h^n\\ 6g^n{+}6h^n & 5g^n{+}4h^n\\ 4g^n{+}\ h^n & 2g^n{+}6h^n\\ 4g^n{+}\ h^n & 2g^n{+}6h^n\\ 4g^n{+}5h^n & 3g^n\\ g^n & h^n\end{bmatrix}=\begin{bmatrix}3g^n{+}6h^n & 5g^n{+}\ h^n\\ 3g^n{+}3h^n & 6g^n{+}2h^n\\ 6g^n{+}3h^n & 6g^n{+}5h^n\\ 5h^n & 3g^n{+}3h^n\\ 2g^n{+}3h^n & 6g^n{+}\ h^n\\ 5h^n & 3g^n{+}3h^n\\ g^n & h^n\end{bmatrix}=\begin{bmatrix}6f_6^n & 6f_7^n\\ 5f_2^n & 5f_3^n\\ 5f_5^n & 5f_6^n\\ 5f_1^n & 5f_2^n\\ 4f_3^n & 4f_4^n\\ 5f_1^n & 5f_2^n\\ f_0^n & f_1^n\end{bmatrix} \tag{2.6}$$

$$T_5\begin{bmatrix}5g^n{+}4h^n & g^n{+}6h^n\\ 5g^n{+}6h^n & 5g^n{+}3h^n\\ 6g^n{+}6h^n & 5g^n{+}4h^n\\ 4g^n{+}\ h^n & 2g^n{+}6h^n\\ 4g^n{+}\ h^n & 2g^n{+}6h^n\\ 4g^n{+}5h^n & 3g^n\\ g^n & h^n\end{bmatrix}=\begin{bmatrix}g^n{+}4h^n & g^n{+}2h^n\\ g^n{+}5h^n & 3g^n{+}4h^n\\ 5g^n{+}2h^n & 4g^n{+}2h^n\\ 4h^n & g^n{+}\ h^n\\ 3g^n & 3h^n\\ 6g^n{+}5h^n & 3g^n{+}2h^n\\ g^n & h^n\end{bmatrix}=\begin{bmatrix}2f_5^n & 2f_6^n\\ 2f_3^n & 2f_4^n\\ f_4^n & f_5^n\\ 4f_1^n & 4f_2^n\\ 3f_0^n & 3f_1^n\\ 5f_6^n & 5f_7^n\\ f_0^n & f_1^n\end{bmatrix} \tag{2.7}$$

$$T_6\begin{bmatrix}5g^n{+}4h^n & g^n{+}6h^n\\ 5g^n{+}6h^n & 5g^n{+}3h^n\\ 6g^n{+}6h^n & 5g^n{+}4h^n\\ 4g^n{+}\ h^n & 2g^n{+}6h^n\\ 4g^n{+}\ h^n & 2g^n{+}6h^n\\ 4g^n{+}5h^n & 3g^n\\ g^n & h^n\end{bmatrix}=\begin{bmatrix}3g^n{+}6h^n & 5g^n{+}\ h^n\\ 3g^n{+}4h^n & g^n{+}4h^n\\ h^n & 2g^n{+}2h^n\\ g^n{+}5h^n & 3g^n{+}4h^n\\ 6g^n{+}4h^n & g^n\\ 5g^n{+}5h^n & 3g^n{+}\ h^n\\ g^n & h^n\end{bmatrix}=\begin{bmatrix}6f_6^n & 6f_7^n\\ 2f_4^n & 2f_5^n\\ f_1^n & f_2^n\\ 2f_3^n & 2f_4^n\\ 3f_7^n & 3f_8^n\\ 6f_2^n & 6f_3^n\\ f_0^n & f_1^n\end{bmatrix} \tag{2.8}$$

Пусть $u \in \mathbb{F}_7^{7N}$, $u = (u^1, \ldots, u^7)$, где $u^1, \ldots, u^7 \in \mathbb{F}_7^N$, $M \in \mathbb{M}_7[N{\times}N]$, $M_0 \in \mathbb{M}_7[7{\times}7]$ и $v^1, \ldots, v^7 \in \mathbb{F}_7^N$ таковы, что выполняется матричное равенство

$$\begin{bmatrix}v^1\\ \vdots\\ v^7\end{bmatrix} = M_0\begin{bmatrix}u^1\\ \vdots\\ u^7\end{bmatrix}, \tag{2.9}$$

в котором элементами вектор-столбцов являются векторы из $\mathbb{F}_7^N$. Тогда, расписав покомпонентно (2.9), при $1 \leqslant t \leqslant 7$ и $1 \leqslant i \leqslant N$ имеем

$$v_i^t = \sum_{k=1}^{7} M_0[t,k]u_i^k$$

а следовательно, учитывая определение кронекерова произведения,

$$\begin{aligned}(M_0 \otimes Mu)_{(t-1)N+i} &= \sum_{k=1}^{7}\sum_{j=1}^{N} M_0[t,k]M[i,j]u_{(k-1)N+j}\\ &= \sum_{j=1}^{N} M[i,j]\sum_{k=1}^{7} M_0[t,k]u_j^k = \sum_{j=1}^{N} M[i,j]v_j^t = (Mv^t)_i,\end{aligned}$$

что в матричном виде можно записать как

$$M_0 \otimes M \begin{bmatrix} u^1 \\ \vdots \\ u^7 \end{bmatrix} = \begin{bmatrix} Mv^1 \\ \vdots \\ Mv^7 \end{bmatrix}. \tag{2.10}$$

Таким образом, на основании формул (2.2)–(2.8), используя лемму 1 и равенства (2.9), (2.10), можно получить следующие равенства.

$$\begin{array}{l}
T_0 \otimes Mf_t^{n+1} = (3Mf_{t+3}^n, 3Mf_{t+5}^n, 3Mf_{t+2}^n,\ Mf_{t+6}^n,\ Mf_{t+6}^n, 2Mf_{t+7}^n, Mf_t^n) \\
T_1 \otimes Mf_t^{n+1} = (2Mf_{t+6}^n, 4Mf_{t+2}^n, 5Mf_{t+3}^n, 6Mf_{t+6}^n, 2Mf_{t+7}^n, 6Mf_{t+5}^n, Mf_t^n) \\
T_2 \otimes Mf_t^{n+1} = (5Mf_t^n\ \ , 6Mf_{t+5}^n, 2Mf_{t+1}^n, 3Mf_{t+2}^n, 5Mf_{t+3}^n, 6Mf_{t+4}^n, Mf_t^n) \\
T_3 \otimes Mf_t^{n+1} = (\ Mf_{t+7}^n, 3Mf_{t+3}^n, 6Mf_{t+2}^n,\ Mf_{t+1}^n, 6Mf_{t+6}^n, 2Mf_{t+3}^n, Mf_t^n) \\
T_4 \otimes Mf_t^{n+1} = (6Mf_{t+6}^n, 5Mf_{t+2}^n, 5Mf_{t+5}^n, 5Mf_{t+1}^n, 4Mf_{t+3}^n, 5Mf_{t+1}^n, Mf_t^n) \\
T_5 \otimes Mf_t^{n+1} = (2Mf_{t+5}^n, 2Mf_{t+3}^n,\ Mf_{t+4}^n, 4Mf_{t+1}^n, 3Mf_t^n\ \ , 5Mf_{t+6}^n, Mf_t^n) \\
T_6 \otimes Mf_t^{n+1} = (6Mf_{t+6}^n, 2Mf_{t+4}^n,\ Mf_{t+1}^n, 2Mf_{t+3}^n, 3Mf_{t+7}^n, 6Mf_{t+2}^n, Mf_t^n)
\end{array} \tag{2.11}$$

Определим наборы $\tau^0, \ldots, \tau^6$ следующим образом.

$$\begin{array}{lll}
\tau^0 = (3,5,2,6,6,7,0) & \tau^1 = (6,2,3,6,7,5,0) & \tau^2 = (0,5,1,2,3,4,0) \\
\tau^3 = (7,3,2,1,6,3,0) & \tau^4 = (6,2,5,1,3,1,0) & \tau^5 = (5,3,4,1,0,6,0) \\
\tau^6 = (6,4,1,3,7,2,0) &&
\end{array} \tag{2.12}$$

Тогда (2.11) можно переписать в следующем виде.

$$\begin{array}{l}
T_0 \otimes Mf_t^{n+1} = (3Mf_{t+\tau_1^0}^n, 3Mf_{t+\tau_2^0}^n, 3Mf_{t+\tau_3^0}^n,\ Mf_{t+\tau_4^0}^n,\ Mf_{t+\tau_5^0}^n, 2Mf_{t+\tau_6^0}^n, Mf_{t+\tau_7^0}^n) \\
T_1 \otimes Mf_t^{n+1} = (2Mf_{t+\tau_1^1}^n, 4Mf_{t+\tau_2^1}^n, 5Mf_{t+\tau_3^1}^n, 6Mf_{t+\tau_4^1}^n, 2Mf_{t+\tau_5^1}^n, 6Mf_{t+\tau_6^1}^n, Mf_{t+\tau_7^1}^n) \\
T_2 \otimes Mf_t^{n+1} = (5Mf_{t+\tau_1^2}^n, 6Mf_{t+\tau_2^2}^n, 2Mf_{t+\tau_3^2}^n, 3Mf_{t+\tau_4^2}^n, 5Mf_{t+\tau_5^2}^n, 6Mf_{t+\tau_6^2}^n, Mf_{t+\tau_7^2}^n) \\
T_3 \otimes Mf_t^{n+1} = (\ Mf_{t+\tau_1^3}^n, 3Mf_{t+\tau_2^3}^n, 6Mf_{t+\tau_3^3}^n,\ Mf_{t+\tau_4^3}^n, 6Mf_{t+\tau_5^3}^n, 2Mf_{t+\tau_6^3}^n, Mf_{t+\tau_7^3}^n) \\
T_4 \otimes Mf_t^{n+1} = (6Mf_{t+\tau_1^4}^n, 5Mf_{t+\tau_2^4}^n, 5Mf_{t+\tau_3^4}^n, 5Mf_{t+\tau_4^4}^n, 4Mf_{t+\tau_5^4}^n, 5Mf_{t+\tau_6^4}^n, Mf_{t+\tau_7^4}^n) \\
T_5 \otimes Mf_t^{n+1} = (2Mf_{t+\tau_1^5}^n, 2Mf_{t+\tau_2^5}^n,\ Mf_{t+\tau_3^5}^n, 4Mf_{t+\tau_4^5}^n, 3Mf_{t+\tau_5^5}^n, 5Mf_{t+\tau_6^5}^n,\ Mf_{t\tau_7^5}^n) \\
T_6 \otimes Mf_t^{n+1} = (6Mf_{t+\tau_1^6}^n, 2Mf_{t+\tau_2^6}^n,\ Mf_{t+\tau_3^6}^n, 2Mf_{t+\tau_4^6}^n, 3Mf_{t+\tau_5^6}^n, 6Mf_{t+\tau_6^6}^n, Mf_{t+\tau_7^6}^n)
\end{array}$$

Откуда следует, что при $0 \leqslant k \leqslant 6$ выполняется

$$Z(T_k \otimes Mf_t^{n+1}) = \sum_{i \in \tau^k} Z(Mf_{t+i}^n). \tag{2.13}$$

Пусть α — вещественное, а i, j, k — целые числа. Введем в рассмотрение следующую величину.

$$\begin{aligned}
\theta(\alpha, k, j, i) &= \cos(\alpha + \tfrac{\pi k}{4}) + \cos(\alpha + \tfrac{\pi(k+2j)}{4}) + \cos(\alpha + \tfrac{\pi(k+i)}{4}) \\
&= 2\cos(\alpha + \tfrac{\pi(k+j)}{4}) \cos\tfrac{\pi j}{4} + \cos(\alpha + \tfrac{\pi(k+i)}{4})
\end{aligned}$$

Тогда

$$
\begin{aligned}
&\theta(\alpha,k,j,i)=\theta(\alpha,k,j+4,i),\\
&\theta(\alpha,k,j,i)=\theta(\alpha,k,j,i+8),\\
&\theta(\alpha,k,0,2)=2\cos(\alpha+\tfrac{\pi k}{4})+\cos(\alpha+\tfrac{\pi(k+2)}{4})\\
&\qquad=\sqrt{5}\left(-\tfrac{2}{\sqrt{5}}\sin(\alpha+\tfrac{\pi(k+2)}{4})+\tfrac{1}{\sqrt{5}}\cos(\alpha+\tfrac{\pi(k+2)}{4})\right)\\
&\qquad=\sqrt{5}\cos\left(\alpha+\tfrac{\pi(k+2)}{4}+\arctan 2\right),\\
&\theta(\alpha,k,0,-2)=2\cos(\alpha+\tfrac{\pi k}{4})+\cos(\alpha+\tfrac{\pi(k-2)}{4})\\
&\qquad=\sqrt{5}\left(\tfrac{2}{\sqrt{5}}\sin(\alpha+\tfrac{\pi(k-2)}{4})+\tfrac{1}{\sqrt{5}}\cos(\alpha+\tfrac{\pi(k-2)}{4})\right)\\
&\qquad=\sqrt{5}\cos\left(\alpha+\tfrac{\pi(k-2)}{4}-\arctan 2\right),\\
&\theta(\alpha,k,1,3)=2\cos(\alpha+\tfrac{\pi(k+1)}{4})\cos\tfrac{\pi}{4}+\cos(\alpha+\tfrac{\pi(k+3)}{4})\\
&\qquad=\sqrt{3}\left(-\tfrac{\sqrt{2}}{\sqrt{3}}\sin(\alpha+\tfrac{\pi(k+3)}{4})+\tfrac{1}{\sqrt{3}}\cos(\alpha+\tfrac{\pi(k+3)}{4})\right)\\
&\qquad=\sqrt{3}\cos\left(\alpha+\tfrac{\pi(k+3)}{4}+\arctan\sqrt{2}\right),\\
&\theta(\alpha,k,1,7)=2\cos(\alpha+\tfrac{\pi(k+1)}{4})\cos\tfrac{\pi}{4}+\cos(\alpha+\tfrac{\pi(k+7)}{4})\\
&\qquad=\sqrt{3}\left(\tfrac{\sqrt{2}}{\sqrt{3}}\sin(\alpha+\tfrac{\pi(k-1)}{4})+\tfrac{1}{\sqrt{3}}\cos(\alpha+\tfrac{\pi(k-1)}{4})\right)\\
&\qquad=\sqrt{3}\cos\left(\alpha+\tfrac{\pi(k-1)}{4}-\arctan\sqrt{2}\right),\\
&\theta(\alpha,k,1,1)=2\cos(\alpha+\tfrac{\pi(k+1)}{4})\cos\tfrac{\pi}{4}+\cos(\alpha+\tfrac{\pi(k+1)}{4})\\
&\qquad=\sqrt{2}\cos(\alpha+\tfrac{\pi(k+1)}{4})+\cos(\alpha+\tfrac{\pi(k+1)}{4})\\
&\qquad=(\sqrt{2}+1)\cos(\alpha+\tfrac{\pi(k+1)}{4}),
\end{aligned}
\tag{2.14}
$$

$$
\begin{aligned}
\theta(\alpha,k,3,3)&=2\cos(\alpha+\tfrac{\pi(k+3)}{4})\cos\tfrac{3\pi}{4}+\cos(\alpha+\tfrac{\pi(k+3)}{4})\\
&=\cos(\alpha+\tfrac{\pi(k+3)}{4})\left(1-\sqrt{2}\right)=(\sqrt{2}-1)\cos(\alpha+\tfrac{\pi(k-1)}{4}).
\end{aligned}
\tag{2.15}
$$

Лемма 2. *Пусть* $M_1,\dots,M_n\in T_{\mathcal{P}}$, $M=M_1\otimes\cdots\otimes M_n$, *и пусть* $n_i=\#\{j\mid 1\leqslant j\leqslant n,\ M_j=T_i\}$, $0\leqslant i\leqslant 6$. *Тогда для любого* $t\in\mathbb{N}$

$$
\begin{aligned}
Z(Mf_t^n)=\tfrac{7^n}{8}+C_M(-1)^t+A_M\cos\big(\lambda_M+\tfrac{\pi t}{2}\big)\\
+B_M\cos\big(\beta_M+\tfrac{\pi t}{4}\big)+D_M\cos\big(\delta_M+\tfrac{3\pi t}{4}\big),\ \text{где}
\end{aligned}
\tag{2.16}
$$

$C_M=\frac{1}{8}(-1)^{n_3+n_4}$,
$A_M=\frac{1}{4}\sqrt{5}^{n_0+n_1+n_2+n_3+n_4+n_5}$,
$B_M=\frac{1}{4}\sqrt{3}^{n_0+n_1+n_2+n_3+n_4}(\sqrt{2}-1)^{n_5}$,
$D_M=\frac{1}{4}\sqrt{3}^{n_0+n_1+n_2+n_3+n_4}(\sqrt{2}+1)^{n_5}$,
$\lambda_M=(n-2n_3-n_6)\arctan 2+\frac{\pi}{2}(3n_0+3n_1+n_2+2n_3+2n_4+n_5+3n_6)$,
$\beta_M=(-n_0-n_1+n_2-n_3-n_4)\arctan\sqrt{2}+\frac{\pi}{4}(5n_0+5n_1+3n_2-n_5+n_6)$,
$\delta_M=(-n_0-n_1+n_2-n_3-n_4)\arctan\sqrt{2}+\frac{3\pi}{4}(-3n_0-3n_1+3n_2+3n_5+n_6)$.

Доказательство. Доказательство проведем индукцией по n.

Базис индукции. Пусть $n=0$. Тогда $n_0=n_1=n_2=\cdots=n_6=0$. $f_{8k}^0=5^kg^0=(0)$ для всех $k\in\mathbb{N}$. Если же $t=8k+i$, где $k\in\mathbb{N}$ и $1\leqslant i\leqslant 7$,

то, поскольку $5^k \not\equiv 0 \pmod 7$ и $(0) \notin \{f_i^0 \mid 1 \leqslant i \leqslant 7\} = \{(1), (2), (6)\}$, имеем $f_t^0 = 5^k f_i^0 \neq (0)$. Матрица $M = I_1$, и поэтому $Mv = v$ для всех $v \in \mathbb{F}_7^1$. Таким образом, $Z(Mf_t^0) = [t \equiv 0 \pmod 8]$. С другой стороны, $C_M = \frac{1}{8}$, $A_M = B_M = D_M = \frac{1}{4}$, $\lambda_M = \beta_M = \delta_M = 0$. Тогда правая часть (2.16), обозначим её R_t, примет вид

$$\begin{aligned} R_t &= \tfrac{1}{8} + \tfrac{1}{8}(-1)^t + \tfrac{1}{4}\cos\tfrac{\pi t}{2} + \tfrac{1}{4}\cos\tfrac{\pi t}{4} + \tfrac{1}{4}\cos\tfrac{3\pi t}{4} \\ &= \tfrac{1}{8} + \tfrac{1}{8}(-1)^t + \tfrac{1}{4}\cos\tfrac{\pi t}{2} + \tfrac{1}{2}\cos\tfrac{\pi t}{2}\cos\tfrac{\pi t}{4}. \end{aligned}$$

Следовательно, для всех $k \in \mathbb{N}$ выполняется

$$\begin{gathered} R_{2k+1} = \tfrac{1}{8} - \tfrac{1}{8} + 0 + 0 = 0, \quad R_{4k+2} = \tfrac{1}{8} + \tfrac{1}{8} - \tfrac{1}{4} + 0 = 0, \\ R_{8k+4} = \tfrac{1}{8} + \tfrac{1}{8} + \tfrac{1}{4} - \tfrac{1}{2} = 0, \quad R_{8k} = \tfrac{1}{8} + \tfrac{1}{8} + \tfrac{1}{4} + \tfrac{1}{2} = 1, \end{gathered}$$

а значит, $R_t = [t \equiv 0 \pmod 8]$. Правая и левая части равенства (2.16) совпадают, поэтому базис индукции выполнен.

Шаг индукции. Пусть для некоторого $n \in \mathbb{N}$ выполнено утверждение леммы. Покажем, что оно справедливо и для $n+1$.

Из (2.13) и (2.16) следует, что при $0 \leqslant k \leqslant 6$ выполняется

$$Z(T_k \otimes Mf_t^{n+1}) = \tfrac{7^{n+1}}{8} + C_M S_k^C + A_M S_k^A + B_M S_k^B + D_M S_k^D,$$

где

$$\begin{aligned} S_k^A &= \textstyle\sum_{i \in \tau^k} \cos(\lambda_M + \frac{\pi(t+i)}{2}), & S_k^B &= \textstyle\sum_{i \in \tau^k} \cos(\beta_M + \frac{\pi(t+i)}{4}), \\ S_k^C &= \textstyle\sum_{i \in \tau^k} (-1)^{t+i}, & S_k^D &= \textstyle\sum_{i \in \tau^k} \cos(\delta_M + \frac{3\pi(t+i)}{4}). \end{aligned} \tag{2.17}$$

Обратим внимание, что для любого $t \in \mathbb{N}$ и любого действительного числа α выполняются следующие равенства.

$$\begin{gathered} (-1)^t + (-1)^{t+1} = 0, \\ \cos\big(\alpha + \tfrac{\pi t}{2}\big) + \cos\big(\alpha + \tfrac{\pi(t+2)}{2}\big) = 0, \ \cos\big(\alpha + \tfrac{\pi t}{2}\big) = \cos\big(\alpha + \tfrac{\pi(t+4)}{2}\big), \\ \cos\big(\alpha + \tfrac{\pi t}{4}\big) + \cos\big(\alpha + \tfrac{\pi(t+4)}{4}\big) = 0, \ \cos\big(\alpha + \tfrac{3\pi t}{4}\big) + \cos\big(\alpha + \tfrac{3\pi(t+4)}{4}\big) = 0. \end{gathered}$$

Тогда из (2.17) и определений τ^k (2.12) следует, что

$$\begin{aligned} S_k^A &= \textstyle\sum_{i \in u^k} \cos(\lambda_M + \frac{\pi(t+i)}{2}), & S_k^B &= \textstyle\sum_{i \in v^k} \cos(\beta_M + \frac{\pi(t+i)}{4}), \\ S_k^C &= (-1)^{[k=3]+[k=4]}(-1)^t, & S_k^D &= \textstyle\sum_{i \in v^k} \cos(\delta_M + \frac{3\pi(t+i)}{4}), \end{aligned}$$

где

$$\begin{gathered} u^0 = (2,2,3), \ u^1 = (2,2,3), \ u^2 = (0,0,1), \\ u^3 = (2,3,3), \ u^4 = (1,1,2), \ u^5 = (0,0,1), \ u^6 = (3), \\ v^0 = (0,5,6), \ v^1 = (0,5,6), \ v^2 = (0,2,3), \\ v^3 = (0,1,3), \ v^4 = (0,1,3), \ v^5 = (0,3,6), \ v^6 = (1), \end{gathered}$$

Используя определение θ, (2.14) и (2.15), имеем

$$\begin{aligned}
S_0^A = S_1^A &= \textstyle\sum_{i\in(2,2,3)} \cos\Big(\lambda_M + \frac{\pi(t+i)}{2}\Big) = \theta(\lambda_M, 2t+4, 0, 2)\\
&= \sqrt{5}\cos\Big(\lambda_M + \tfrac{\pi(t+3)}{2} + \arctan 2\Big),\\
S_2^A = S_5^A &= \textstyle\sum_{i\in(0,0,1)} \cos\Big(\lambda_M + \frac{\pi(t+i)}{2}\Big) = \theta(\lambda_M, 2t, 0, 2)\\
&= \sqrt{5}\cos\Big(\lambda_M + \tfrac{\pi(t+1)}{2} + \arctan 2\Big),\\
S_3^A &= \textstyle\sum_{i\in(2,3,3)} \cos\Big(\lambda_M + \frac{\pi(t+i)}{2}\Big) = \theta(\lambda_M, 2t+6, 0, -2)\\
&= \sqrt{5}\cos\Big(\lambda_M + \tfrac{\pi(t+2)}{2} - \arctan 2\Big),\\
S_4^A &= \textstyle\sum_{i\in(1,1,2)} \cos\Big(\lambda_M + \frac{\pi(t+i)}{2}\Big) = \theta(\lambda_M, 2t+2, 0, 2)\\
&= \sqrt{5}\cos\Big(\lambda_M + \tfrac{\pi(t+2)}{2} + \arctan 2\Big),\\
S_6^A &= \textstyle\sum_{i\in(3)} \cos\Big(\lambda_M + \frac{\pi(t+i)}{2}\Big) = \cos\Big(\lambda_M + \frac{\pi(t+3)}{2}\Big);
\end{aligned}$$

$$\begin{aligned}
S_0^B = S_1^B &= \textstyle\sum_{i\in(0,5,6)} \cos\Big(\beta_M + \frac{\pi(t+i)}{4}\Big) = \theta(\beta_M, t+6, -3, -1)\\
&= \theta(\beta_M, t+6, 1, 7) = \sqrt{3}\cos\Big(\beta_M + \tfrac{\pi(t+5)}{4} - \arctan\sqrt{2}\Big),\\
S_2^B &= \textstyle\sum_{i\in(0,2,3)} \cos\Big(\beta_M + \frac{\pi(t+i)}{4}\Big) = \theta(\beta_M, t, 1, 3)\\
&= \sqrt{3}\cos\Big(\beta_M + \tfrac{\pi(t+3)}{4} + \arctan\sqrt{2}\Big),\\
S_3^B = S_4^B &= \textstyle\sum_{i\in(0,1,3)} \cos\Big(\beta_M + \frac{\pi(t+i)}{4}\Big) = \theta(\beta_M, t+1, 1, -1)\\
&= \theta(\beta_M, t+1, 1, 7) = \sqrt{3}\cos\Big(\beta_M + \tfrac{\pi t}{4} - \arctan\sqrt{2}\Big),\\
S_5^B &= \textstyle\sum_{i\in(0,3,6)} \cos\Big(\beta_M + \frac{\pi(t+i)}{4}\Big) = \theta(\beta_M, t, 3, 3)\\
&= (\sqrt{2}-1)\cos\Big(\beta_M + \tfrac{\pi(t-1)}{4}\Big),\\
S_6^B &= \textstyle\sum_{i\in(1)} \cos\Big(\beta_M + \frac{\pi(t+i)}{4}\Big) = \cos\Big(\beta_M + \frac{\pi(t+1)}{4}\Big);
\end{aligned}$$

$$\begin{aligned}
S_0^D = S_1^D &= \textstyle\sum_{i\in(0,5,6)} \cos\Big(\delta_M + \frac{3\pi(t+i)}{4}\Big) = \theta(\delta_M, 3t, 9, 15)\\
&= \theta(\delta_M, 3t, 1, 7) = \sqrt{3}\cos\Big(\delta_M + \tfrac{3\pi(t-3)}{4} - \arctan\sqrt{2}\Big),\\
S_2^D &= \textstyle\sum_{i\in(0,2,3)} \cos\Big(\delta_M + \frac{3\pi(t+i)}{4}\Big) = \theta(\delta_M, 3t+6, -3, 3)\\
&= \theta(\delta_M, 3t+6, 1, 3) = \sqrt{3}\cos\Big(\delta_M + \tfrac{3\pi(t+3)}{4} + \arctan\sqrt{2}\Big),\\
S_3^D = S_4^D &= \textstyle\sum_{i\in(0,1,3)} \cos\Big(\delta_M + \frac{3\pi(t+i)}{4}\Big) = \theta(\delta_M, 3t+9, -3, -9)\\
&= \theta(\delta_M, 3t+9, 1, 7) = \sqrt{3}\cos\Big(\delta_M + \tfrac{3\pi t}{4} - \arctan\sqrt{2}\Big),\\
S_5^D &= \textstyle\sum_{i\in(0,3,6)} \cos\Big(\delta_M + \frac{3\pi(t+i)}{4}\Big) = \theta(\delta_M, 3t, 9, 9)\\
&= \theta(\delta_M, 3t, 1, 1) = (\sqrt{2}+1)\cos\Big(\delta_M + \tfrac{3\pi(t+3)}{4}\Big),\\
S_6^D &= \textstyle\sum_{i\in(1)} \cos\Big(\delta_M + \frac{3\pi(t+i)}{4}\Big) = \cos\Big(\delta_M + \frac{3\pi(t+1)}{4}\Big).
\end{aligned}$$

Таким образом, во всех случаях при $0 \leqslant k \leqslant 6$

$$C_M S_k^C = C_{T_k \otimes M}(-1)^t, \qquad B_M S_k^B = B_{T_k \otimes M} \cos\bigl(\beta_{T_k \otimes M} + \tfrac{\pi t}{4}\bigr),$$
$$A_M S_k^A = A_{T_k \otimes M} \cos\bigl(\lambda_{T_k \otimes M} + \tfrac{\pi t}{2}\bigr), \quad D_M S_k^D = D_{T_k \otimes M} \cos\bigl(\delta_{T_k \otimes M} + \tfrac{3\pi t}{4}\bigr),$$

и, следовательно,

$$Z\bigl((T_k \otimes M) f_t^n\bigr) = \tfrac{7^{n+1}}{8} + C_{T_k \otimes M}(-1)^t + A_{T_k \otimes M} \cos\bigl(\lambda_{T_k \otimes M} + \tfrac{\pi t}{2}\bigr) + B_{T_k \otimes M} \cos\bigl(\beta_{T_k \otimes M} + \tfrac{\pi t}{4}\bigr) + D_{T_k \otimes M} \cos\bigl(\delta_{T_k \otimes M} + \tfrac{3\pi t}{4}\bigr).$$

Шаг индукции выполнен. Лемма доказана. □

Теорема 1. *В конечном поле порядка 7 справедлива следующая оценка*

$$L_{T_{\mathcal{P}}^{\otimes}}(n) \geqslant \tfrac{7}{8} 7^n - \tfrac{7}{8}(\sqrt{2}+1)^n.$$

Доказательство. По лемме 2, учитывая, что для всех $M \in T_{\mathcal{P}}^{\otimes n}$

$$\sqrt{2} - 1 < |-1| < \sqrt{3} < \sqrt{5} < \sqrt{2} + 1,$$
$$|C_M| \leqslant \tfrac{1}{8}(\sqrt{2}+1)^n, |A_M| \leqslant \tfrac{1}{4}(\sqrt{2}+1)^n,$$
$$|B_M| \leqslant \tfrac{1}{4}(\sqrt{2}+1)^n, |D_M| \leqslant \tfrac{1}{4}(\sqrt{2}+1)^n,$$

выполняется $\max\{Z(Mg^n) \mid M \in T_{\mathcal{P}}^{\otimes n}\} \leqslant \frac{7^n}{8} + \frac{7}{8}(\sqrt{2}+1)^n$. Тогда, поскольку $L(\langle M, c\rangle) = 7^n - Z(c)$, а $T_{\mathcal{P}}^{\otimes n} = \{M^{-1} \mid M \in T_{\mathcal{P}}^{\otimes n}\}$

$$L_{T_{\mathcal{P}}^{\otimes}}(g^n) = \min\{L(\langle M, c\rangle) \mid M \in T_{\mathcal{P}}^{\otimes n},\, c \in \mathbb{F}_7^N,\, Mc = g^n\}$$
$$= \min\{7^n - Z(M^{-1}g^n) \mid M \in T_{\mathcal{P}}^{\otimes n}\} = 7^n - \max\{Z(Mg^n) \mid M \in T_{\mathcal{P}}^{\otimes n}\}$$
$$\geqslant 7^n - \Bigl(\tfrac{7^n}{8} + \tfrac{7}{8}(\sqrt{2}+1)^n\Bigr) = \tfrac{7}{8}7^n - \tfrac{7}{8}(\sqrt{2}+1)^n.$$

Значит, $L_{T_{\mathcal{P}}^{\otimes}}(n) = \max\{L_{T_{\mathcal{P}}^{\otimes}}(f) \mid f \in \mathbb{F}_7^N\} \geqslant \frac{7}{8}7^n - \frac{7}{8}(\sqrt{2}+1)^n$. □

Следствие 1. *В поле $\mathbb{F}_7$ справедлива оценка $L_{\mathcal{P}}(n) \geqslant \frac{7}{8}7^n - \frac{7}{8}(\sqrt{2}+1)^n$.*

Доказательство. В теореме 2 из [4] доказано, что в поле нечетной характеристики $L_{\mathcal{P}}(n) = L_{T_{\mathcal{P}}^{\otimes}}(n)$. 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. Нижняя оценка сложности функций над конечным полем порядка 4 в классе поляризованных полиномов / А. С. Балюк, А. С. Зинченко // Изв. Иркут. гос. ун-та. Сер. Математика. – 2016. – Т. 16. – С. 19–29.

3. Балюк А. С. Нижняя оценка сложности пятизначных функций в классе поляризованных полиномов / А. С. Балюк, А. С. Зинченко // Дискрет. математика. – 2016. – Т. 28, № 4. – С. 29–37.
4. 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.
5. Грэхэм Р. Конкретная математика. Основание информатики : пер. с англ. / Р. Грэхем, Д. Кнут, О. Паташник. – М. : Мир, 1998. – 703 с.
6. Казимиров А. С. Верхние оценки сложности функций над непростыми конечными полями в классе поляризованных полиномов / А. С. Казимиров, С. Ю. Реймеров // Изв. Иркут. гос. ун-та. Сер. Математика. – 2016. – Т. 17. – С. 37–45.
7. 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.
8. Перязев Н. А. Сложность булевых функций в классе полиномиальных поляризованных форм / Н. А. Перязев // Алгебра и логика. – 1995. – Т. 34, № 3. – С. 323–326.
9. 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, 664000, Россия, г. Иркутск, ул. К. Маркса, 1, тел.: (3952)940160 (e-mail: sacha@hotmail.ru)

Зинченко Анна Сергеевна, кандидат физико-математических наук, доцент, Институт математики, экономики и информатики, Иркутский государственный университет, 664000, Россия, 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 Seven-Valued Functions in the Class of Polarized Polynomials

Abstract. One of the directions of the investigation of functions over finite fields is the study of their representations, including polynomial ones. In the area of polynomial representations of functions the problem of estimating the complexity of such representations can be highlighted.

The complexity of the polynomial, representing the function, is the number of its nonzero terms. Each function can be represented by several different polynomials from the same class. The complexity of a function in the class of polynomials is the least possible complexity of a polynomial from this class, representing the function. The complexity of the given set of functions in the class of polynomials is the maximal complexity of a function from the set in this class of polynomials.

In the case of functions over a finite field of order 2 (Boolean functions), exact values of the complexity of such representations are known for many classes of polynomial forms.

But for functions over finite fields of order greater than two, even in fairly simple classes of polynomials, only mismatched upper and lower bounds of complexity have been found.

This paper is devoted to the study of the representation of seven-valued functions by polarized polynomials. The polynomials of this class have the form of a sum of a finite number of products of a certain type.

For the case of Boolean and three-valued functions, effective lower bounds for the complexity in the class of polarized polynomials are known, as well as a weaker power estimate for functions over a finite field of prime order.

In previous papers, the authors obtained effective lower bounds for the complexity of functions over finite fields of order 4 and 5 in the class of polarized polynomials.

In this paper an effective lower bound for the complexity of seven-valued functions in the class of polarized polynomials has been obtained.

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. *Proc. of the Int. Workshop on Discrete Mathematics and Mathematical Cybernetics*, Ratmino, 2003, pp 8–9. (in Russian)
2. Baliuk A.S., Zinchenko A.S. Lower bound of the complexity of functions over finite field of order 4 in the class of polarized polynomials. *Izv. Irkutsk. Gos. Univ., Ser. Mat.*, 2016, vol. 16, pp. 19–29. (in Russian)
3. Baliuk A.S., Zinchenko A.S. Lower bound of the complexity of five-valued functions in the class of polarized polynomials. *Diskr. Mat.*, 2016, vol. 28, issue 4, pp. 29–37. (in Russian)
4. Baliuk A.S., Yanushkovsky G.V. Upper bounds of the complexity of functions over finite fields in some classes of Kroneker forms. *Izv. Irkutsk. Gos. Univ., Ser. Mat.*, 2015, vol. 14, pp. 3–17. (in Russian)
5. Graham R., Knuth D., Patashnik O. Concrete Mathematics. A Foundation for Computer Science. Addison Wesley, 1994. 672 p.
6. Kazimirov A.S., Reymerov S. Yu. On upper bounds of the complexity of functions over nonprime finite fields in some classes of polarized polynomials. *Izv. Irkutsk. Gos. Univ., Ser. Mat.*, 2016, vol. 17, pp. 37–45. (in Russian)
7. Markelov N.K. A lower estimate of the complexity of three-valued logic functions in the class of polarized polynomials. *Vestn. Mosk. Univ., Ser. 15: Vychisl. Matem. Kibern.*, 2012. vol. 36. issue 3. pp. 150–154.
8. 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.
9. Selezneva S.N. On the complexity of the representation of functions of many-valued logics by polarized polynomials. *Discrete Math. Appl.*, 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, Russian Federation, tel.: (3952)940160 (e-mail: sacha@hotmail.ru).

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