Серия «Математика»
2016. Т. 17. С. 37—45

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

ИЗВЕСТИЯ
Иркутского
государственного
университета

УДК 519.715
MSC 68Q17

Верхние оценки сложности функций над непростыми конечными полями в классе поляризованных полиномов *

А. С. Казимиров, С. Ю. Реймеров
Иркутский государственный университет

Аннотация. В настоящее время активно исследуются представления дискретных функций над конечными полями, в том числе полиномиальные. Одним из основных направлений этих исследований является сложность таких представлений.

В статье предложены новые верхние оценки сложности дискретных функций над некоторыми конечными полями в классе поляризованных полиномов. При этом результаты излагаются на языке матричных форм. Под матричной формой понимается представление вектора функции в виде произведения квадратной невырожденной матрицы и вектор-столбца. Сложность функции в классе поляризованных полиномов совпадает со сложностью функции в классе матричных форм специального вида.

Под сложностью матричной формы понимается число ненулевых элементов в векторе этой формы. Каждая функция может быть реализована несколькими матричными формами из одного класса. Под сложностью функции в классе понимается минимально возможная сложность реализующей ее матричной формы из этого класса.

В данной работе получены верхние оценки для функций над полями порядков 2^k и p^k, где p — простое и $p \geqslant 3$.

Ключевые слова: конечное поле; полином; поляризованный полином; сложность.

1. Введение

Пусть q — степень простого числа, $\mathbb{F}_q$ — конечное поле порядка q, n — натуральное число, $n \geqslant 1$, $N = q^n$.

* Работа выполнена при частичной финансовой поддержке РФФИ, проект 16-31-00280, и ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технического комплекса России на 2014-2020 годы (14.579.21.0092), проект № RFMEFI57914X0092.

В статье используются следующие обозначения и соглашения:

- $\mathbb{N} = \{0, 1, \ldots\}$ — множество натуральных чисел;
- $\mathbb{Z}$ — множество целых чисел;
- $\operatorname{avg} S = \frac{1}{|S|} \sum\limits_{x \in S} x$ — среднее арифметическое конечного непустого числового множества S;
- если α — действительное число, то $\lfloor \alpha \rfloor = \max\{i \in \mathbb{Z} \mid i \leqslant \alpha\}$;
- нотация Айверсона [3]: если R — некоторое утверждение, то

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

- целое число k в контексте операций над $\mathbb{F}_q$ равняется $a \in \mathbb{F}_q$, где

$$a = (-1)^{[k<0]} \Big(\underbrace{1 + \ldots + 1}_{|k| \text{ раз}} \Big),$$

  в частности, в $\mathbb{F}_q$ выполняется равенство $q - 1 = -1$;
- будем считать, что для любого $a \in \mathbb{F}_q$ выполняется $a^0 = 1$;
- биномиальный коэффициент $\binom{i}{j}$ при $i < j$ равен 0;
- если M — матрица размера $m \times k$, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant k$, то через $M[i, j]$ обозначим 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;
- $Z(M) = |\{(i, j) \mid M[i, j] = 0, 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant k\}|$ — количество нулевых элементов матрицы M размера $m \times k$;
- $\mathbb{M}_q[m \times k]$ — множество всех матриц размера $m \times k$ с элементами из $\mathbb{F}_q$;
- функцию $f : \mathbb{F}_q^n \to \mathbb{F}_q$ будем отождествлять с вектором ее значений $f \in \mathbb{F}_q^N$, $f = (f_1, \ldots, f_N)$, полагая $f_k = f(\sigma^k)$ для всех k, $1 \leqslant k \leqslant N$, и вместо $f : \mathbb{F}_q^n \to \mathbb{F}_q$ будем писать $f \in \mathbb{F}_q^N$.

2. Матричные формы дискретных функций

Следуя [1], введем следующие определения.

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

$$\Phi_c^v(x_1, \ldots, x_n) = \sum_{\sigma \in \mathbb{F}_q^n} c_t (x_1 + v_1)^{\sigma_1} \ldots (x_n + v_n)^{\sigma_n}, \tag{2.1}$$

где $c \in \mathbb{F}_q^N$, 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 (2.1) задает некоторую функцию $\Phi_c^v \in \mathbb{F}_q^N$. Сложностью полинома Φ_c^v назовем величину $L(\Phi_c^v) = |\{c_t \mid c_t \neq 0,\ 1 \leqslant t \leqslant N\}|$. При этом выполняется $L(\Phi_c^v) = q^n - Z(c)$.

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

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

Понятие поляризованного полинома использовалось в работах [7; 9; 6; 1; 2]. Среди верхних оценок сложности можно отметить следующие. В работе [9] для простого q было показано, что справедливо неравенство

$$L_{\mathcal{P}}(n) \leqslant \left\lfloor \frac{q(q-1)}{q(q-1)+1} q^n \right\rfloor.$$

В [1] была получена параметрическая верхняя оценка для различных классов полиномов.

Определение 2. *Пусть $M \in \mathbb{M}_q[N \times N]$ — квадратная матрица. Пару $\langle M, c\rangle$, где $c \in \mathbb{F}_q^N$, назовем матричной формой.*

Матричная форма задает некоторую функцию $f \in \mathbb{F}_q^N$, определяемую равенством $f = Mc$. Под сложностью матричной формы будем понимать $L(\langle M, c\rangle) = |\{c_t \mid c_t \neq 0,\ 1 \leqslant t \leqslant N\}|$.

Пусть $K \subseteq \mathbb{M}_q[N \times N]$ — некоторое, возможно пустое, множество матриц. Классом матричных форм, порожденных множеством K, назовем множество $\{\langle M, c\rangle \mid M \in K,\ c \in \mathbb{F}_q^N\}$.

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

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

Аналогичным образом вводятся определения сложности семейства функций и класса всех n-местных функций.

Матрицу $M \in \mathbb{M}_q[q \times q]$ назовем верхней треугольной, или просто треугольной, если $M[i,i] \neq 0$ для всех i, $1 \leqslant i \leqslant q$ и $M[i,j] = 0$ для всех i, j, $1 \leqslant j < i \leqslant q$. Множество всех треугольных матриц размера $q \times q$ будем обозначать $\mathbb{T}_q[q]$. Заметим, что так определенные треугольные матрицы являются невырожденными.

Для каждого $a \in \mathbb{F}_q$ определим матрицы $M_a \in \mathbb{T}_q[q]$ следующим образом:

$$M_a[i,j] = \binom{j-1}{i-1} a^{|j-i|}, 1 \leqslant i,j \leqslant q.$$

Множество таких матриц обозначим через $T_{\mathcal{P}} = \{M_a \mid a \in \mathbb{F}_q\}$.

В [1] показано, что сложность функции в классе поляризованных полиномов совпадает со сложностью функции в классе матричных форм, порожденных множеством $T_{\mathcal{P}}$: $L_{\mathcal{P}}(f) = L_{\mathcal{T}_P}(f)$.

Также для каждого $a \in \mathbb{F}_q$ определим матрицы $T_a \in \mathbb{T}_q[p]$:

$$T_a[i,j] = \binom{j-1}{i-1} a^{|j-i|}, 1 \leqslant i,j \leqslant p.$$

Лемма 1. *Для всех $a \in \mathbb{F}_q$ выполняется $T_a^{-1} = T_{-a}$.*

Доказательство. При $1 \leqslant i \leqslant j \leqslant q$ выполняется (см. таблицу 99 в [3])

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

$$= \sum_{k=i}^{j} \binom{k-1}{i-1} (-a)^{k-i} \binom{j-1}{k-1} a^{j-k} = a^{j-i} \binom{j-1}{i-1} \sum_{k=i}^{j} (-1)^{k-i} \binom{j-i}{k-i} =$$

$$= a^{j-i} \binom{j-1}{i-1} (1-1)^{j-i} = [i=j].$$

Так как T_a и T_{-a} являются верхними треугольными матрицами, то $T_a^{-1} = T_{-a}$. □

3. Верхние оценки сложности

В [1] была получена параметрическая верхняя оценка сложности для различных классов кронекеровых форм:

Теорема 1. *Пусть $K \subseteq \mathbb{T}_q[q]$ и для любой функции $f \in \mathbb{F}_q^q$ выполняется $\operatorname{avg}\{Z(M^{-1}f) \mid M \in K\} \geqslant \beta + \delta[f_q = 0]$, для некоторых вещественных $\beta > 0$ и $\delta \geqslant 0$. Тогда $L_{K^{\otimes}}(n) \leqslant \lfloor (1-\alpha)q^n \rfloor$, где $\alpha = \frac{\beta}{q-\delta}$.*

Лемма 2. *При $a \in \mathbb{F}_q$ выполняется $M_a = T_{a^{p^{k-1}}} \otimes \ldots \otimes T_{a^p} \otimes T_a$.*

Доказательство. Представим каждое из чисел $i-1$ и $j-1$ в p-ричной системе счисления:

$$i-1 = (i_k-1)p^{k-1} + \ldots + (i_2-1)p + i_1 - 1,$$
$$j-1 = (j_k-1)p^{k-1} + \ldots + (j_2-1)p + j_1 - 1.$$

С использованием теоремы Люка́ (см., например, упр. 5.61 в [3])

$$\binom{j-1}{i-1} \bmod p = \binom{j_k-1}{i_k-1} \dots \binom{j_1-1}{i_1-1} \bmod p$$

выполним преобразования для элемента матрицы $M_a[i,j]$:

$$M_a[i,j] = \binom{j\ -\ 1}{i\ -\ 1} a^{j-i} = \binom{j_k-1}{i_k-1} \dots \binom{j_1-1}{i_1-1} a^{(j_k-i_k)p^{k-1}} \dots a^{(j_1-i_1)p^{1-1}} =$$

$$= \binom{j_k-1}{i_k-1} a^{(j_k-i_k)p^{k-1}} \dots \binom{j_1-1}{i_1-1} a^{(j_1-i_1)p^{1-1}}.$$

По определению матриц T_a имеем:

$$M_a[i,j] = T_{a^{p^{k-1}}}[i_k, j_k] \dots T_{a^{p^{1-1}}}[i_1, j_1].$$

Из определения кронекерова произведения следует

$$M_a[i,j] = \big(T_{a^{p^{k-1}}} \otimes \dots \otimes T_{a^p} \otimes T_a\big)[i,j].$$

Таким образом, получаем $M_a = T_{a^{p^{k-1}}} \otimes \dots \otimes T_{a^p} \otimes T_a$. □

С использованием лемм 1, 2 получаем $\{M_a | a \in \mathbb{F}_q\} = \{M_a^{-1} | a \in \mathbb{F}_q\}$ и, таким образом, $\operatorname{avg}\{Z(M_a^{-1} f) \mid a \in \mathbb{F}_q\} = \operatorname{avg}\{Z(M_a f) \mid a \in \mathbb{F}_q\}$.

Теорема 2. *Пусть $p \geqslant 3$ — простое, $k \geqslant 1$, $q = p^k$. Тогда*

$$L_{T_{\mathcal{P}}}(n) \leqslant \left\lfloor \frac{q(q-1)-k}{q(q-1)} q^n \right\rfloor.$$

Доказательство. Представим число $i-1$ в p-ричной системе счисления:

$$i - 1 = (i_k - 1)p^{k-1} + \dots + (i_t - 1)p^{t-1} + \dots + (i_1 - 1)p^0.$$

По лемме 2 имеем $M_a[i,j] = T_{a^{p^{k-1}}}[i_k, j_k] \dots T_{a^{p^{1-1}}}[i_1, j_1]$. Рассмотрим некоторые элементы матрицы M_a. Для $M_a[p^k, j]$ имеем:

$$M_a[p^k, j] = T_{a^{p^{k-1}}}[p, j_k] \dots T_{a^{p^{1-1}}}[p, j_1]$$

Поскольку T_a — верхние треугольные матрицы размера $p \times p$, то данное произведение не равно нулю только при $j_s = p$ для всех $s, 1 \leqslant s \leqslant k$, то есть при $j = p^k$. В случае $j = p^k$ произведение равно 1. Таким образом, выполняется $M_a[p^k, j] = [j{=}p^k]$.

Для $M_a[q{-}p^{t-1}, j]$ имеем:

$$M_a[q{-}p^{t-1}, j] = T_{a^{p^{k-1}}}[p, j_k] \dots T_{a^{p^{t-1}}}[p{-}1, j_t] \dots T_a[p, j_1].$$

Множители $T_{a^{p^{s-1}}}[p, j_s]$ равны 1 при $j_s = p$ и 0 иначе. Множитель $T_{a^{p^{t-1}}}[p{-}1, j_t]$ при $j_t = p-1$ равен 1 , при $j_t = p$ равен $-a^{p^{t-1}}$ и равен 0 всех остальных случаях. Таким образом,

$$M_a[q{-}p^{t-1}, j] = [j{=}q{-}p^{t-1}] - a^{p^{t-1}}[j{=}q].$$

Для $M_a[q{-}2p^{t-1}, j]$ имеем:

$$M_a[q{-}2p^{t-1}, j] = T_{a^{p^{k-1}}}[p, j_k]\ldots T_{a^{p^{t-1}}}[p{-}2, j_t]\ldots T_a[p, j_1].$$

Для множителя $T_{a^{p^{t-1}}}[p{-}2, j_t]$ возможны следующие случаи:

$$T_{a^{p^{t-1}}}[p{-}2, j_t] = \begin{cases} 1, & \text{при } j_t = p-2; \\ -2a^{p^{t-1}}, & \text{при } j_t = p-1; \\ a^{2p^{t-1}}, & \text{при } j_t = p; \\ 0, & \text{иначе.} \end{cases}$$

Получаем

$$M_a[q{-}2p^{t-1}, j] = [j{=}q{-}2p^{t-1}] - 2a^{p^{t-1}}[j{=}q{-}p^{t-1}] + a^{2p^{t-1}}[j{=}q].$$

Рассмотрим произвольную функцию $f \in \mathbb{F}_q^q$. Определим множества $K_i = \{a \in \mathbb{F}_q \mid (M_a f)_i = 0\}$, $1 \leqslant i \leqslant q$.

Для функции f возможны следующие случаи.

1. $f_q \neq 0$. Рассмотрим значение $(M_a f)_{q-p^{t-1}} = f_{q-p^{t-1}} - a^{p^{t-1}} f_q$. При выборе $a = \left(f_{q-p^{t-1}}/f_q\right)^{p^{k-t+1}}$ получаем $f_{q-p^{t-1}} - \left(f_{q-p^{t-1}}/f_q\right)^q f_q = 0$. Таким образом, $(M_a f)_{q-p^{t-1}} = 0$ и, следовательно, $|K_{q-p^{t-1}}| \geqslant 1$. Для a возможно k вариантов выбора, поэтому среди чисел $|K_i|$ как минимум k штук больше нуля.

2. $f_q = 0, f_{q-p^{t-1}} \neq 0$. Рассмотрим

$$(M_a f)_{q-2p^{t-1}} = f_{q-2p^{t-1}} - 2a^{p^{t-1}} f_{q-p^{t-1}} + a^{2p^{t-1}} f_q.$$

При выборе $a = \left(f_{q-2p^{t-1}}/2f_{q-p^{t-1}}\right)^{p^{k-t+1}}$ получаем $(M_a f)_{q-2p^{t-1}} = 0$, $|K_{q-2p^{t-1}}| \geqslant 1$. Также имеем $|K_q| = q$.

3. $f_q = f_{q-p^{t-1}} = 0$. Рассмотрим $(M_a f)_{q-p^{t-1}} = f_{q-p^{t-1}} - a^{p^{t-1}} f_q = 0$. В этом случае $|K_{q-p^{t-1}}| = q$, $|K_q| = q$.

Оценим $\operatorname{avg}\{Z(M_a f) \mid a \in \mathbb{F}_q\}$. По определению K_i имеем

$$\operatorname{avg}\{Z(M_a f) \mid a \in \mathbb{F}_q\} = \frac{1}{q}\big(|K_1| + \ldots + |K_q|\big).$$

Тогда $\operatorname{avg}\{Z(M_a f) \mid a \in \mathbb{F}_q\} \geqslant \frac{k}{q} + [f_q = 0]$.

По теореме 1 из [1] $L_{T_\mathcal{P}}(n) \leqslant \lfloor (1-\alpha)q^n \rfloor$. Для данного случая имеем $\alpha = \frac{k/q}{q-1}$, при подстановке получаем

$$L_{T_\mathcal{P}}(n) \leqslant \left\lfloor \frac{q(q-1)-k}{q(q-1)} q^n \right\rfloor. \qquad \square$$

Теорема 3. *Пусть* $q = 2^k$, $k \geqslant 1$. *Тогда*

$$L_{T_{\mathcal{P}}}(n) \leqslant \left\lfloor \frac{q(q-1)}{q(q-1)+k}\, q^n \right\rfloor$$

Доказательство. Представим число $i-1$ в двоичной системе счисления:

$$i-1 = (i_k-1)2^{k-1} + \ldots + (i_t-1)2^{t-1} + \ldots + (i_1-1)2^0.$$

По лемме 2 имеем

$$M_a[i,j] = T_{a^{2^{k-1}}}[i_k, j_k] \ldots T_{a^{2^{1-1}}}[i_1, j_1].$$

По аналогии с доказательством предыдущей теоремы найдем значения следующих элементов матрицы M_a:

$$M_a[2^k, j] = T_{a^{2^{k-1}}}[2, j_k] \ldots T_{a^{2^{1-1}}}[2, j_1] = [j{=}2^k].$$

$$\begin{aligned} M_a[q{-}2^{t-1}, j] &= T_{a^{2^{k-1}}}[2, j_k] \ldots T_{a^{2^{t-1}}}[1, j_t] \ldots T_a[2, j_1] \\ &= [j{=}q{-}2^{t-1}] - a^{2^{t-1}}[j{=}q]. \end{aligned}$$

Рассмотрим произвольную функцию $f \in \mathbb{F}_q^q$. Определим множества $K_i = \{a \in \mathbb{F}_q \mid (M_a f)_i = 0\}$, $1 \leqslant i \leqslant q$.

Для функции f возможны следующие случаи.

1. $f_q \neq 0$. Рассмотрим значение $(M_a f)_{q-2^{t-1}} = f_{q-2^{t-1}} - a^{2^{t-1}} f_q$. При выборе $a = \left(f_{q-2^{t-1}}/f_q\right)^{2^{k-t+1}}$ получаем $f_{q-2^{t-1}} - \left(f_{q-2^{t-1}}/f_q\right)^q f_q = 0$. Таким образом, $(M_a f)_{q-2^{t-1}} = 0$ и $|K_{q-2^{t-1}}| \geqslant 1$. Для a возможно k вариантов выбора, поэтому среди чисел $|K_i|$ как минимум k штук больше нуля.

2. $f_q = 0$. Рассмотрим значение $(M_a f)_q = f_q = 0$. В этом случае $|K_q| = q$.

По определению K_i имеем $\operatorname{avg}\{Z(M_a f) \mid a \in \mathbb{F}_q\} = \frac{1}{q}\big(|K_1|{+}\ldots{+}|K_q|\big)$. Тогда

$$\operatorname{avg}\{Z(M_a f) \mid a \in \mathbb{F}_q\} \geqslant \frac{k}{q}[f_q \neq 0] + [f_q = 0] = \frac{k}{q} + \frac{q-k}{q}[f_q = 0].$$

По теореме 1 из [1] $L_{T_{\mathcal{P}}}(n) \leqslant \lfloor (1-\alpha)q^n \rfloor$. Для данного случая имеем $\alpha = \frac{k/q}{q-(q-k)/q} = \frac{k}{q(q-1)+k}$, при подстановке получаем

$$L_{T_{\mathcal{P}}}(n) \leqslant \left\lfloor \frac{q(q-1)}{q(q-1)+k}\, q^n \right\rfloor. \qquad \square$$

Список литературы

1. 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.

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. Грэхэм Р. Конкретная математика. Основание информатики : пер. с англ. / Р. Грэхэм, Д. Кнут, О. Паташник. – М. : Мир, 1998. – 703 с.
4. Зинченко А. С. Полиномиальные операторные представления функций k-значной логики / А. С. Зинченко, В. И. Пантелеев // Дискретный анализ и исследование операций. Сер. 1. – 2006. – Т. 13, № 3. – С. 13–26.
5. Лидл Р. Конечные поля : пер. с англ. / Р. Лидл, Г. Нидеррайтер. – М. : Мир, 1988. – Т. 1. – 430 с.
6. 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.
7. Перязев Н. А. Сложность булевых функций в классе полиномиальных поляризованных форм / Н. А. Перязев // Алгебра и логика. – 1995. – Т. 34, № 3. – С. 323–326.
8. Селезнева С. Н. О сложности задания k-значных функций обобщенно-поляризованными полиномами / С. Н. Селезнева // Дискрет. математика. – 2009. – Т. 21, № 4. – С. 20–29.
9. Селезнева С. Н. О сложности представления функций многозначных логик поляризованными полиномами / С. Н. Селезнева // Дискрет. математика. – 2002. – Т. 14, № 2. – С. 48–53.

Казимиров Алексей 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: a.kazimirov@gmail.com)

Реймеров Сергей Юрьевич, старший преподаватель, Институт математики, экономики и информатики, Иркутский государственный университет, 664003, Иркутск, ул. К. Маркса, 1, тел.: (3952)242210 (e-mail: sergeyreym@gmail.com)

A. S. Kazimirov, S. Yu. Reymerov

On upper bounds of the complexity of functions over non-prime finite fields in some classes of polarized polynomials

Abstract. Recently, the interest to polynomial representations of functions over finite fields and over finite rings is being increased. Complexity of those representations is widely studied.

This paper introduces new upper bounds on complexity of discrete functions over particular finite fields in class of polarized polynomials. The results are state in the terms of matrix forms. A matrix form is representation of functions vector of values as a product of nonsingular matrix and a vector of coefficients. The complexity of matrix form of a special kind is equal to complexity of polarized polynomial for same function.

A complexity of a matrix form is a number of nonzero coefficients in its vector. Every function can be represented by variety of matrix forms of the same class. A complexity of a function in a class of matrix forms is the minimal complexity of forms in the class representing this function.

Известия Иркутского государственного университета.
2016. Т. 17. Серия «Математика». С. 37–45

This paper introduces new upper bounds on complexity of functions in class of polarized polynomials over fields of orders 2^k and p^k, p is prime and $p \geqslant 3$.

Keywords: finite field, polynomial, polarized polynomial, complexity.

References

1. Baliuk A. S., Yanushkovsky G.V. Upper bounds of the complexity of functions over finite fields in some classes of Kroneker forms (in Russian). *Izvestiya Irkustkogo gosudarstvennogo universiteta. Series Mathematics*, 2015, vol. 14, pp. 3-17.
2. Baliuk A.S., Zinchenko A.S. Lower bound on complexity of functions over finite field of order 4 in class of polarized polynomials (in Russian). *Izvestiya Irkustkogo gosudarstvennogo universiteta. Series Mathematics*, 2016, vol. 16, pp. 19-29.
3. Graham R., Knuth D., Patashnik O. Concrete Mathmatics. A Foundation for Computer Science. Addison Wesley, 1994. 672 p.
4. Zinchenko A.S., Panteleev V.I. Polinomial operator representations of k-valued functions (in Russian). *Diskretnyi Analiz i Issledovanie Operatsii. Series 1*, 2006, vol. 13, no 3, pp. 13–26.
5. Lidl R., Niederreiter H. Finite Fields (Encyclopedia of Mathematics and its Applications). Cambridge University Press, England, 1984. 660 p.
6. 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.
7. Peryazev N.A. The complexity of Boolean functions in the class of polarized polynomial forms (in Russian). *Algebra and Logic*, 1995, vol. 34, no 3, pp. 323–326.
8. Selezneva S.N. On the complexity of representation of k-valued functions by generalised polarised polynomials. *Discrete Mathematics and Applications*, 2010, vol. 19, issue 6, pp. 653–663.
9. Selezneva S.N. On the complexity of representations of functions over multivalued logics by polarized polynomials (in Russian). *Discrete Mathematics and Applications*, 2002, vol. 14, no 2. pp. 48–53.

Kazimirov Alexey Sergeevich, Candidate of Sciences (Physics and Mathematics), Irkutsk State University, 1, K. Marx st., Irkutsk, 664003; tel.: (3952)242210 (e-mail: a.kazimirov@gmail.com).

Reymerov Sergey Yurievich, Senior Lecturer, Irkutsk State University, 1, K. Marx st., Irkutsk, 664003; tel.: (3952)242210
(e-mail: sergeyreym@gmail.com).