Серия «Математика»
2014. Т. 10. С. 3—12

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

ИЗВЕСТИЯ
Иркутского
государственного
университета

УДК 519.715

О верхней оценке сложности задания квазиполиномами функций над конечными полями *

А. С. Балюк
Иркутский государственный университет

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

В данной работе исследуется сложность задания функций квазиполиномами над конечными полями. Квазиполином можно рассматривать как полином многих переменных, в котором вхождения $x_i^0, \ldots, x_i^{k-1}$ одной из переменных заменены на функции из некоторого множества $\{g_0(x_i), \ldots, g_{k-1}(x_i)\}$ линейно независимых одноместных функций.

Под сложностью полинома над конечным полем обычно понимают количество слагаемых в нем, число вхождений переменных или степень. В случае квазиполиномов напрямую можно оценивать количество слагаемых, число вхождений переменных и степень требуют обобщения. В статье в качестве сложности квазиполинома исследуется количество слагаемых в нем. Для случая квазиполиномов по модулю простого k ранее была известна верхняя оценка такой сложности, а именно, сложность задания квазиполиномами n-местной функции над конечным полем простого порядка k не превосходит величины $\frac{k}{k+1}k^n$.

В работе получена верхняя оценка сложности представления квазиполиномами функций над произвольным конечным полем порядка q, которая при $q \geqslant 3$ усиливает ранее известную верхнюю оценку, полученную для случая квазиполиномов по модулю простого числа. А именно, если $q = k^n$, где k — простое, а $n \geqslant 1$, для любой n-местной функции над конечным полем порядка q сложность её задания квазиполиномами ограничена сверху величиной $\frac{q-1}{q-q^{1-q}}q^n$.

Ключевые слова: конечное поле, полином, квазиполином, сложность.

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

Введение

В настоящей работе используются следующие обозначения:

- $|A|$ или $\#A$ — число элементов конечного множества A;
- $\mathbb{N} = \{0, 1, 2, \dots\}$ — множество натуральных чисел;
- $\mathbb{F}_q$ — конечное поле порядка q, ноль и единицу поля $\mathbb{F}_q$ будем обозначать 0 и 1 соответственно;
- $\mathbb{F}_q^N$ — N-мерное векторное пространство над $\mathbb{F}_q$;
- элемент (вектор) пространтва $v \in \mathbb{F}_q^N$ будем отождествлять с упорядоченным набором $(v_0, v_1, \dots, v_{N-1})$;
- тензорное произведение $w = u \otimes v$ векторов $u \in \mathbb{F}_q^{N_1}$ и $v \in \mathbb{F}_q^{N_2}$ — это вектор $w \in \mathbb{F}_q^{N_1+N_2}$, такой что $w_{iN_1+j} = u_i v_j$, где $0 \leqslant i < N_1$, $0 \leqslant j < N_2$;
- $\|v\| = \#\{i \mid v_i \neq 0,\ 0 \leqslant i < N\}$ — вес $v \in \mathbb{F}_q^N$;
- если $V \subseteq \mathbb{F}_q^N$, то $\|V\| = \min\limits_{v \in V} \|v\|$;
- $\mathbb{M}_q[m \times n]$ — множество всех матриц размера $m \times n$ над полем $\mathbb{F}_q$;
- если $A \in \mathbb{M}[m \times n]$, то A^j — j-й столбец, а A_{ij} — ij-й элемент матрицы A, $0 \leqslant i < m$, $0 \leqslant j < n$;
- $\mathbb{M}_q[n]$ — множество всех невырожденных матриц размера $n \times n$ над полем $\mathbb{F}_q$;
- $A \otimes B$ — тензорное (кронекерово) произведение матриц A и B;
- $A^{\otimes n} = \underbrace{A \otimes \dots \otimes A}_{n \text{ раз}}$ — тензорная степень матрицы A, $A^{\otimes 0} = (1)$;
- $\mathbb{M}_q^{\otimes n} = \{M_1 \otimes M_2 \otimes \dots \otimes M_n \mid M_i \in \mathbb{M}_q[q],\ 1 \leqslant i \leqslant n\}$;
- если $v \in \mathbb{F}_q^N$, $N = q^n$, то $[v] = \{Mv \mid M \in \mathbb{M}_q^{\otimes n}\}$.

Определение 1. *Отображение $f : \mathbb{F}_q^n \to \mathbb{F}_q$ будем называть n-местной функцией над конечным полем $\mathbb{F}_q$.*

Пусть α_0, α_1, …, α_{q-1} суть все элементы поля $\mathbb{F}_q$, упорядоченные некоторым образом, при этом $\alpha_0 = 0$, а $\alpha_1 = 1$. На основе этого порядка образуем лексикографический порядок упорядоченных наборов из $\mathbb{F}_q$, на который в дальнейшем будем ссылаться как на *лексикографическое упорядочение.*

Пусть $v^0, v^1, \dots, v^{N-1}$ — лексикографическое упорядочение всех наборов длины n с элементами из $\mathbb{F}_q$, здесь $v^i \in \mathbb{F}_q^n$, $0 \leqslant i < N$, $N = q^n$. Тогда функцию $f : \mathbb{F}_q^n \to \mathbb{F}_q$ можно однозначно задать вектором $u \in \mathbb{F}_q^N$, так что $u_i = f(v^i)$.

Пусть $p(x_1, \dots, x_n) \in \mathbb{F}[x_1, \dots, x_n]$ — полином от многих переменных над полем F_q, такой, что его степень по каждой переменной не превосходит $q - 1$. Этот полином определяет n-местную функцию над F_q, которая может быть задана некоторым вектором $w \in \mathbb{F}_q^N$, где $N = q^n$.

С другой стороны, каждый такой полином можно однозначно задать вектором $v \in F_q^N$, где $N = q^n$ следующим образом:

$$p(x_1, x_2, \ldots, x_n) = \sum_{i=0}^{N-1} v_i x_1^{d_{i1}} x_2^{d_{i2}} \ldots x_n^{d_{in}}, \quad d_{ij} = \left\lfloor \frac{i}{q^{j-1}} \right\rfloor \bmod q, \quad (0.1)$$

где $1 \leqslant j \leqslant n$.

Положим $0^0 = 1$, где 0 — это ноль, а 1 — единица поля $\mathbb{F}_q$. Тогда выражение $x_j^{d_{ij}}$ из (0.1) можно рассматривать как функцию $x_j^{d_{ij}} : F_q^1 \to F_q$, заданную вектором $(\alpha_0^{d_{ij}}, \alpha_1^{d_{ij}}, \ldots, \alpha_{q-1}^{d_{ij}})$, где $\alpha_0, \alpha_1, \ldots, \alpha_{q-1}$ — лексикографическое упорядочение элементов из $\mathbb{F}_q$. Выражение $x_1^{d_{i1}} x_2^{d_{i2}} \ldots x_n^{d_{in}}$ из (0.1) можно рассматривать как n-местную функцию над $\mathbb{F}_q$, заданную некоторым вектором u. Если $u^1, \ldots, u^n$ — векторы, задающие одноместные функции $x_1^{d_{i1}}, \ldots, x_n^{d_{in}}$ соответственно, то вектор $u = u^1 \otimes \cdots \otimes u^n$ задает n-местную функцию $x_1^{d_{i1}} \ldots x_n^{d_{in}}$.

Пусть $U \in \mathbb{M}[q \times q]$ такая, что

$$U_{kj} = \alpha_k^j, \quad 0 \leqslant k < q,\ 0 \leqslant j < q, \quad (0.2)$$

$w \in \mathbb{F}_q^N$ — вектор, задающий полином $p(x_1, \ldots, x_n)$, рассматриваемый в виде n-местной функции. Тогда (0.1) можно записать в матричном виде:

$$w = U^{\otimes n} v. \quad (0.3)$$

В дальнейшем будем отождествлять полином $p(x_1, \ldots, x_n)$ с вектором v, а функцию, задаваемую этим полиномом, с вектором w из (0.3).

Определитель матрицы U — это определитель Вандермонда, поэтому

$$\det U = \prod_{0 \leqslant i < j < q} (\alpha_i - \alpha_j) \neq 0,$$

поскольку $\alpha_i - \alpha_j \neq 0$, а поле, как известно, не содержит делителей нуля.

Из этого следует в частности, что $U^{\otimes n}$ — невырожденная матрица, и каждая n-местная функция w единственным образом задается полиномом. При этом функция $(0, \ldots, 0)$ задается полиномом $(0, \ldots, 0)$.

Аналогично работе [3] введем понятие квазиполинома. Пусть v^0, v^1, $\ldots$, $v^{q-1} \in \mathbb{F}_q^q$ — линейно независимые векторы. Следуя [3], множество $\delta = \{v^0, v^1, \ldots, v^{q-1}\}$ будем называть *поляризующим*. Множеству δ поставим в соответствие невырожденную матрицу $D \in \mathbb{M}_q[q]$, с элементами $D_{ij} = v_i^j$. Эту матрицу будем называть *поляризацией*. Таким образом, поляризация — это матрица $D \in \mathbb{M}_q[q]$.

Определение 2. *Квазиполиномом с поляризацией $D \in M_q[q]$ по выделенной переменной x_i для функции $f : \mathbb{F}_q^n \to F_q$, заданной вектором*

$w \in \mathbb{F}_q^N$, где $N = q^n$, будем называть вектор $v \in \mathbb{F}_q^N$, такой что выполняется

$$w = (U^{\otimes(i-1)} \otimes D \otimes U^{\otimes(n-i)})v.$$

Поскольку U и D — невырожденные, для каждой функции существует единственный квазиполином с заданной поляризацией D по выделенной переменной x_i.

Сложность полиномиальных представлений k-значных функций исследовалась, например, в работах [1; 4]. В качестве меры сложности использовалась длина (количество слагаемых) и обобщение понятия степени полинома.

Следуя [3], *длиной* квазиполинома v будем называть его вес $\|v\|$.

Определение 3. Минимальной длиной *функции $f : \mathbb{F}_q^n \to \mathbb{F}_q$, заданной вектором $w \in \mathbb{F}_q^N$, в классе квазиполиномов назовем величину*

$$l(w) = \min\{\|v\| \mid w = (U^{\otimes(i-1)} \otimes D \otimes U^{\otimes(n-i)})v, D \in \mathbb{M}_q[q]\}.$$

В работе [3] приводится верхняя оценка величины $l(w)$, а именно, для любой функции $f : \mathbb{F}_q^n \to \mathbb{F}_q$, заданной вектором $w \in \mathbb{F}_q^N$, где $N = q^n$, q — простое,

$$l(w) \leqslant \frac{q}{q+1} q^n.$$

В данной работе эта оценка усилена с помощью обобщения метода получения верхних оценок сложности из работы [2].

1. Основной результат

Для доказательства основного результата нам потребуется вспомогательная лемма.

Лемма. *Пусть*

$$Z \geqslant \sum_{t=1}^{k} tT_t, \quad T_t \geqslant c_t T_0 - \sum_{i=t+1}^{k} c_t T_i, \quad c_t = \frac{k-1}{k^t - 1},\ T_t \geqslant 0,\ 1 \leqslant t \leqslant k.$$

Тогда

$$Z \geqslant \left(\frac{k}{k-1} - \frac{k}{k^k - 1} \right) T_0.$$

Доказательство. Будем доказывать неравенство индуктивно следующей цепочкой: $Z \geqslant Z_1 \geqslant \cdots \geqslant Z_k \geqslant Z_{k+1}$, где Z_p будем искать в форме $Z_p = b_p T_0 + \sum_{t=p}^{k} a_{p,t} T_t$, где $1 \leqslant p \leqslant k+1$.

При $p = 1$, положив $a_{1,t} = t$, $b_1 = 0$ имеем требуемое.

Предположим, что при некотором p, $1 \leqslant p \leqslant k$, выполняется

$$Z \geqslant Z_1 \geqslant \cdots \geqslant Z_p, \quad Z_p = b_p T_0 + \sum_{t=p}^{k} a_{p,t} T_t.$$

Тогда

$$Z_p = b_p T_0 + a_{p,p} T_p + \sum_{t=p+1}^{k} a_{p,t} T_t$$

Если $a_{p,p} \geqslant 0$, то

$$Z_p \geqslant b_p T_0 + \sum_{t=p+1}^{k} a_{p,t} T_t + a_{p,p} \left(c_p T_0 - \sum_{t=p+1}^{k} c_p T_t \right)$$

$$= (b_p + a_{p,p} c_p)\, T_0 + \sum_{t=p+1}^{k} (a_{p,t} - a_{p,p} c_p)\, T_t$$

Если $a_{p,p} \geqslant 0$, то положив $a_{p+1,t} = a_{p,t} - a_{p,p} c_p$ и $b_{p+1} = b_p + a_{p,p} c_p$, получим $Z_p \geqslant Z_{p+1}$, где $Z_{p+1} = b_{p+1} T_0 + \sum_{t=p+1}^{k} a_{p+1,t} T_t$. Рассмотрим рекуррентное соотношение $a_{p+1,t} = a_{p,t} - a_{p,p} c_p$, где $p \geqslant 1$, $t \geqslant 1$, с начальными условиями $a_{1,t} = t$.

$$a_{p+1,t+1} - a_{p+1,t} = (a_{p,t+1} - a_{p,p} c_p) - (a_{p,t} - a_{p,p} c_p)$$
$$= a_{p,t+1} - a_{p,t} = \cdots = a_{1,t+1} - a_{1,t} = (t+1) - t = 1,$$
$$a_{p,t} = a_{p,t-1} + 1 = a_{p,t-2} + 2 = \cdots = a_{p,1} + (t-1),$$

Положим $d_p = a_{p,1}$, $d_1 = 1$. Тогда $a_{p,t} = d_p + (t-1)$. Получается, что $a_{p,p} \geqslant 0$ тогда и только тогда, когда $d_p \geqslant 1 - p$.

$$d_{p+1} = d_p - a_{p,p} c_p = d_p - (d_p + p - 1) c_p$$
$$= (1 - c_p) d_p - (p-1) c_p$$
$$= (1 - \frac{k-1}{k^p - 1}) d_p - (p-1) \frac{k-1}{k^p - 1} = k \frac{k^{p-1} - 1}{k^p - 1} d_p - (p-1) \frac{k-1}{k^p - 1}$$

Пусть $g_p = (k^{p-1} - 1) d_p$, тогда $g_1 = 0$ и

$$g_{p+1} = k g_p - (p-1)(k-1) = k(k g_{p-1} - (p-2)(k-1)) - (p-1)(k-1)$$
$$= k^2 g_{p-1} - k(p-2)(k-1) - (p-1)(k-1) = \ldots$$
$$= k^{p-1} g_1 - (k-1) \sum_{i=1}^{p-1} i k^{p-1-i} = -(k-1) \sum_{i=1}^{p-1} i k^{p-1-i}.$$

$$\sum_{i=1}^{p-1} i k^{p-1-i} = \frac{k^p - 1 - pk + p}{(k-1)^2},$$

так как при $p = 1$ выражение обращается ноль и

$$k\frac{k^p - 1 - pk + p}{(k-1)^2} + p = \frac{k^{p+1} - 1 - (p+1)k + (p+1)}{(k-1)^2}.$$

Таким образом,

$$g_p = \frac{(p-1)(k-1) - (k^{p-1} - 1)}{k-1},$$
$$d_p = \frac{p-1}{k^{p-1}-1} - \frac{1}{k-1}.$$

Имеем, $d_1 = 1$, $d_2 = 0$, $d_p \geqslant -\frac{1}{k-1} > -1$ при $p \geqslant 3$. Таким образом $d_p \geqslant 1 - p$, а следовательно $a_{p,p} \geqslant 0$ и $Z_p \geqslant Z_{p+1}$, при $1 \leqslant p \leqslant k$.

Рассмотрим рекуррентное соотношение $b_{p+1} = b_p + a_{p,p}c_p$. Поскольку $a_{p,p}c_p = d_p - d_{p+1}$, имеем

$$b_{p+1} = b_p + d_p - d_{p+1} = b_{p-1} + d_{p-1} - d_p + d_p - d_{p+1}$$
$$= b_{p-1} + d_{p-1} - d_{p+1} = \cdots = b_1 + d_1 - d_{p+1} = 1 - d_{p+1},$$
$$Z_{k+1} = \sum_{t=k+1}^{k} a_{k+1,t}T_t + b_{k+1}T_0 = b_{k+1}T_0,$$
$$b_{k+1} = 1 - d_{k+1} = 1 - \left(\frac{k}{k^k-1} - \frac{1}{k-1}\right) = \frac{k}{k-1} - \frac{k}{k^k-1},$$

что завершает доказательство леммы. □

Теорема. *Пусть $\mathbb{F}_q$ — конечное поле порядка q, $N = q^n$, где $n \in \mathbb{N}$. Тогда для любого $w \in \mathbb{F}_q^N$*

$$l(w) \leqslant \frac{q-1}{q-q^{1-q}}q^n.$$

Доказательство. Пусть $U \in \mathbb{M}_q[q\times q]$ удовлетворяет (0.2). Пусть $v \in \mathbb{F}_q^N$ такой, что $w = U^{\otimes n}v$.

Рассмотрим матрицу $B \in \mathbb{M}_q[q\times\frac{N}{q}]$, такую что $B_{ij} = v_{iN/q+j}$, $0 \leqslant i < q$, $0 \leqslant j < \frac{N}{q}$.

Пусть B^j — это j-й столбец матрицы B.

Пусть $I = \{0, \ldots, \frac{N}{q} - 1\}$,

Индуктивно определим непересекающиеся множества $I_t \subseteq I$ и векторы $u^t \in \mathbb{F}_q^q$, $0 \leqslant t \leqslant q$, следующим образом.

В качестве u^0 возьмем вектор, все элементы которого равны нулю, $I_0 = \{j \in I \mid B^j = u^0\}$.

Пусть уже определены множества I_i и векторы u^i, $1 \leqslant i < t$. Для каждого $u \in \mathbb{F}_q^q$ определим множество

$$I_t(u) = \{j \in I \setminus (I_0 \cup \cdots \cup I_{t-1}) \mid B^j = c_t u + \sum_{i=0}^{t-1} c_i u^i, c \in \mathbb{F}_q^{t+1}\}.$$

Это множество будет пусто, если u — линейно зависит от $u^1, \ldots, u^{t-1}$. Кроме того, если c — ненулевой элемент поля $\mathbb{F}_q^q$, то $I_t(u) = I_t(cu)$. Поэтому среди всех множеств вида $I_t(u)$ существует не более $\frac{q^{q-t+1}}{q-1}$ различных непустых множеств. Возьмем $u^t \in \mathbb{F}_q^q$ такое, что для любого $u \in \mathbb{F}_q^q$ выполняется $|I_t(u^t)| \geqslant |I_t(u)|$. Положим $I_t = I_t(u^t)$. Тогда

$$|I_t| \geqslant \frac{q-1}{q^{q-t+1}-1}(|I| - |I_0| - \ldots - |I_{t-1}|). \tag{1.1}$$

Пусть $E \in \mathbb{M}_q[q]$ — единичная матрица, а E^i — её i-й столбец. По построению, векторы $u^1, \ldots, u^q$ линейно независимы. Поэтому существует матрица $H \in \mathbb{M}_q[q]$, такая что $u^i = HE^i$.

Пусть $C = H^{-1}B$.

По построению, если $j \in I_{t+1}$, то C_{tj} — ненулевой элемент поля $\mathbb{F}_q$, а если $i > t$, то C_{ij} равен нулю.

Рассмотрим верхнюю треугольную матрицу $G \in \mathbb{M}_q[q]$ с единицами на главной диагонали. Элементы матрицы G_{it} и множества $J_{it}(c)$, $0 \leqslant i < t < q$, $c \in \mathbb{F}_q$, определим индуктивно следующим образом.

Положим $J_{01}(c) = \{j \in I_2 \mid C_{0j} + cC_{1j} = 0\}$. В качестве G_{01} возьмем такой элемент поля $\mathbb{F}_q$, чтобы для любого $c \in \mathbb{F}_q$ выполнялось $|J_{01}(G_{01})| \geqslant |J_{01}(c)|$.

Пусть для всех $c \in \mathbb{F}_q$, уже определены множества $J_{ik}(c)$ и элементы матрицы G_{ik}, $0 \leqslant i < k < t$. Для каждого $c \in \mathbb{F}_q$ и каждого i, $0 \leqslant i < t$, определим множество

$$J_{it}(c) = \{j \in I_{t+1} \mid \sum_{k=0}^{t-1} G_{ik}C_{kj} + cC_{tj} = 0\}.$$

В качестве G_{it} возьмем такой элемент поля $\mathbb{F}_q$, чтобы для любого $c \in \mathbb{F}_q$ выполнялось $|J_{it}(G_{it})| \geqslant |J_{it}(c)|$. Поскольку количество различных множеств вида $J_{it}(c)$ равняется q, то $|J_{it}(G_{it})| \geqslant \frac{1}{q}|I_{t+1}|$.

Пусть $A = GC$. Подсчитаем количество Z_A нулевых элементов в матрице A. Если $i > t$ и $j \in I_{t+1}$, то

$$A_{ij} = \sum_{k=0}^{q-1} G_{ik}C_{kj} = 0,$$

поскольку $G_{ik} = 0$ при $k < i$, а $C_{kj} = 0$ при $k > t$. Если $i < t$ и $j \in J_{it}(G_{it})$, то

$$A_{ij} = \sum_{k=0}^{q-1} G_{ik}C_{kj} = \sum_{k=0}^{t} G_{ik}C_{kj} + \sum_{k=t+0}^{q-1} G_{ik}C_{kj} = 0,$$

поскольку $\sum_{k=0}^{t} G_{ik}C_{kj} = 0$ из-за $j \in J_{it}(G_{it})$, а $C_{kj} = 0$ при $k > t$ из-за $j \in I_{t+1}$.

Таким образом,

$$Z_A \geqslant \sum_{t=0}^{q}(q-t)|I_t| + \sum_{t=1}^{q-1}\sum_{i=0}^{t-1}|J_{it}(G_{it})| \geqslant \sum_{t=0}^{q}(q-t)|I_t| + \sum_{t=1}^{q-1}\sum_{i=0}^{t-1}\frac{1}{q}|I_{t+1}|.$$

Упростим выражение.

$$\sum_{t=0}^{q}(q-t)|I_t| + \sum_{t=1}^{q-1}\sum_{i=0}^{t-1}\frac{1}{q}|I_{t+1}| = \sum_{t=0}^{q}(q-t)|I_t| + \sum_{t=2}^{q}\frac{t-1}{q}|I_t|$$

$$= q|I_0| + \sum_{t=1}^{q}\left(q-t+\frac{t-1}{q}\right)|I_t| = q|I_0| + \frac{q-1}{q}\sum_{t=1}^{q}(q-t+1)|I_t|$$

$$= q|I_0| + \frac{q-1}{q}\sum_{t=1}^{q}t|I_{q-t+1}| = q|I_0| + \frac{q-1}{q}\sum_{t=1}^{q}tT_t$$

где $T_t = |I_{q-t+1}|$.

Перепишем (1.1) в виде

$$T_t \geqslant c_tT_0 - \sum_{i=t+1}^{q}c_tT_i, \quad \text{где } c_t = \frac{q-1}{q^t-1},\ T_0 = |I| - |I_0|$$

Используя лемму и равенство $|I| = q^{n-1}$, получим

$$Z_A \geqslant q|I_0| + \frac{q-1}{q}\left(\frac{q}{q-1} - \frac{q}{q^q-1}\right)(|I| - |I_0|)$$

$$= \left(1 - \frac{q-1}{q^q-1}\right)|I| + \left(q-1+\frac{q-1}{q^q-1}\right)|I_0|$$

$$\geqslant \left(1-\frac{q-1}{q^q-1}\right)q^{n-1} = \frac{q^{q-1}-1}{q^q-1}q^n.$$

Положим $D = UHG^{-1}$. Матрица D невырожденная в силу невырожденности матриц U, H и G. Зададим вектор $u \in \mathbb{F}_q^N$ следующим образом: $u_{iN/q+j} = A_{ij}$. Тогда

$$(D \otimes U^{\otimes(n-1)})u = U^{\otimes n}\left((HG^{-1}) \otimes E^{\otimes(n-1)}\right)u.$$

Для всех неотрицательных целых j и t, меньших N, введем обозначение $e_{jt} = \begin{cases}1, & \text{если } j = t;\\ 0, & \text{если } j \neq t.\end{cases}$.

Пусть $F = HG^{-1}$. Рассмотрим элемент вектора

$$(F \otimes E^{\otimes(n-1)})u$$

с индексом $iN/q + j$. Его значение можно вычислить следующим образом

$$\sum_{k=0}^{q-1}\sum_{t=0}^{N/q-1} F_{ik}e_{jt}u_{kN/q+t} = \sum_{k=0}^{q-1} F_{ik}u_{kN/q+j} = \sum_{k=0}^{q-1} F_{ik}A_{kj} = B_{ij}.$$

Значит, $(F \otimes E^{\otimes(n-1)})u = v$, а $(D \otimes U^{\otimes(n-1)})u = U^{\otimes n}v = w$. Таким образом, u — квазиполином для w и

$$l(w) \leqslant \|u\| = q^n - Z_A \leqslant q^n - \frac{q^{q-1}-1}{q^q-1}q^n = \frac{q^q - q^{q-1}}{q^q-1}q^n = \frac{q-1}{q-q^{1-q}}q^n.$$

Теорема доказана. □

Список литературы

1. Пантелеев В. И. Полиномиальные разложения k-значных функций по операторам дифференцирования и нормализации / В. И. Пантелеев // Изв. высш. учеб. заведений. Математика. – 1998. – № 1. – С. 17–21.
2. Перязев Н. А. Сложность булевых функций в классе полиномиальных поляризованных форм / Н. А. Перязев // Алгебра и логика. – 1995. – Т. 34. – №. 3. – С. 323–326.
3. Селезнева С. Н. О сложности k-значных функций в одном классе полиномов / С. Н. Селезнева // Проблемы теоретической кибернетики : материалы XVI Междунар. конф. (Нижний Новгород, 20–25 июня 2011 г.). – Н. Новгород : Изд-во Нижегор. ун-та, 2011. – С. 430–434.
4. 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, Иркутский государственный университет, 664003, Иркутск, ул. К. Маркса, 1, тел.: (3952)240435 (e-mail: sacha@hotmail.ru)

A. S. Baliuk

On Upper Bound of the Complexity of Quasi Polynomial Representations of Functions over Finite Fields

Abstract. Representations of functions over finite fields, including polynomial representations, are being actively investigated. The complexity of such representations is one of main directions of research.

This paper is about quasi polynomial complexity of functions over finite fields. Quasi polynomial can be considered as a regular polynomial with the following transformation: every occurence $x_i^0, \ldots, x_i^{k-1}$ of selected variable x_i is replaced by a function from a set $\{g_0(x_i), \ldots, g_{k-1}(x_i)\}$ of linearly independent unary functions.

The number of terms, the number of occurences of variables, or the degree of a polynomial are usually used as a measure of complexity. In the case of quasi polynomials one can use the number of terms as a natural measure of complexity, while further generalization are required for the number of occurences of variables and the degree of a polynomial. In this paper the number of terms is used as a measure of complexity. Previously, the upper bound of such a complexity was known for polynomials over finite fields of prime order. Namely, the quasi polynomial complexity of n-ary function over finite field of prime order k is at most $\frac{k}{k+1}k^n$.

In this paper an upper bound for the quasi polynomial complexity of functions over finite fields of arbitrary order q has been obtained, which significantly improves previously known upper bound for modulo prime quasi polynomials, if $q \geqslant 3$. Namely, the quasi polynomial complexity of any n-ary function over finite field of order q is at most $\frac{q-1}{q-q^{1-q}}q^n$.

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

References

1. Panteleev V. I. Polynomial representations of k-valued functions by derivative and normalization operators (in Russian). *Russian Mathematics (Iz. VUZ). Izvestiya VUZ. Matematika.*, 1998, no. 1, pp. 17–21.
2. 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.
3. Selezneva S. N. On the complexity of k-valued functions in one class of polynomials (in Russian). *Problemy Theoreticheskoi Kibernetiki*, Nizhny Novgorod, University of Nizhny Novgorod, 2011, pp. 430–434.
4. 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), Associate Professor, Irkutsk State University, 1, K. Marx st., Irkutsk, 664003, tel.: (3952)240435 (e-mail: `sacha@hotmail.ru`)