Серия «Математика»
2015. Т. 14. С. 3—17

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

ИЗВЕСТИЯ
Иркутского
государственного
университета

УДК 519.715

Верхние оценки сложности функций над конечными полями в некоторых классах кронекеровых форм *

А. С. Балюк
Иркутский государственный университет

Г. В. Янушковский
Высшая школа экономики

Аннотация. 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 конечными полями и их обобщениям: обобщенным и разностным поляризованным полиномам. Полиномы этих классов представляют собой суммы произведений множителей определенного вида. Различие в классах заключается в ограничениях, накладываемых на вид множителей. 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 понимается минимально возможная сложность реализующего ее полинома из этого класса.

Ранее были известны верхние оценки сложности произвольной многоместной функции над простым конечным полем порядка больше двух в классах поляризованных и разностных поляризованных полиномов, а также в классе обобщенно поляризованных полиномов.

Представление n-местной функции над конечным полем порядка q поляризованным полиномом или его обобщением можно рассматривать как кронекерову форму, в том смысле, что векторное представление функции получается как линейное преобразование вектора коэффициентов полинома, при этом матрица линейного преобразования представляет собой кронекерово произведение n невырожденных матриц ранга q. Этот подход позволил усилить верхнюю оценку для случаев поляризованных и разностных поляризованных полиномов и распространить ее на случай произвольного конечного поля нечетного порядка, а верхнюю оценку для случая обобщенно поляризованных полиномов усилить и распространить на случай произвольного конечного поля порядка большего двух.

Ключевые слова: конечное поле, полином, кронекерова форма, сложность.

1. Введение

В настоящей статье используются некоторые понятия из теории конечных полей, которые можно посмотреть в [3].

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

Будем использовать следующие обозначения и соглашения:

- $\#S$ — число элементов конечного множества S;
- $\mathbb{N} = \{0, 1, 2, \dots\}$ — множество натуральных чисел;
- $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ — множество целых чисел;
- $\min S$ обозначает наименьший, а $\max S$ — наибольший элемент конечного непустого множества $S \subset \mathbb{Z}$, будем также считать, что $\min \varnothing = N + 1$ и $\max \varnothing = -1$;
- $\operatorname{avg} S = \frac{1}{\#S} \sum\limits_{x \in S} x$ — среднее арифметическое конечного непустого множества $S \subset \mathbb{Z}$, при этом $\min S \leqslant \operatorname{avg} S \leqslant \max S$;
- если α — действительное число, то $\lfloor \alpha \rfloor = \max\{i \in \mathbb{Z} \mid i \leqslant \alpha\}$;
- нотация Айверсона [1]: 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

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

  в частности, в $\mathbb{F}_q$ выполняется равенство $q - 1 = -1$;
- условимся, что для любого $a \in \mathbb{F}_q$ выполняется $a^0 = 1$;
- 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;
- M^T — транспонированная матрица для матрицы M;
- $Z(M) = \#\{(i, j) \mid M[i, j] = 0,\ 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant k\}$ — 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 $\mathbb{F}_q$;
- $I_m \in \mathbb{M}_q[m \times m]$ — 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 $\mathbb{F}_q$;
- $Z(v) = \#\{i \mid v_i = 0,\ 1 \leqslant i \leqslant m\}$ — количество нулевых элементов вектора $v \in \mathbb{F}_q^m$;

* Работа выполнена при финансовой поддержке РФФИ, грант 13-01-00621.

– 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 $a \in \mathbb{F}_q$, задает линейный порядок на $\mathbb{F}_q$;
– функция, обратная к ℓ, определяется для каждого $k \in \mathbb{Z}$ следующим образом: $\ell^{-1}(k) = \xi^{k-2}[k \not\equiv 0 \pmod q]$;
– 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, $1 \leqslant k \leqslant N$, и вместо $f : \mathbb{F}_q^n \to \mathbb{F}_q$ будем писать $f \in \mathbb{F}_q^N$;
– $\mathbb{F}_q[x]$ — кольцо многочленов над $\mathbb{F}_q$;
– $\deg(h)$ — степень многочлена $h \in \mathbb{F}_q[x]$.

2. Некоторые классы поляризованных полиномов

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

$$\Phi_c^v(x_1, \ldots, x_n) = \sum_{t=1}^N c_t (x_1 + v_1)^{\ell(\sigma_1^t)-1} \ldots (x_n + v_n)^{\ell(\sigma_n^t)-1}, \tag{2.1}$$

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.

Пусть $a \in \mathbb{F}_q$, $h : \mathbb{F}_q \to \mathbb{F}_q$. Положим $\mathrm{d}^a\big(h(x)\big) = h(x) + h(x+a)[a \neq 0]$.

Определение 2. *Пусть $v \in \mathbb{F}_q^n$. Выражение*

$$\Phi_c^v(x_1, \ldots, x_n) = \sum_{t=1}^N c_t \mathrm{d}^{v_1}\Big(x_1^{\ell(\sigma_1^t)-1}\Big) \ldots \mathrm{d}^{v_n}\Big(x_n^{\ell(\sigma_n^t)-1}\Big), \tag{2.2}$$

где $c \in \mathbb{F}_q^N$, назовем разностным поляризованным полиномом переменных $x_1, \ldots, x_n$ над $\mathbb{F}_q$ с поляризацией v и вектором коэффициентов c.

Определение 3. *Пусть $S = \{h_{ik} \in \mathbb{F}_q[x] \mid 1 \leqslant k \leqslant q,\ 1 \leqslant i \leqslant n\}$ — семейство многочленов над $\mathbb{F}_q$, в котором $\deg(h_{ik}) = k-1$. Выражение*

$$\Phi_c^S(x_1, \ldots, x_n) = \sum_{t=1}^N c_t h_{1\ell(\sigma_1^t)}(x_1) \ldots h_{n\ell(\sigma_n^t)}(x_n), \tag{2.3}$$

где $c \in \mathbb{F}_q^N$, назовем обобщенно поляризованным полиномом переменных $x_1, \ldots, x_n$ над $\mathbb{F}_q$ с поляризацией S и вектором коэффициентов c.

Определение 4. *Пусть* $\mathcal{F} \subseteq \{(h_1, \dots, h_q) \mid h_i : \mathbb{F}_q \to \mathbb{F}_q,\ 1 \leqslant i \leqslant q\}$ — *семейство упорядоченных наборов функций одной переменной над* $\mathbb{F}_q$ *и* $S = \{(h_{i1}, \dots, h_{iq}) \mid 1 \leqslant i \leqslant n\}$, $S \subseteq \mathcal{F}$. *Выражение*

$$\Phi_c^S(x_1, \dots, x_n) = \sum_{t=1}^{N} c_t h_{1\ell(\sigma_1^t)}(x_1) \dots h_{n\ell(\sigma_n^t)}(x_n), \tag{2.4}$$

где $c \in \mathbb{F}_q^N$, *назовем полиномом переменных* $x_1, \dots, x_n$ *по семейству* $\mathcal{F}$ *с поляризацией* S *и вектором коэффициентов* c.

Зафиксируем три вида семейств:

$$\mathcal{P} = \{(h_1, \dots, h_q) \mid h_i(x) = (x+a)^{i-1},\ 1 \leqslant i \leqslant q,\ a \in \mathbb{F}_q\},$$
$$\mathcal{D} = \{(h_1, \dots, h_q) \mid h_i(x) = \mathrm{d}^a(x^{i-1}),\ 1 \leqslant i \leqslant q,\ a \in \mathbb{F}_q\},$$
$$\mathcal{G} = \{(h_1, \dots, h_q) \mid h_i \in \mathbb{F}_q[x],\ \deg(h_i) = i-1,\ 1 \leqslant i \leqslant q\}.$$

Легко видеть, что поляризованные полиномы вида (2.1) — это полиномы по семейству $\mathcal{P}$, разностные поляризованные полиномы вида (2.2) — это полиномы по семейству $\mathcal{D}$, обобщенные поляризованные полиномы вида (2.3) — это полиномы по семейству $\mathcal{G}$.

Если переменным $x_1, \dots, x_n$ придавать всевозможные значения из $\mathbb{F}_q$, то полином Φ_c^S из (2.4) задает некоторую функцию $\Phi_c^S \in \mathbb{F}_q^N$. Сложностью полинома назовем величину $L(\Phi_c^S) = \#\{c_t \mid c_t \neq 0,\ 1 \leqslant t \leqslant N\}$. Отметим, что $L(\Phi_c^S) = q^n - Z(c)$.

Сложностью функции $f \in \mathbb{F}_q^N$ в классе полиномов по семейству $\mathcal{F}$ назовем величину $L_{\mathcal{F}}(f) = \min\{L(\Phi_c^S) \mid c \in \mathbb{F}_q^N,\ S \subseteq \mathcal{F},\ \Phi_c^S = f\}$. Отметим, что $L_{\mathcal{F}}(f) = q^n - \max\{Z(c) \mid c \in \mathbb{F}_q^N,\ S \subseteq \mathcal{F},\ \Phi_c^S = f\}$.

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

Понятие поляризованного полинома использовалось в работах [5; 7; 4]. В работе [7] для простого q было показано, что справедливо неравенство $L_{\mathcal{P}}(n) \leqslant \left\lfloor \frac{q(q-1)}{q(q-1)+1} q^n \right\rfloor$. Понятие разностного поляризованного полинома использовалось в работе [2], где для простого $q \geqslant 3$ было показано, что справедливо неравенство $L_{\mathcal{D}}(n) \leqslant \left\lfloor \frac{q(q-1)}{q(q-1)+1} q^n - \frac{(q-1)^{n+1}}{q^{n-1}(q^2-q+1)} \right\rfloor$. В настоящей работе эти оценки будут усилены и распространены на случай произвольного конечного поля нечетной характеристики.

Понятие обобщенного поляризованного полинома использовалось в работе [6], где для простого q было показано, что справедливо неравенство $L_{\mathcal{G}}(n) \leqslant \left\lfloor \frac{q}{q+1} q^n \right\rfloor$. В настоящей работе эта оценка усилена и распространена на случай произвольного конечного поля $\mathbb{F}_q$ при $q \geqslant 3$.

Отметим, что для случая $q = 2$ нижние оценки величин $L_{\mathcal{P}}(n)$ и $L_{\mathcal{G}}(n)$ совпадают сверхними [5].

3. Кронекеровы полиномиальные формы

Определение 5. *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

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

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

$$L_K(F) = \max\{L_K(f) \mid f \in F\}.$$

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

Определение 6. *Пусть $K_1 \subseteq \mathbb{M}_q[N\times N]$, $K_2 \subseteq \mathbb{M}_q[N\times N]$ — множества квадратных матриц. Если существует невырожденная матрица $M^* \in \mathbb{M}_q[N\times N]$ такая, что выполняется $K_2 = \{M^*M \mid M \in K_1\}$, то множества K_1 и K_2, а также классы матричных форм, порожденных этими множествами, назовем эквивалентными.*

Лемма 1. *Пусть $K_1 \subseteq \mathbb{M}_q[N\times N]$ и $K_2 \subseteq \mathbb{M}_q[N\times N]$. Если K_1 и K_2 эквивалентны, то $L_{K_1}(n) = L_{K_2}(n)$.*

Доказательство. Пусть $M^* \in \mathbb{M}_q[N\times N]$ — невырожденная матрица, такая что $K_2 = \{M^*M \mid M \in K_1\}$. Поскольку M^* — невырожденная матрица, то для любой функции $f \in \mathbb{F}_q^N$ найдется $g \in \mathbb{F}_q^N$, такая что $f = M^*g$. При этом,

$$\begin{aligned} L_{K_2}(f) &= \min\{L(\langle M, c\rangle) \mid M \in K_2,\ c \in \mathbb{F}_q^N,\ f = Mc\} \\ &= \min\{L(\langle M^*M, c\rangle) \mid M \in K_1,\ c \in \mathbb{F}_q^N,\ f = M^*Mc\} \\ &= \min\{L(\langle M, c\rangle) \mid M \in K_1,\ c \in \mathbb{F}_q^N,\ g = Mc\} = L_{K_1}(g) \end{aligned}$$

Поскольку $\{f \in \mathbb{F}_q^N \mid f = M^*g,\ g \in \mathbb{F}_q^N\} = \mathbb{F}_q^N$, получаем

$$L_{K_2}(n) = \max\{L_{K_2}(f) \mid f \in \mathbb{F}_q^N\} = \max\{L_{K_1}(g) \mid g \in \mathbb{F}_q^N\} = L_{K_1}(n). \ \square$$

Пусть $K \subseteq \mathbb{M}_q[q\times q]$. Множество $K^{\otimes}$ определим следующим образом:

$$K^{\otimes} = \{M_1 \otimes \cdots \otimes M_n \mid M_i \in K,\ 1 \leqslant i \leqslant n\}.$$

Очевидно, что $K^{\otimes} \subseteq \mathbb{M}_q[N\times N]$.

Матричную форму $\langle M, c\rangle$ назовем кронекеровой, если $M \in \mathbb{M}_q[q\times q]^{\otimes}$.

Определим класс кронекеровых форм, порожденных множеством K как $\{\langle M, c\rangle \mid c \in \mathbb{F}_q^N,\ M \in K^{\otimes}\}$. В соответствии с ранее введенными обозначениями сложность функции $f \in \mathbb{F}_q^N$, множества функций $F \subseteq \mathbb{F}_q^N$ и множества $\mathbb{F}_q^N$ обозначаются $L_{K^{\otimes}}(f)$, $L_{K^{\otimes}}(F)$ и $L_{K^{\otimes}}(n)$ соответственно.

Лемма 2. *Пусть $M_1, \ldots, M_n \in \mathbb{M}_q[q\times q]$. Если $M = M_1 \otimes \cdots \otimes M_n$ — кронекерово произведение матриц, то для всех $v, w \in \mathbb{F}_q^n$ выполняется*

$$M[\ell(v), \ell(w)] = M_1[\ell(v_1), \ell(w_1)] \cdot \ldots \cdot M_n[\ell(v_n), \ell(w_n)].$$

Доказательство. Пусть $v, w \in \mathbb{F}_q^n$, $i_k = \ell(v_k)$, $j_k = \ell(w_k)$, $1 \leqslant k \leqslant n$. Тогда

$$M_1[\ell(v_1), \ell(w_1)] \ldots M_n[\ell(v_n), \ell(w_n)] = M_1[i_1, j_1] \ldots M_n[i_n, j_n]$$
$$= M\Big[1 + \sum_{k=1}^{n}(i_k - 1)q^{n-k}, 1 + \sum_{k=1}^{n}(j_k - 1)q^{n-k}\Big]$$
$$= M\Big[1 + \sum_{k=1}^{n}(\ell(v_k) - 1)\, q^{n-k}, 1 + \sum_{k=1}^{n}(\ell(w_k) - 1)\, q^{n-k}\Big] = M[\ell(v), \ell(w)].\square$$

Лемма 3. *Пусть $c \in \mathbb{F}_q^N$, $\mathcal{F} \subseteq \{(h_1, \ldots, h_q) \mid h_i : \mathbb{F}_q \to \mathbb{F}_q,\ 1 \leqslant i \leqslant q\}$ — семейство наборов функций, $S = \{(h_{k1}, \ldots, h_{kq}) \in \mathcal{F} \mid 1 \leqslant k \leqslant n\} \subseteq \mathcal{F}$, $M = M_1 \otimes \cdots \otimes M_n$ — кронекерово произведение матриц $M_k \in \mathbb{M}_q[q\times q]$, $1 \leqslant k \leqslant n$, элементы которых заданы формулами $M_k[i, j] = h_{kj}\left(\ell^{-1}(i)\right)$. Тогда полином (2.4) задает ту же функцию, что и матричная форма $\langle M, c\rangle$. При этом их сложности равны $L(\Phi_c^S) = L(\langle M, c\rangle)$.*

Доказательство. Сложности равны, поскольку и $L(\Phi_c^S)$, и $L(\langle M, c\rangle)$ определены как $\#\{c_t \mid c_t \neq 0,\ 1 \leqslant t \leqslant N\}$.

Пусть $f = Mc$. Покажем, что для любого i, $1 \leqslant i \leqslant N$, выполняется $f_i = \Phi_c^S(\sigma_1^i, \ldots, \sigma_n^i)$.

$$f_i = \sum_{t=1}^{N} M[i, t]c_t = \sum_{t=1}^{N} c_t M[\ell(\sigma^i), \ell(\sigma^t)] =$$
$$= \sum_{t=1}^{N} c_t M_1[\ell(\sigma_1^i), \ell(\sigma_1^t)] \ldots M_n[\ell(\sigma_n^i), \ell(\sigma_n^t)] =$$
$$= \sum_{t=1}^{N} c_t h_{1\ell(\sigma_1^t)}\left(\ell^{-1}(\ell(\sigma_1^i))\right) \ldots h_{n\ell(\sigma_n^t)}\left(\ell^{-1}(\ell(\sigma_n^i))\right) =$$

$$= \sum_{t=1}^{N} c_t h_{1\ell(\sigma_1^t)}(\sigma_1^i) \dots h_{n\ell(\sigma_n^t)}(\sigma_n^i) = \Phi_c^S(\sigma_1^i, \dots, \sigma_n^i).$$

Это означает, что Φ_c^S и $\langle M, c\rangle$ задают одну и ту же функцию f. □

Лемма 4. *Пусть* $\mathcal{F} \subseteq \{(h_1, \dots, h_q) \mid h_i : \mathbb{F}_q \to \mathbb{F}_q,\ 1 \leqslant i \leqslant q\}$ *— семейство наборов функций,* $K = \{M_{h_1 \dots h_q} \in \mathbb{M}_q[q\times q] \mid (h_1, \dots, h_q) \in \mathcal{F}\}$ *— множество матриц с элементами* $M_{h_1\dots h_q}[i,j] = h_j\left(\ell^{-1}(i)\right)$*. Тогда для любой функции* $f \in \mathbb{F}_q^N$ *выполняется* $L_{\mathcal{F}}(f) = L_{K^\otimes}(f)$*, для любого множества* $F \subseteq \mathbb{F}_q^N$ *выполняется* $L_{\mathcal{F}}(F) = L_{K^\otimes}(F)$*, и* $L_{\mathcal{F}}(n) = L_{K^\otimes}(n)$*.*

Доказательство. Пусть $S = \{(h_{k1}, \dots, h_{kq}) \in \mathcal{F} \mid 1 \leqslant k \leqslant n\} \subseteq \mathcal{F}$. Положим $M = M_{h_{11}\dots h_{1q}} \otimes \dots \otimes M_{h_{n1}\dots h_{nq}}$. Очевидно, что $M \in K^\otimes$. Пусть $c \in \mathbb{F}_q^N$. По лемме 3 матричная форма $\langle M, c\rangle$ задает ту же функцию, что и полином Φ_c^S, причем $L(\Phi_c^S) = L(\langle M, c\rangle)$.

Пусть $M \in K^\otimes$. Тогда найдутся матрицы $M_{h_{11}\dots h_{1q}}, \dots, M_{h_{n1}\dots h_{nq}} \in K$, такие что $M = M_{h_{11}\dots h_{1q}} \otimes \dots \otimes M_{h_{n1}\dots h_{nq}}$. Определим множество наборов функций $S = \{(h_{k1}, \dots, h_{kq}) \in \mathcal{F} \mid 1 \leqslant k \leqslant n\}$. Очевидно, $S \subseteq \mathcal{F}$. Пусть $c \in \mathbb{F}_q^N$. По лемме 3 полином Φ_c^S задает ту же функцию, что и матричная форма $\langle M, c\rangle$, причем $L(\Phi_c^S) = L(\langle M, c\rangle)$.

Таким образом, между кронекеровыми формами, порожденными множеством K, и полиномами по семейству $\mathcal{F}$ существует взаимнооднозначное соответствие, сохраняющее сложность.

Пусть $f \in \mathbb{F}_q^N$ — произвольная функция. Тогда

$$\begin{aligned} L_{\mathcal{F}}(f) &= \min\{L(\Phi_c^S) \mid c \in \mathbb{F}_q^N,\ S \subseteq \mathcal{F},\ \Phi_c^S = f\} \\ &= \min\{L(\langle M, c\rangle) \mid c \in \mathbb{F}_q^N,\ M \in K^\otimes,\ Mc = f\} = L_{K^\otimes}(f). \end{aligned}$$

Пусть $F \subseteq \mathbb{F}_q^N$ — произвольное множество функций. Тогда выполняется $L_{\mathcal{F}}(F) = \max\{L_{\mathcal{F}}(f) \mid f \in F\} = \max\{L_{K^\otimes}(f) \mid f \in F\} = L_{K^\otimes}(F)$, а также $L_{\mathcal{F}}(n) = L_{\mathcal{F}}(\mathbb{F}_q^N) = L_{K^\otimes}(\mathbb{F}_q^N) = L_{K^\otimes}(n)$. □

Лемма 4 определяет взаимнооднозначное соответствие между полиномами по семейству и кронекеровыми формами, поэтому далее будем рассматривать только кронекеровы формы. Так, класс полиномов по семейству $\mathcal{P}$ эквивалентен классу кронекеровых форм, порожденных множеством $K_{\mathcal{P}} = \{M_a \in \mathbb{M}_q[q\times q] \mid M_a[i,j] = \left(\ell^{-1}(i)+a\right)^{j-1},\ a \in \mathbb{F}_q\}$, класс полиномов по семейству $\mathcal{D}$ эквивалентен классу кронекеровых форм, порожденных множеством $K_{\mathcal{D}} = \{M_a \in \mathbb{M}_q[q\times q] \mid a \in \mathbb{F}_q\}$, где $M_a[i,j] = \left(\ell^{-1}(i)\right)^{j-1} + \left(\ell^{-1}(i)+a\right)^{j-1}[a \neq 0]$, класс полиномов по семейству $\mathcal{G}$ эквивалентен классу кронекеровых форм, порожденных множеством $K_{\mathcal{G}} = \{M_{h_1\dots h_q} \in \mathbb{M}_q[q\times q] \mid h_j \in \mathbb{F}_q[x],\ \deg(h_j) = j-1,\ 1 \leqslant j \leqslant q\}$, где $M_{h_1\dots h_q}[i,j] = h_j\left(\ell^{-1}(i)\right)$.

Лемма 5. *Выполняются следующие включения:* $K_{\mathcal{P}} \subseteq K_{\mathcal{G}}$, $K_{\mathcal{D}} \subseteq K_{\mathcal{G}}$.

Доказательство. Пусть $M \in K_{\mathcal{P}}$. Тогда существует $a \in \mathbb{F}_q$, такое что $M[i,j] = \big(\ell^{-1}(i) + a\big)^{j-1}$. Положим $h_j(x) = (x+a)^{j-1}$. Тогда $h_j \in \mathbb{F}_q[x]$ и $\deg(h_j) = j-1$. Поэтому $M[i,j] = h_j\left(\ell^{-1}(i)\right)$, $M \in K_{\mathcal{G}}$ и $K_{\mathcal{P}} \subseteq K_{\mathcal{G}}$.

Случай $K_{\mathcal{D}} \subseteq K_{\mathcal{G}}$ доказывается аналогично. □

4. Треугольные кронекеровы формы

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.

Класс кронекеровых форм, порожденный множеством, состоящим только из треугольных матриц, будем называть треугольным.

Определим матрицу $U \in \mathbb{M}_q[q\times q]$ поэлементно следующим образом: $U[i,j] = [i=1][j=1] - [i=q][j=1] - \xi^{-(i-1)(j-2)}[i\neq 1][j\neq 1]$, и положим $T_{\mathcal{F}} = \{UM \mid M \in K_{\mathcal{F}}\}$, $\mathcal{F} \in \{\mathcal{P}, \mathcal{D}, \mathcal{G}\}$.

Лемма 6. *Множества* $T_{\mathcal{P}}$, $T_{\mathcal{D}}$ *и* $T_{\mathcal{G}}$ *состоят только из треугольных матриц, при этом* $T_{\mathcal{P}} = \{M_a \in \mathbb{T}_q[q] \mid M_a[i,j] = \binom{j-1}{i-1}a^{j-i},\ a \in \mathbb{F}_q\}$, $T_{\mathcal{D}} = \{M_a \in \mathbb{T}_q[q] \mid M_a[i,j] = [i{=}j] + \binom{j-1}{i-1}a^{j-i}[a{\neq}0],\ a \in \mathbb{F}_q\}$, $T_{\mathcal{G}} = \mathbb{T}_q[q]$.

Доказательство. Пусть $M \in K_{\mathcal{G}}$. Тогда существуют $h_1, \ldots, h_q \in \mathbb{F}_q[x]$, такие что $M[i,j] = h_j\left(\ell^{-1}(i)\right)$, причем $\deg(h_j) = j-1$. В силу определения функции ℓ^{-1} имеем: $M[i,j] = h_j(\xi^{i-2})[i\neq 1] + h_j(0)[i=1]$. Для определенности, положим $h_j(x) = c_{j1} + c_{j2}x + \cdots + c_{jj}x^{j-1}$. Рассмотрим элемент произведения матриц $(UM)[i,j]$:

$$
\begin{aligned}
(UM)[i,j] &= \sum_{k=1}^{q} M[k,j]U[i,k] = \sum_{k=1}^{q} \Big(h_j(0)[k=1] + h_j(\xi^{k-2})[k\neq 1]\Big) \\
&\quad \cdot \Big([i=1][k=1] - [i=q][k=1] - \xi^{-(i-1)(k-2)}[i\neq 1][k\neq 1]\Big) \\
&= c_{j1}[i=1] - c_{j1}[i=q] - \sum_{k=2}^{q}\sum_{t=1}^{j} c_{jt}\xi^{(t-1)(k-2)-(i-1)(k-2)}[i\neq 1] \\
&= c_{j1}[i=1] - c_{j1}[i=q] - \sum_{t=1}^{j} c_{jt}[i\neq 1]\sum_{k=0}^{q-2}\xi^{k(t-i)}
\end{aligned}
$$

Поскольку $\sum\limits_{k=0}^{q-2}\xi^{kt} = -[t \equiv 0 \pmod{q-1}]$ (см. упр. 2.50 в [3]), имеем:

$$(UM)[i,j] = c_{j1}[i=1] - c_{j1}[i=q] + \sum_{t=1}^{j} c_{jt}[i \neq 1][t - i \equiv 0 \pmod{q-1}]$$
$$= c_{j1}[i=1] - c_{j1}[i=q] + c_{ji}[2 \leqslant i \leqslant j] + c_{j1}[i=q] = c_{ji}[1 \leqslant i \leqslant j].$$

Таким образом, если $j < i$, то $(UM)[i,j] = 0$, и $(UM)[i,i] = c_{ii} \neq 0$ как старший коэффициент h_i. Значит, $UM \in \mathbb{T}_q[q]$ и $T_{\mathcal{G}} \subseteq \mathbb{T}_q[q]$.

Поскольку матрицы в $\mathbb{T}_q[q]$ — невырожденные, то и матрицы из $K_{\mathcal{G}}$, и матрица U — невырожденные. А из того, что $\#K_{\mathcal{G}} = \#\mathbb{T}_q[q]$ следует, что $T_{\mathcal{G}} = \mathbb{T}_q[q]$.

Так как по лемме 5 выполняются включения $K_{\mathcal{P}} \subseteq K_{\mathcal{G}}$ и $K_{\mathcal{D}} \subseteq K_{\mathcal{G}}$, то также выполняются включения $T_{\mathcal{P}} \subseteq \mathbb{T}_q[q]$ и $T_{\mathcal{D}} \subseteq \mathbb{T}_q[q]$.

Пусть $M \in K_{\mathcal{P}}$. Тогда найдется $a \in \mathbb{F}_q$, такое что $M[i,j] = h_j\left(\ell^{-1}(i)\right)$, где $h_j(x) = (x+a)^{j-1}$. Раскроем скобки: $h_j(x) = \sum_{i=1}^{j} \binom{j-1}{i-1} a^{i-j} x^{i-1}$. Значит, $(UM)[i,j] = \binom{j-1}{i-1} a^{i-j}$.

Пусть $M \in K_{\mathcal{D}}$. Тогда найдется $a \in \mathbb{F}_q$, такое что $M[i,j] = h_j\left(\ell^{-1}(i)\right)$, где $h_j(x) = x^{j-1} + (x+a)^{j-1}[a \neq 0]$. Раскроем скобки:

$$h_j(x) = x^{j-1} + \sum_{i=1}^{j} \tbinom{j-1}{i-1} a^{i-j} x^{i-1}[a{\neq}0] = \sum_{i=1}^{j} \Big([i{=}j] + \tbinom{j-1}{i-1} a^{i-j}[a{\neq}0] \Big) x^{i-1}.$$

Значит, $(UM)[i,j] = [i=j] + \binom{j-1}{i-1} a^{i-j}[a \neq 0]$. □

5. Верхние оценки сложности

Лемма 7. *Пусть $M_1, \ldots, M_n \in \mathbb{M}_q[q{\times}q]$, $M = M_1 \otimes \cdots \otimes M_n$, $v \in \mathbb{F}_q^N$, $w = Mv$. Пусть матрицы V и W размера $q \times \frac{N}{q}$ с элементами из $\mathbb{F}_q$ являются матричными представлениями векторов v и w в том смысле, что $V[i,j] = v_k$ и $W[i,j] = w_k$, где $k = (i-1)\frac{N}{q} + j$.*

Тогда $W = M_1 V (M_2 \otimes \cdots \otimes M_n)^T$.

Доказательство. Введем обозначения:

$$l(k) = 1 + \left\lfloor q\tfrac{k-1}{N} \right\rfloor, \quad r(k) = k - \tfrac{N}{q}\left\lfloor q\tfrac{k-1}{N} \right\rfloor, \quad M' = (M_2 \otimes \cdots \otimes M_n)^T.$$

Заметим, что если $k = (i-1)\frac{N}{q} + j$, то $i = l(k)$, $j = r(k)$, а также, что $M[k,t] = M_1[l(k), l(t)] \cdot M'[r(t), r(k)]$. Выполним преобразования:

$$w_k = \sum_{t=1}^{N} M[k,t] v_t = \sum_{t=1}^{N} M_1[l(k), l(t)] \cdot M'[r(t), r(k)] \cdot V[l(t), r(t)]$$

$$= \sum_{i=1}^{q} M_1[l(k), i] \sum_{j=1}^{N/q} V[i, j] \cdot M'[j, r(k)] = (M_1 V M')[l(k), r(k)].$$

Так как $W[l(k), r(k)] = w_k$, получаем $W = M_1 V (M_2 \otimes \cdots \otimes M_n)^T$. □

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 $\alpha = \frac{\beta}{q-\delta}$.*

Доказательство. Сначала определим ограничения на β и δ. Поскольку для любой $f \in \mathbb{F}_q^q$ выполняется $\operatorname{avg}\{Z(M^{-1}f) \mid M \in K\} \geqslant \beta + \delta[f_q = 0]$, то для любого непустого $F \subseteq \mathbb{F}_q^q$ выполняется

$$\beta + \delta[f_q = 0] \leqslant \frac{1}{\#F} \sum_{f \in F} \frac{1}{\#K} \sum_{M \in K} Z(M^{-1}f) = \frac{1}{\#K} \sum_{M \in K} \frac{1}{\#F} \sum_{f \in F} Z(M^{-1}f).$$

Положим $F = \{f \in \mathbb{F}_q^q \mid f_q = 0\}$ и заметим, что для любой $M \in K$, в силу невырожденности и треугольности, выполняется $\{M^{-1}f \mid f \in \mathbb{F}_q^q\} = \mathbb{F}_q^q$, $\{M^{-1}f \mid f \in F\} = F$ и $\{M^{-1}f \mid f \in \mathbb{F}_q^q \backslash F\} = \mathbb{F}_q^q \backslash F$. Из того, что

$$\sum_{f \in \mathbb{F}_q^q} Z(f) = q^q \text{ и } \sum_{f \in F} Z(f) = q^{q-1}\left(\frac{q-1}{q} + 1\right) = q^{q-1}\left(2 - \frac{1}{q}\right),$$

следует, что $\sum\limits_{f \in \mathbb{F}_q^q \backslash F} Z(f) = \sum\limits_{f \in \mathbb{F}_q^q} Z(f) - \sum\limits_{f \in F} Z(f) = (q^q - q^{q-1})\left(1 - \frac{1}{q}\right)$.

Тогда $\beta + \delta \leqslant \dfrac{1}{\#K} \sum\limits_{M \in K} \dfrac{1}{\#F} \sum\limits_{f \in F} Z(f) = \dfrac{1}{\#K} \sum\limits_{M \in K} \dfrac{q^{q-1}}{q^{q-1}}\left(2 - \dfrac{1}{q}\right) = 2 - \dfrac{1}{q},$

$$\beta \leqslant \frac{1}{\#K} \sum_{M \in K} \frac{1}{\#(\mathbb{F}_q^q \backslash F)} \sum_{f \in \mathbb{F}_q^q \backslash F} Z(f) = \frac{1}{\#K} \sum_{M \in K} \frac{q^q - q^{q-1}}{q^q - q^{q-1}}\left(1 - \frac{1}{q}\right) = 1 - \frac{1}{q}.$$

Таким образом, $0 < \beta \leqslant 1 - \frac{1}{q}$, $0 \leqslant \delta \leqslant 2 - \frac{1}{q} - \beta$. Заметим также, что $0 < \frac{\beta}{1-\delta/q} = \frac{q^2\beta}{q^2 - q\delta} \leqslant \frac{q^2\beta}{(q-1)^2 + q\beta} = 1 - \frac{(q-1)^2 - q(q-1)\beta}{(q-1)^2 + q\beta} \leqslant 1$.

Теорема будет доказана, если для любой функции $f \in \mathbb{F}_q^N$ выполняется $L_{K^\otimes}(f) \leqslant \lfloor (1-\alpha)q^n \rfloor$. Доказывать будем индукцией по n.

Пусть $n = 1$. Тогда $N = q$, $\lfloor (1-\alpha)q^n \rfloor = \left\lfloor q - \frac{\beta}{1-\delta/q} \right\rfloor = \lfloor q - \beta \rfloor$. Пусть теперь $f \in \mathbb{F}_q^q$ — произвольная функция. По условию теоремы $\operatorname{avg}\{Z(M^{-1}f \mid M \in K\} \geqslant \beta$. Тогда $Z(M^{-1}f) \geqslant \beta$ для некоторой матрицы $M \in K$. Положим $c = M^{-1}f$. Тогда $L(\langle M, c\rangle) = q - Z(c) \leqslant q - \beta$. В силу целочисленности $L_{K^\otimes}$ имеем: $L_{K^\otimes}(f) \leqslant \lfloor q - \beta \rfloor = \lfloor (1-\alpha)q^n \rfloor$.

Пусть теперь $n > 1$, и $f \in \mathbb{F}_q^N$ — произвольная функция.

Определим функцию $g \in \mathbb{F}_q^{N/q}$ покоординатно следующим образом: $g_j = f_{j+(q-1)N/q}$, где $1 \leqslant j \leqslant \frac{N}{q}$. По предположению индукции найдутся матрицы $M_2^*, \ldots, M_n^* \in K$, $M' = M_2^* \otimes \cdots \otimes M_n^*$ и вектор $c^* \in \mathbb{F}_q^{N/q}$, такие что $g = M'c^*$ и $L(\langle M', c^* \rangle) \leqslant \lfloor (1-\alpha)q^{n-1} \rfloor$. Тогда $Z(c^*) \geqslant \alpha q^{n-1}$.

Для каждой матрицы $M \in K$ определим вектор $c^M \in \mathbb{F}_q^N$ такой, что $f = (M \otimes M')c^M$. Матрицы из $\mathbb{T}_q[q]$ невырожденные, поэтому можно записать $c^M = (M^{-1} \otimes (M')^{-1})f$. Тогда, по лемме 7, $C_M = M^{-1}V((M')^{-1})^T$, где C_M — матричное представление вектора c^M, а V — матричное представление вектора f. Заметим, что $Z(c^M) = Z(C_M)$.

Положим $W = V((M')^{-1})^T$. В этом случае $V^T = M'W^T$. Поскольку $V^T[j,q] = V[q,j] = f_{j+(q-1)N/q} = g_j$, то в силу того, что $g = M'c^*$, получаем $W^T[j,q] = W[q,j] = c_j^*$, $1 \leqslant j \leqslant \frac{N}{q}$.

Пусть $w^1, \ldots, w^{N/q}$ — столбцы матрицы W. Тогда $w_i^j = W[i,j]$ и $w_q^j = c_j^*$, $1 \leqslant i \leqslant q$, $1 \leqslant j \leqslant \frac{N}{q}$. Таким образом,

$$\operatorname{avg}\{Z(c^M) \mid M \in K\} = \frac{1}{\#K} \sum_{M \in K} Z(C_M) = \frac{1}{\#K} \sum_{M \in K} \sum_{j=1}^{N/q} Z(M^{-1}w^j)$$

$$= \sum_{j=1}^{N/q} \operatorname{avg}\{Z(M^{-1}w^j) \mid M \in K\} \geqslant \sum_{j=1}^{N/q} (\beta + \delta[w_q^j = 0])$$

$$= \beta\tfrac{N}{q} + \delta Z(c^*) \geqslant \beta q^{n-1} + \delta\alpha q^{n-1} = \tfrac{\beta+\delta\alpha}{q} q^n = \tfrac{\beta(q-\delta)+\delta\beta}{q(q-\delta)} q^n = \tfrac{\beta}{q-\delta} q^n = \alpha q^n.$$

Значит, найдется такая матрица $M \in K$, что выполняется $Z(c^M) \geqslant \alpha q^n$. Следовательно, $L_{K^\otimes}(f) \leqslant L(\langle M \otimes M', c^M \rangle) = q^n - Z(c^M) \leqslant (1-\alpha)q^n$ и $L_{K^\otimes}(f) \leqslant \lfloor (1-\alpha)q^n \rfloor$ в силу целочисленности $L_{K^\otimes}(f)$. □

Лемма 8. *Пусть $K \subseteq \mathbb{T}_q[q]$, $\#K = q$ и выполнены два условия:*
1) для любого $a \in \mathbb{F}_q$ найдется $M \in K$, такая что $\frac{M[q-1,q]}{M[q,q]} = a$;
2) для любого $a \in \mathbb{F}_q$ найдется $M \in K$, такая что $\frac{M[q-2,q-1]}{M[q-1,q-1]} = a$.
Тогда $L_{K^\otimes}(n) \leqslant \left\lfloor \frac{q(q-1)-1}{q(q-1)} q^n \right\rfloor$.

Доказательство. Пусть $f \in \mathbb{F}_q^q$ — произвольная функция. Для удобства введем обозначение: $K_i = \{M \in K \mid (M^{-1}f)_i = 0\}$, $1 \leqslant i \leqslant q$. Тогда $\operatorname{avg}\{Z(M^{-1}f) \mid M \in K\} = \frac{1}{q}(\#K_1 + \cdots + \#K_q)$.

Если $f_q \neq 0$, то по условию 1 леммы найдется такая матрица $M \in K$, что $\frac{M[q-1,q]}{M[q,q]} = \frac{f_{q-1}}{f_q}$. Пусть $c = M^{-1}f$. Тогда $f = Mc$, $f_q = M[q,q]c_q$ и $f_{q-1} = M[q-1,q-1]c_{q-1} + M[q-1,q]c_q$, откуда получаем, что $c_q = \frac{f_q}{M[q,q]}$ и $c_{q-1} = \frac{f_{q-1} - M[q-1,q]c_q}{M[q-1,q-1]} = \frac{f_{q-1} - f_q M[q-1,q]/M[q,q]}{M[q-1,q-1]} = \frac{f_{q-1} - f_q f_{q-1}/f_q}{M[q-1,q-1]} = 0$. Значит, $\#K_{q-1} \geqslant 1$ и $\operatorname{avg}\{Z(M^{-1}f) \mid M \in K\} \geqslant \frac{1}{q} = \frac{1}{q} + [f_q = 0]$.

Если $f_q = 0$, но $f_{q-1} \neq 0$, то для любой матрицы $M \in K$, поскольку M^{-1} — треугольная, выполняется $(M^{-1}f)_q = 0$. Значит $\#K_q = q$. С другой стороны, по условию 2 леммы найдется такая матрица $M \in K$, что $\frac{M[q-2,q-1]}{M[q-1,q-1]} = \frac{f_{q-2}}{f_{q-1}}$. Пусть $c = M^{-1}f$, то есть $f = Mc$. Так как $f_q = 0$ и $c_q = 0$, то тогда выполняются равенства $f_{q-1} = M[q-1,q-1]c_{q-1}$ и $f_{q-2} = M[q-2,q-2]c_{q-2} + M[q-2,q-1]c_{q-1}$. Значит, $c_{q-1} = \frac{f_{q-1}}{M[q-1,q-1]}$ и $c_{q-2} = \frac{f_{q-2} - f_{q-1}M[q-2,q-1]/M[q-1,q-1]}{M[q-2,q-2]} = \frac{f_{q-2} - f_{q-1}f_{q-2}/f_{q-1}}{M[q-2,q-2]} = 0$. Таким образом, $\#K_{q-2} \geqslant 1$ и $\operatorname{avg}\{Z(M^{-1}f) \mid M \in K\} \geqslant \frac{1}{q} + 1 = \frac{1}{q} + [f_q = 0]$.

Если же $f_q = f_{q-1} = 0$, то для любой матрицы $M \in K$, в силу треугольности матрицы M^{-1}, выполняется $(M^{-1}f)_q = (M^{-1}f)_{q-1} = 0$. Значит $\#K_{q-1} = \#K_q = q$ и $\operatorname{avg}\{Z(M^{-1}f) \mid M \in K\} \geqslant 2 > \frac{1}{q} + [f_q = 0]$.

Таким образом, для любой одноместной функции $f \in \mathbb{F}_q^q$ выполняется $\operatorname{avg}\{Z(M^{-1}f) \mid M \in K\} \geqslant \frac{1}{q} + [f_q = 0]$. Тогда по теореме 1 $L_{K^\otimes}(n) \leqslant \lfloor (1-\alpha)q^n \rfloor$, где $\alpha = \frac{1/q}{q-1}$, то есть $L_{K^\otimes}(n) \leqslant \left\lfloor \frac{q(q-1)-1}{q(q-1)} q^n \right\rfloor$. □

Теорема 2. *Если q нечетно, то*

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

Доказательство. Из лемм 1 и 4 следует, что $L_{\mathcal{P}}(n) = L_{K_{\mathcal{P}}^\otimes}(n) = L_{T_{\mathcal{P}}^\otimes}(n)$.

По лемме 6 для любого $a \in \mathbb{F}_q$ матрица M_a, элементы которой вычисляются по формулам $M_a[i,j] = \binom{j-1}{i-1} a^{j-i}$, принадлежит множеству $T_{\mathcal{P}}$. Тогда $M_a[i,i] = 1$ и $M_a[i-1,i] = (i-1)a$, $2 \leqslant i \leqslant q$.

Так как элемент 2 обратим в поле нечетной характеристики, то для произвольного $a \in \mathbb{F}_q$ выполняется $\frac{M_{-a/2}[q-2,q-1]}{M_{-a/2}[q-1,q-1]} = (q-2)(-a/2) = a$ и $\frac{M_{-a}[q-1,q]}{M_{-a}[q,q]} = (q-1)(-a) = a$. Тогда выполнены условия леммы 8, из которой и следует верхняя оценка. □

Теорема 3. *Если q нечетно, то*

$$L_{\mathcal{D}}(n) = L_{K_{\mathcal{D}}^\otimes}(n) = L_{T_{\mathcal{D}}^\otimes}(n) \leqslant \left\lfloor \frac{q(q-1)-1}{q(q-1)} q^n \right\rfloor.$$

Доказательство. Из лемм 1 и 4 следует, что $L_{\mathcal{D}}(n) = L_{K_{\mathcal{D}}^\otimes}(n) = L_{T_{\mathcal{D}}^\otimes}(n)$.

По лемме 6 для любого элемента $a \in \mathbb{F}_q$ матрица M_a, в которой $M_a[i,j] = [i=j] + \binom{j-1}{i-1} a^{j-i}[a \neq 0]$, принадлежит множеству $T_{\mathcal{D}}$. Тогда $M_a[i,i] = 1 + [a \neq 0]$ и $M_a[i-1,i] = (i-1)a$, $2 \leqslant i \leqslant q$.

Так как $2 \neq 0$ в поле нечетной характеристики, то для любого $a \in \mathbb{F}_q$ выполняется $\frac{M_{-a}[q-2,q-1]}{M_{-a}[q-1,q-1]} = \frac{(q-2)(-a)}{1+[a\neq 0]} = a$ и $\frac{M_{-2a}[q-1,q]}{M_{-2a}[q,q]} = \frac{(q-1)(-2a)}{1+[a\neq 0]} = a$. Тогда применима лемма 8, из которой и следует верхняя оценка. □

Теорема 4. $L_{\mathcal{G}}(n) = L_{K_{\mathcal{G}}^{\otimes}}(n) = L_{\mathbb{T}_q[q]^{\otimes}}(n) \leqslant \left\lfloor \dfrac{q+(q-1)^{-1}-1}{q+(q-1)^{-1}} q^n \right\rfloor$.

Доказательство. В силу лемм 1 и 4, $L_{\mathcal{G}}(n) = L_{K_{\mathcal{G}}^{\otimes}}(n) = L_{\mathbb{T}_q[q]^{\otimes}}(n)$.

Пусть множества F_k, $0 \leqslant k \leqslant q$, определены следующим образом: $F_k = \{f \in \mathbb{F}_q^q \mid f_i = 0,\ i \geqslant k{+}1\}$. Тогда множества $F_0, F_1 \backslash F_0, \ldots, F_q \backslash F_{q-1}$ попарно не пересекаются и $\mathbb{T}_q[q] = F_0 \cup F_1 \backslash F_0 \cup \cdots \cup F_q \backslash F_{q-1}$, при этом $\#F_0 = 1$, и $\#(F_k \backslash F_{k-1}) = q^k - q^{k-1}$, $1 \leqslant k \leqslant q$.

Пусть $f \in \mathbb{F}_q^q$ — произвольная функция. Так как матрица, обратная к треугольной, сама является треугольной, то $\{M^{-1} \mid M \in \mathbb{T}_q[q]\} = \mathbb{T}_q[q]$. Значит, $\operatorname{avg}\{Z(M^{-1}f) \mid M \in \mathbb{T}_q[q]\} = \operatorname{avg}\{Z(Mf) \mid M \in \mathbb{T}_q[q]\}$. Для удобства введем обозначение: $K_i = \{M \in \mathbb{T}_q[q] \mid (Mf)_i = 0\}$, $1 \leqslant i \leqslant q$. Тогда $\operatorname{avg}\{Z(Mf) \mid M \in \mathbb{T}_q[q]\} = \frac{1}{\#\mathbb{T}_q[q]}(\#K_1 + \cdots + \#K_q)$.

Положим $\beta = \delta = \frac{q-1}{q}$.

Если $f \in F_0$, то $Mf \in F_0$ для любой $M \in \mathbb{T}_q[q]$. Следовательно, $\#K_i = \#\mathbb{T}_q[q]$ при $1 \leqslant i \leqslant q$, и $\operatorname{avg}\{Z(Mf) \mid M \in \mathbb{T}_q[q]\} = q \geqslant \beta + \delta[f_q{=}0]$.

Теперь рассмотрим случай, когда $f \in F_k \setminus F_{k-1}$ для некоторого k. Для всех $M \in \mathbb{T}_q[q]$ выполняется $(Mf)_i = 0$, если $i \geqslant k+1$. Значит, $\#K_i = \#\mathbb{T}_q[q]$ при $i \geqslant k+1$. Поскольку $(Mf)_k = M[k,k]f_k \neq 0$ для любой $M \in \mathbb{T}_q[q]$, то $\#K_k = 0$.

Пусть теперь $1 \leqslant i < k$. Тогда $f_k \neq 0$ и для любой $M \in \mathbb{T}_q[q]$ выполняется $(Mf)_i = M[i,k]f_k + \sum_{j=i}^{k-1} M[i,j]f_j$. Подсчитаем количество матриц $M \in \mathbb{T}_q[q]$, для которых $(Mf)_i = 0$, то есть $M[i,k] = -\frac{1}{f_k}\sum_{j=i}^{k-1} M[i,j]f_j$. Поскольку значение $M[i,k]$ среди всех матриц $M \in \mathbb{T}_q[q]$ равновероятно принимает любое значение из $\mathbb{F}_q$, но только одно из них обеспечивает выполнение равенства $(Mf)_i = 0$, то, очевидно, $\#K_i = \frac{1}{q}\#\mathbb{T}_q[q]$.

Таким образом,

$$\operatorname{avg}\{Z(Mf) \mid M \in \mathbb{T}_q[q]\} = \frac{1}{\#\mathbb{T}_q[q]}\left(\sum_{i=1}^{k-1}\frac{1}{q}\#\mathbb{T}_q[q] + \sum_{i=k+1}^{q}\#\mathbb{T}_q[q]\right)$$
$$= \frac{k-1}{q} + q - k = \frac{q-1}{q} + \frac{q-1}{q}(q-k) \geqslant \frac{q-1}{q} + \frac{q-1}{q}[k \leqslant q-1].$$

Так как $f_q = 0$ при $k \leqslant q-1$, то $\operatorname{avg}\{Z(Mf) \mid M \in \mathbb{T}_q[q]\} \geqslant \beta + \delta[f_q = 0]$.

Таким образом, для любой функции $f \in \mathbb{F}_q^q$ справедливо неравенство $\operatorname{avg}\{Z(M^{-1}f) \mid M \in \mathbb{T}_q[q]\} \geqslant \beta + \delta[f_q = 0]$. Тогда по теореме 1, полагая $\alpha = \frac{(q-1)/q}{q-(q-1)/q} = \frac{1}{q+(q-1)^{-1}}$, получаем $L_{\mathbb{T}_q[q]^{\otimes}}(n) \leqslant \left\lfloor \frac{q-1+(q-1)^{-1}}{q+(q-1)^{-1}} q^n \right\rfloor$. □

Список литературы

1. Грэхэм Р. Конкретная математика. Основание информатики : пер. с англ. / Р. Грэхэм, Д. Кнут, О. Паташник. – М. : Мир, 1998. – 703 с.
2. Зинченко А. С. Полиномиальные операторные представления функций k-значной логики / А. С. Зинченко, В. И. Пантелеев // Дискрет. анализ и исслед. операций. Сер. 1. – 2006. – Т. 13, № 3. – С. 13–26.
3. Лидл Р. Конечные поля : пер. с англ. / Р. Лидл, Г. Нидеррайтер. – М. : Мир, 1988. – Т. 1. – 430 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 задания k-значных функций обобщенно-поляризованными полиномами / С. Н. Селезнева // Дискрет. математика. – 2009. – Т. 21, № 4. – С. 20–29.
7. 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, Иркутск, ул. К. Маркса, 1, тел.: (3952)242210 (e-mail: sacha@hotmail.ru)

Янушковский Григорий Викторович, студент, факультет компьютерных наук, Высшая школа экономики, 101000, Москва, ул. Мясницкая, 20, тел.: (495)5310031 (e-mail: grisha_ya@inbox.ru)

A. S. Baliuk, G. V. Yanushkovsky

Upper Bounds of the Complexity of Functions over Finite Fields in Some Classes of Kroneker Forms

Abstract. Polynomial representations of Boolean functions have been studied well enough. 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 fields and their generalizations: differentially and generically polarized polynomials. Such a polynomial is a finite sum of products. The difference between classes of polynomials is in constraints, applied to the 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.

Известия Иркутского государственного университета.
2015. Т. 14. Серия «Математика». С. 3–17

Previously, the upper bounds were known for arbitrary n-variable function over primary finite field of order, greater than 2, for the classes of polarized and differentially polarized polynomials, as well as for the class of generically polarized polynomials.

A representation of an n-ary function over finite field of order q by a polarized polynomial or its generalization can be considered as a Kroneker form. This means, that the function, considered as a vector in appropriate linear space, is computed by a linear transformation of a vector of coefficients of the polynomial, where the matrix of this linear transformation is a Kroneker product of n nonsingular matrices with rank q. This approach helped us to improve the upper bound for polarized and differentially polarized polynomials for the case of any finite field of odd order, and to improve the upper bound for generically polarized polynomials for the case of any finite field of order, greater than 2.

Keywords: finite field, polynomial, Kroneker form, complexity.

References

1. Graham R., Knuth D., Patashnik O. Concrete Mathmatics. A Foundation for Computer Science. Addison Wesley, 1994. 672 p.
2. Zinchenko A.S., Panteleev V.I. Polinomialnie operatornie predstavlenija funkcij k-znachnoj logiki (in Russain). *Diskretnyi Analiz i Issledovanie Operatsii. Series 1.* – 2006, vol. 13, no 3, pp. 13-26.
3. Lidl R., Niederreiter H. Finite Fields (Encyclopedia of Mathematics and its Applications). Cambridge University Press, England, 1984. 660 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. 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.
6. 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.
7. 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.

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).

Yanushkovskiy Grigoriy Victorovich, Student, Higher School of Economics, 20, Myasnitskaya st., Moscow, 101000, tel.: (495)5310031 (e-mail: grisha_ya@inbox.ru).