Оценка максимального числа ненулевых коэффициентов многочлена функции при действии группы перестановок на таблицу значений функции

Гремяков А.О.[1]

Для коэффициентов полиномов функций над конечными полями F_q рассматривается задача отыскания нижней оценки на максимум минимума числа ненулевых коэффициентов в полиноме, где максимум берется по всем функциям, а минимум — по их преобразованиям, соответствующим различным заданиям поля. При этом возможно рассматривать различные типы таких преобразований.

В работе получена оценка $L(q) \geq q - 2$ на максимум минимума числа ненулевых коэффициентов в полиноме для определенного типа преобразований, оставляющих нулевой элемент поля на месте.

Ключевые слова: коэффициенты полиномов, булевы функции, полином булевой функции, таблица значений функции, sagemath.

Основные определения, обозначения и утверждения

$\mathbb{F}_q$ — конечное поле из $q = p^n$ элементов, где p — простое.

f — функция над конечным полем $\mathbb{F}_q$, f: $\mathbb{F}_q \to \mathbb{F}_q$.

Пусть дана исходная таблица значений функции.

[1] *Гремяков Александр Олегович* — аспирант каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ имени М.В.Ломоносова, e-mail: sandshats@gmail.com.

Gremyakov Alexander Olegovich — graduate student, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intelligent Systems.

x	$f(x)$
x_0	$f(x_0)$
$\vdots$	$\vdots$
x_{q-1}	$f(x_{q-1})$

Рассмотрим биективное преобразование σ, после которого таблица преобразуется следующим образом:

x	$f(x)$
$\sigma(x_0)$	$\sigma(f(x_0))$
$\vdots$	$\vdots$
$\sigma(x_{q-1})$	$\sigma(f(x_{q-1}))$

$pol_f(x_1, \ldots, x_m) = \sum\limits_{0 \le j_k < q-1} c_{j_1,\ldots,j_m} x_1^{j_1} \cdot \ldots \cdot x_m^{j_m}$ —- полином функции f в поле, $c_{j_1,\ldots,j_m} \in \mathbb{F}_q$. Заметим, что количество таких полиномов совпадает с количеством функций и равенство полиномов означает равенство функций, из чего следует, что каждая функция задается ровно одним полиномом.

Если функция зависит только от одной переменной, будем применять следующее обозначение.

Через v_f обозначим вектор значений функции. А через v_{pol_f} — вектор коэффициентов полинома функции.

Рассмотрим в поле $\mathbb{F}_7$ функцию от одной переменной с таблицей

x	$f(x)$
0	1
3	1
2	1
6	1
4	2
5	1
1	2

Тогда $v_f = (1,1,1,1,2,1,2)$, $pol_f(x) = 1+4x+2x^2+5x^3+4x^4+2x^5+5x^6$, а $v_{pol_f} = (1,4,2,5,4,2,5)$.

S_q — множество перестановок элементов поля (симметрическая группа из q элементов), а s_q — множество перестановок элементов поля, переводящие базис в базис.

Зафиксируем S как группу перестановок элементов поля сохраняющих ноль на месте.

Через $zero_{pol}(f)$ обозначим число нулевых коэффициентов функции f в ее представлении полиномом $pol_f(x_1, \ldots, x_m)$, а число ненулевых коэффициентов обозначим через $nonzero_{pol}(f)$

Обозначим за $T^{\sigma}(f)$ множество функций, которые получаются из функции f над конечным полем $\mathbb{F}_q$, с помощью многократного применения преобразования σ и через $T^{S}(f)$ множество функций, которые получаются из функции f над конечным полем $\mathbb{F}_q$, с помощью преобразований из множества S. Соответственно $T_{pol}(f)$ множество полиномов функций, которые получаются из функции f над конечным полем $\mathbb{F}_q$.

Через $P_q(m)$ обозначим множество всех функций от m переменных над над конечным полем $\mathbb{F}_q$.

Через $l_m(f)$ обозначим минимум числа ненулевых коэффициентов в полиноме от m переменных, представляющим функцию над конечным полем $\mathbb{F}_q$, где минимум берется по классу функции, или иначе говоря её орбите на множестве всех функций под действием группы преобразований.

Через $L_m(q)$ обозначим максимум минимума числа ненулевых коэффициентов в полиноме от m переменных, представляющим функцию над конечным полем $\mathbb{F}_q$, где максимум берется по всем функциям, а минимум по их преобразованиям, соответствующим различным заданиям поля.

Условие задачи в введенных обозначениях можно записать следующим образом:

$$L = L_1(p^n) = \max_{g \in P_q} \min_{f \in T(g)} nonzero\big(pol_f(x)\big), \text{ где } P_q = P_q(1)$$

.

$$l_m(f) = l(f) = \min_{f \in T(f)} nonzero\big(pol_f(x)\big).$$

В указанных обозначениях можно сформулировать полученный результат: $L(q) \geq$ q-2 при действии на множество функций рассматриваемых биективных преобразований, оставляющих ноль на месте.

Быстрое вычисление полинома функции

Покажем, как коэффициенты полинома функции выражаются через значения некоторой матрицы и вектора значений функции одной переменной. Результат утверждения 2 можно найти в [1].

Индикаторные функции

$$j_{\delta_i}(x) = \begin{cases} 1, & x = \delta_i \\ 0, & x \neq \delta_i \end{cases}.$$

Индикаторные функции представляются такими полиномами

$$j_{\delta_i}(x) = 1 - (x - \delta_i)^{q-1}.$$

Доказательство. Каждая функция в поле представляется только одним полиномом. Очевидно индикаторные функции представляются таким полиномом. □

Если $v_{p_f} = (c_0, c_1, \cdots, c_{q-1})$, то эти коэффициенты выражаются через транспонированный вектор значений функции следующим образом:

$$\begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{q-3} \\ c_{q-2} \\ c_{q-1} \end{pmatrix} = - \begin{pmatrix} -1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1^{q-2} & a_2^{q-2} & \cdots & a_{q-2}^{q-2} & a_{q-1}^{q-2} \\ 0 & 1^{q-3} & a_2^{q-3} & \cdots & a_{q-2}^{q-3} & a_{q-1}^{q-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1^2 & a_2^2 & \cdots & a_{q-2}^2 & a_{q-1}^2 \\ 0 & 1 & a_2 & \cdots & a_{q-2} & a_{q-1} \\ 1 & 1 & 1 & \cdots & 1 & 1 \end{pmatrix} \begin{pmatrix} f(0) \\ f(1) \\ f(a_2) \\ \vdots \\ f(a_{q-3}) \\ f(a_{q-2}) \\ f(a_{q-1}) \end{pmatrix}.$$

Доказательство. Очевидно, что функцию можно представить следующим образом $f(x) = \sum_{\sigma \in \mathbf{F}_\sigma} j_\sigma(x) \cdot f(\sigma)$. После подстановки вместо индикаторных функций их представление полиномом после простых преобразований выражения получаем

$$f(x) = \sum_{\sigma\in\mathbf{F}_\sigma} j_\sigma(x)\cdot f(\sigma) = \sum_{\sigma\in\mathbf{F}_\sigma}\Big(1-(x-\sigma)^{q-1}\Big)f(\sigma) =$$
$$\sum_{\sigma\in\mathbf{F}_\sigma}\Big(1-\frac{(x-\sigma)^q}{x-\sigma}\Big)f(\sigma) = \sum_{\sigma\in\mathbf{F}_\sigma}\Big(1-\frac{x^q-\sigma^q}{x-\sigma}\Big)f(\sigma) =$$
$$\sum_{\sigma\in\mathbf{F}_\sigma}\Big(1-(x^{q-1}+x^{q-2}\sigma+\cdots+x\sigma^{q-2}+\sigma^{q-1})\Big)f(\sigma) =$$
$$-\sum_{i=0}^{k-2}x^{q-1-i}\Big(\sum_{\sigma\in\mathbf{F}_\sigma}\sigma^i f(\sigma)\Big)+f(0).$$

Отсюда получаем представление коэффициентов полинома из утверждения, так как последнее выражение можно представить с помощью матрицы.

□

Матрицу из утверждения обозначим

$$M_q(0,1,a_2,\cdots,a_{q-2},a_{q-1}) = -\begin{pmatrix} -1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1^{q-2} & a_2^{q-2} & \cdots & a_{q-2}^{q-2} & a_{q-1}^{q-2} \\ 0 & 1^{q-3} & a_2^{q-3} & \cdots & a_{q-2}^{q-3} & a_{q-1}^{q-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1^2 & a_2^2 & \cdots & a_{q-2}^2 & a_{q-1}^2 \\ 0 & 1 & a_2 & \cdots & a_{q-2} & a_{q-1} \\ 1 & 1 & 1 & \cdots & 1 & 1 \end{pmatrix}.$$

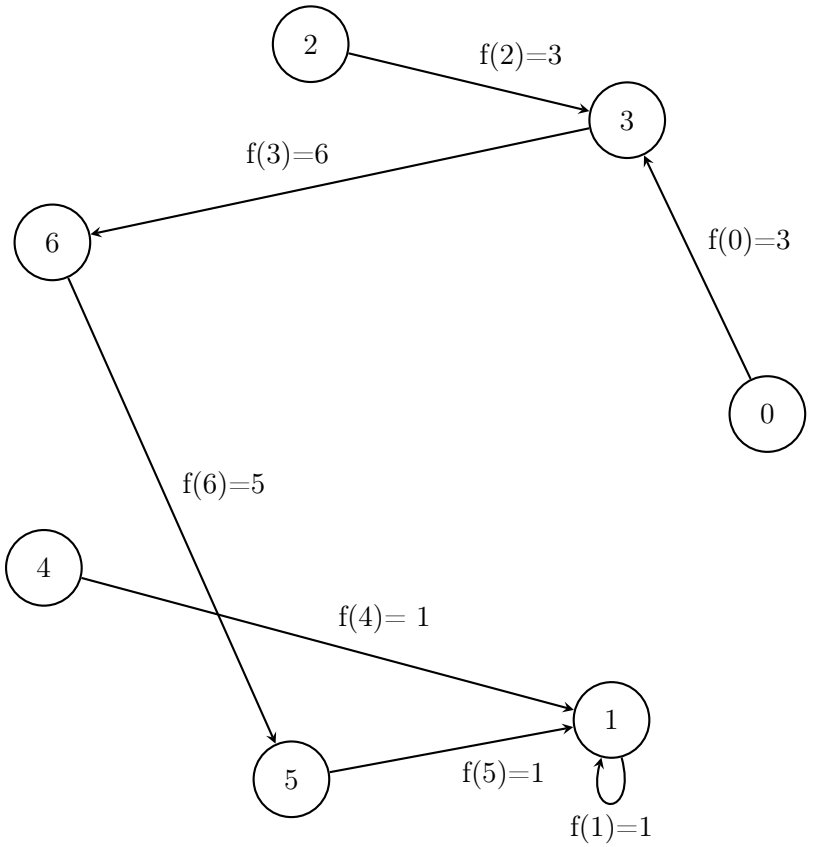
Разбиение на классы и количество классов (орбит) на множестве функций при действии на них рассматриваемыми преобразованиями

Функции из P_q можно представлять в виде ориентированных графов: вершины графов будут соответствовать значениям аргументов функций, а стрелки графа, выходящие из этих вершин будут направлены в вершины, приписанное значение аргумента которым соответствует значению функции на аргументе, значению которого соответствует вершина, откуда направлена стрелка.

Рассмотрим функцию f(x) в P_7, которая задаётся следующей таблицей:

x	$f(x)$
0	3
3	6
2	3
6	5
4	1
5	1
1	1

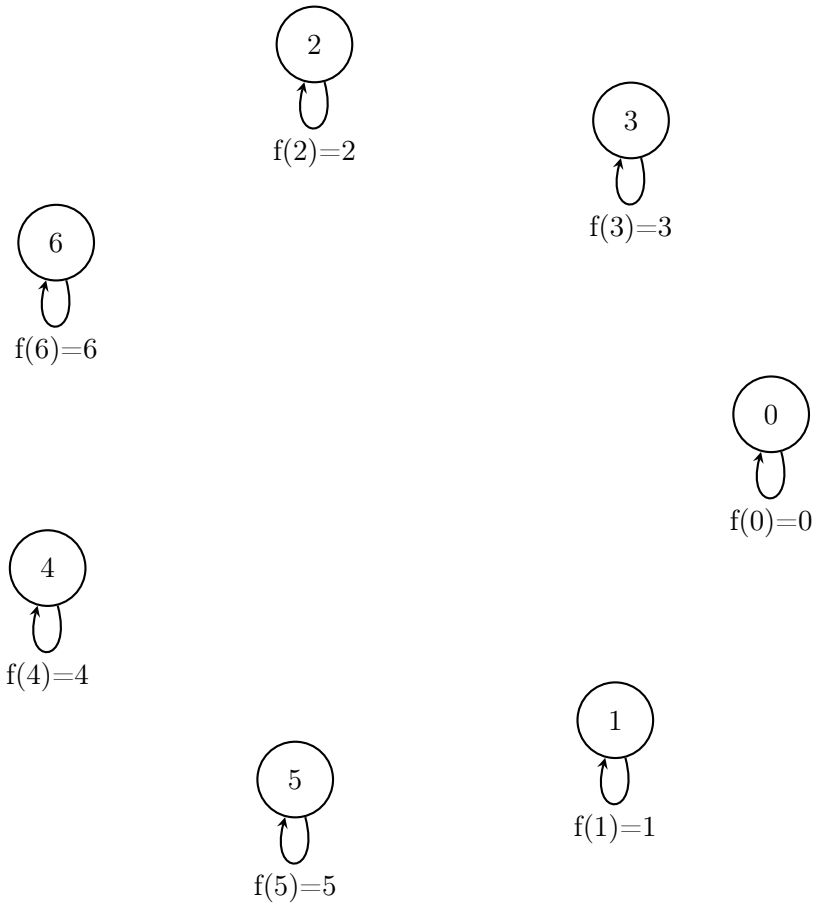
Тогда она задаётся следующим графом.



В следующих разделах не будем подписывать ребра ориентированного графа.

Рассмотрим функцию f(x) = x. Тогда очевидно, её вершины будут переходить сами в себя.

Нарисуем граф такой функции в P_7

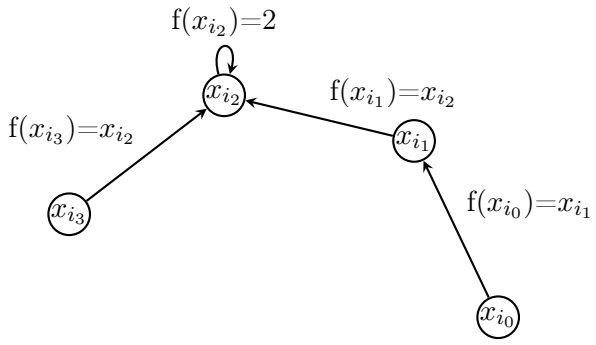


Следующее утверждение описывает разбиение функций из P_q на классы при действии преобразования рассматриваемого типа.

Граф функции не меняется под действием преобразования рассматриваемого типа.

Доказательство. Рассмотрим связный подграф какой-то функции из P_q, покажем, что он не изменится под действием преобразования.

Но очевидно, что если x_{i_j} перейдут в $\sigma(x_{i_j})$, то у рёбер и вершин ориентированного графа просто будет меняться обозначения, а сам граф будет переходить в изоморфный граф.



□

Таким образом, преобразования рассматриваемого типа сохраняют ориентированные графы функций: отображения из q точек на самих себя. Это и даёт разбиение функций на классы.

Количество таких классов описывается последовательностью A001372 на OIES.

Приведем некоторые значения этой последовательности: 1, 1, 3, 7, 19, 47, 130, 343, 951, 2615, 7318, 20491, 57903, 163898, 466199, 1328993, 3799624, 10884049, 31241170, 89814958, 258604642, 745568756, 2152118306, 6218869389, 17988233052, 52078309200, ...

Соответственно те члены, которые соответствуют $q = p^n$, будут описывать количество классов, на которые функции рабиваются под действием такого преобразования, в P_q.

Примеры, перебор $\mathbb{F}_q$ для $q \in \{2, 3, 7\}$ для преобразований рассматриваемого типа

Рассмотрим вырожденный случай: q = 2. Матрица для вычисления полиномов в поле $\mathbb{F}_2$

$$M_2(0,1) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

В этом случае всего 4 функции и только три класса.
$l(f) = 2$ в таком классе:
Это единственное q, для которого L(q) = q.
$l(f) = 1$ в таком классе:
Это функция f(x) = x.

И остаётся класс, где содержатся константы 0 и 1. Где l(f) = 0, из-за того, что там содержится 0.

Матрица для вычисления полиномов в поле $\mathbb{F}_3$

$$M_3((0,2,1)) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 2 & 2 & 2 \end{pmatrix}$$

Вектора, в классах которых l(f) = q-1 (l(f)=2):

Вектора, где l(f) = q-2 (l(f) = 1):

Рассмотрим класс с вектором $v_{f_0}(x) = (2,\ 1,\ 1)$

$$v_{y_0}(x) = (0,\ 0,\ 2)\,, v_{pol_{y_0}}(x) = (0,\ 1,\ 1)$$
$$v_{y_1}(x) = (1,\ 2,\ 2)\,, v_{pol_{y_1}}(x) = (1,\ 0,\ 1)$$
$$v_{y_2}(x) = (0,\ 1,\ 0)\,, v_{pol_{y_2}}(x) = (0,\ 1,\ 2)$$
$$v_{y_3}(x) = (2,\ 1,\ 1)\,, v_{pol_{y_3}}(x) = (2,\ 0,\ 2)$$

Как видим, $v_{pol_{y_j}}$ здесь имеют не более одного нулевого коэффициента. Всего векторов в классе 6.

Рассмотрим так же и остальные классы, где достигается такая оценка: $v_{f_1}(x) = (1,\ 1,\ 2)$ и $v_{f_2}(x) = (1,\ 0,\ 2)$. Для $v_{f_1}(x) = (1,\ 1,\ 2)$ оценка в классе достигается на векторах:

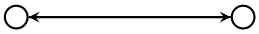
$$v_{y_4}(x) = (2,\ 0,\ 0)\,, v_{pol_{y_4}}(x) = (2,\ 0,\ 1)$$
$$v_{y_5}(x) = (1,\ 0,\ 0)\,, v_{pol_{y_5}}(x) = (1,\ 0,\ 2)$$

Все вектора в этом классе:

$$v_{y_4}(x) = (2,\ 0,\ 0)\,, v_{pol_{y_4}}(x) = (2,\ 0,\ 1)$$
$$v_{y_5}(x) = (1,\ 0,\ 0)\,, v_{pol_{y_8}}(x) = (1,\ 0,\ 2)$$
$$v_{y_6}(x) = (2,\ 1,\ 2)\,, v_{pol_{y_6}}(x) = (2,\ 2,\ 1)$$
$$v_{y_7}(x) = (1,\ 1,\ 0)\,, v_{pol_{y_7}}(x) = (1,\ 1,\ 1)$$
$$v_{y_8}(x) = (2,\ 0,\ 2)\,, v_{pol_{y_5}}(x) = (2,\ 1,\ 2)$$
$$v_{y_9}(x) = (1,\ 1,\ 2)\,, v_{pol_{y_9}}(x) = (1,\ 2,\ 2)$$

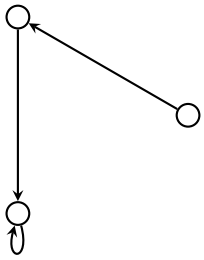
Для вектора $v_{f_2}(x) = (1,\ 0,\ 2)$ всего два вектора в классе:

$v_{f_0}(x) = (1,\, 0)$
$v_{pol_{f_0}}(x) = (1,\, 1)$

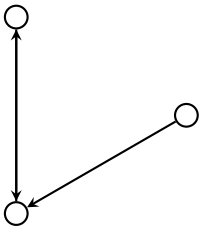


$v_{f_0}(x) = (0,\, 1)$
$v_{pol_{f_0}}(x) = (0,\, 1)$

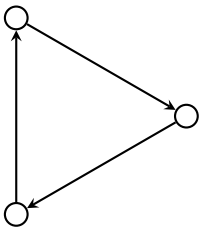
$v_{f_0}(x) = (2,\, 1,\, 1)$
$v_{pol_{f_0}}(x) = (2,\, 0,\, 2)$



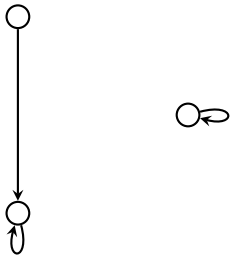
$v_{f_1}(x) = (1,\, 1,\, 2)$
$v_{pol_{f_1}}(x) = (1,\, 2,\, 2)$



$v_{f_2}(x) = (1,\, 0,\, 2)$
$v_{pol_{f_2}}(x) = (1,\, 1,\, 0)$



$v_{f_3}(x) = (0,\, 1,\, 1)$
$v_{pol_{f_3}}(x) = (0,\, 0,\, 1)$



$$v_{y_{10}}(x) = (2,\ 1,\ 0)\,, v_{pol_{y_{10}}}(x) = (2,\ 1,\ 0)$$

$$v_{y_{11}}(x) = (1,\ 0,\ 2)\,, v_{pol_{y_{11}}}(x) = (1,\ 1,\ 0)$$

И оценка достигается на обоих векторах.

Матрица для вычисления полиномов в поле $\mathbb{F}_7$

$$M_7(0,3,2,6,4,5,1) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 3 & 1 & 5 & 4 & 6 \\ 0 & 3 & 5 & 6 & 3 & 5 & 6 \\ 0 & 1 & 6 & 1 & 6 & 1 & 6 \\ 0 & 5 & 3 & 6 & 5 & 3 & 6 \\ 0 & 4 & 5 & 1 & 3 & 2 & 6 \\ 6 & 6 & 6 & 6 & 6 & 6 & 6 \end{pmatrix}$$

В P_7 оценка L(q) = q-2 достигается уже всего в трёх классах:

Порядок класса, содержащего вектор $v_{f_2}(x) = (1,\ 1,\ 1,\ 1,\ 6,\ 4,\ 5)$ равен 840, выписывать его полностью не имеет смысла, но можно привести некоторые вектора, на которых достигается оценка l(f) = q-2, самая низкая в этом классе. Опять же, таких векторов в нём всего 161, вот некоторые из них:

$$v_{y_0}(x) = (2,\ 6,\ 3,\ 4,\ 2,\ 2,\ 2)\,, v_{pol_{y_0}}(x) = (2,\ 6,\ 1,\ 5,\ 0,\ 2,\ 0)$$

$$v_{y_1}(x) = (6,\ 6,\ 4,\ 2,\ 5,\ 6,\ 6)\,, v_{pol_{y_1}}(x) = (6,\ 6,\ 5,\ 6,\ 0,\ 4,\ 0)$$

$$v_{y_2}(x) = (4,\ 4,\ 4,\ 4,\ 5,\ 1,\ 0)\,, v_{pol_{y_2}}(x) = (4,\ 4,\ 6,\ 0,\ 0,\ 1,\ 6)$$

$$v_{y_3}(x) = (4,\ 4,\ 4,\ 5,\ 6,\ 1,\ 4)\,, v_{pol_{y_3}}(x) = (4,\ 6,\ 4,\ 3,\ 0,\ 1,\ 0)$$

$$v_{y_4}(x) = (5,\ 0,\ 5,\ 5,\ 5,\ 1,\ 3)\,, v_{pol_{y_4}}(x) = (5,\ 4,\ 2,\ 0,\ 0,\ 2,\ 4)$$

$$v_{y_5}(x) = (5,\ 5,\ 5,\ 5,\ 1,\ 4,\ 3)\,, v_{pol_{y_5}}(x) = (5,\ 6,\ 6,\ 5,\ 0,\ 2,\ 0)$$

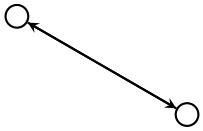
$$v_{y_6}(x) = (2,\ 2,\ 5,\ 2,\ 2,\ 1,\ 0)\,, v_{pol_{y_6}}(x) = (2,\ 0,\ 5,\ 5,\ 1,\ 1,\ 0)$$

$$v_{y_7}(x) = (2,\ 1,\ 3,\ 1,\ 1,\ 1,\ 0)\,, v_{pol_{y_7}}(x) = (2,\ 0,\ 4,\ 6,\ 0,\ 4,\ 5)$$

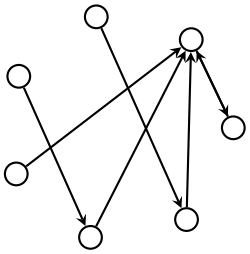
$$v_{y_8}(x) = (3,\ 5,\ 3,\ 3,\ 3,\ 1,\ 0)\,, v_{pol_{y_8}}(x) = (3,\ 6,\ 6,\ 3,\ 0,\ 0,\ 3)$$

Вот некоторые вектора на которых l(f) = q-3 (l(f) = 4):

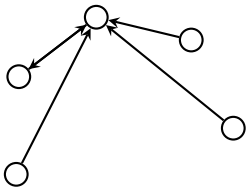
$v_{f_4}(x) = (0,\ 2,\ 1)$
$v_{pol_{f_4}}(x) = (0,\ 1,\ 0)$



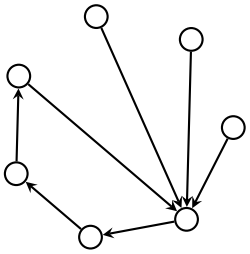
$v_{f_5}(x) = (2,\ 0,\ 1)$
$v_{pol_{f_5}}(x) = (2,\ 2,\ 0)$



$v_{f_0}(x) = (3,\ 0,\ 1,\ 5,\ 3,\ 3,\ 3)$
$v_{pol_{f_0}}(x) = (3,\ 4,\ 0,\ 1,\ 5,\ 1,\ 3)$



$v_{f_1}(x) = (2,\ 2,\ 6,\ 2,\ 2,\ 1,\ 5)$
$v_{pol_{f_1}}(x) = (2,\ 5,\ 5,\ 6,\ 6,\ 1,\ 1)$



$v_{f_2}(x) = (1,\ 1,\ 1,\ 1,\ 6,\ 4,\ 5)$
$v_{pol_{f_2}}(x) = (1,\ 5,\ 5,\ 1,\ 2,\ 3,\ 2)$

Оценка $L(q) \geq q - 2$

Теорема 1. *$L(q) \geq q$-2 при действии на множество функций биективных преобразований, оставляющих ноль на месте.*

Доказательство. Рассмотрим класс функций, который задаётся следующим графом:

Введём обозначения $I = \{1, 2, 3, ..., q-1\}$ и $\mathfrak{I}_k = I/\{k\}, k \neq 0$.

Такие функции задаются следующим образом: $f(0) = 0, f(x_i) = x_i$, для $i \in \mathfrak{I}_k$, и $f(x_k) = x_j$, где $j \in \mathfrak{I}_k$. Заметим, что $x_k \neq x_j$, так как это разные элементы поля.

Вектор значений этой функции имеет вид, соответствующий следующим двум вариантам: 1)$v_f = (0, x_1, \cdots, x_j, \cdots, x_{q-1})$;
2)$v_f = (0, x_1, \cdots, x_j)$.

Подействуем на этот вектор матрицей $M_q(0, 1, a_2, \cdots, a_{q-2}, a_{q-1})$ (обозначение 13) и посмотрим, какие получаются коэффициенты у полинома, т.е. рассмотрим значения вектора

$$v_{pol_f} = (c_0, c_1, \cdots, c_{q_2}, c_{q-1}).$$

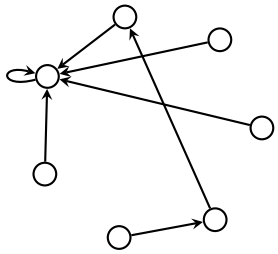
Поскольку для рассматриваемых функций все аргументы кроме одного переходят в себя, то поменяем обозначения аргументов матрицы: $M_q(0, x_1, \cdots, x_{q-1})$.

Рассмотрим коэффициент c_{q-1}. Так как последняя строка матрицы состоит из единиц, имеем $c_{q-1} = \sum\limits_{i \in \mathfrak{I}_k} x_i + x_j = -x_k + x_j \neq 0$. Отсюда получаем, что коэффициент при старшем мономе в этом классе всегда отличен от нуля.

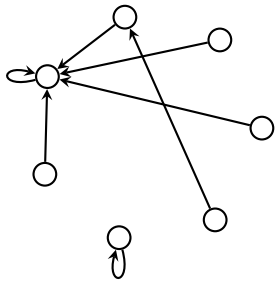
Коэффициент $c_0 = x_0 = 0$, поскольку $k \neq 0$ и x_0 это нулевой элемент поля.

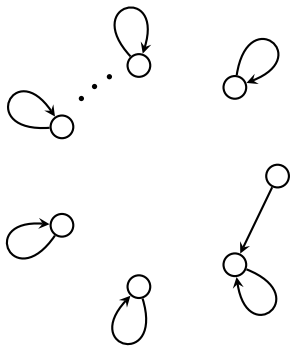
В силу того, что $k \neq 0$ коэффициенты c_{q-1-t}, где $1 \leq t \leq q-3$, равны $\sum\limits_{i \in \mathfrak{I}_k} x_i^t \cdot x_i + x_j \cdot x_k^t = \sum\limits_{i \in \mathfrak{I}_k} x_i^{t+1} + x_j \cdot x_k^t$. В силу утверждения имеем: $\sum\limits_{i \in \mathfrak{I}_k} x_i^{t+1} = -x_k^{t+1}$. Тогда получаем, что коэффициенты выражаются следующим образом: $c_{q-1-t} = -x_k^{t+1} + x_j \cdot x_k^t = x_k^t \cdot (x_j - x_k)$. В поле отсутствуют делители нуля, поэтому произведение не равно нулю, если ни один из множителей не равен нулю. При этом $x_j - x_k$ не равно нулю, так как x_j и x_k разные элементы поля, а $x_k \neq 0$ в силу того, что ноль неподвижен.

$v_{f_3}(x) = (6,\ 6,\ 6,\ 6,\ 6,\ 1,\ 2)$
$v_{pol_{f_3}}(x) = (6,\ 5,\ 0,\ 6,\ 3,\ 1,\ 2)$



$v_{f_4}(x) = (6,\ 6,\ 6,\ 6,\ 6,\ 5,\ 2)$
$v_{pol_{f_4}}(x) = (6,\ 0,\ 6,\ 3,\ 1,\ 2,\ 5)$





Отдельно рассмотрим коэффициент c_1. В этом случае имеем $c_1 = \sum\limits_{i \in \Im_k} x_i^{q-2} \cdot x_i + x_j \cdot x_k^{q-2} = \sum\limits_{i \in \Im_k} x_i^{q-1} + x_j \cdot x_k^{q-2} = \sum\limits_{i=1}^{q-2} 1 + x_j \cdot x_k^{q-2}$, который равен нулю в случае, если $x_j \cdot x_k^{q-2} = 2$.

Получаем, что в ноль обращается только c_0 и в некоторых случаях c_1.

Таким образом, на таком классе $l(f) \geq q - 2$, что доказывает утверждение теоремы.

□

Список литературы

[1] Таранников, Ю. В. Дискретная математика. Задачник : учебное пособие для академического бакалавриата / Ю. В. Таранников. — М. : Издательство Юрайт, 2016. — 385 с.

[2] Лидл Р., Нидеррайтер Г. Конечные поля. Издательство Мир, 1988

[3] Pinaki Das, The number of permutation polynomials of a given degree over a finite field 2002, Finite fields and their application 8, 478-490.

[4] Официальный сайт системы sagemath: http://www.sagemath.org/index.html

[5] The On-Line Encyclopedia of Integer Sequences, https://oeis.org/

Estimation of the maximum number of nonzero coefficients of a function polynomial under the action of a permutation group on a table of function values

Gremyakov A.O.

For coefficients of polynomials of functions over finite fields F_q, we consider the problem of finding a lower bound for the maximum minimum of the number of nonzero coefficients in the polynomial, where the maximum is taken over all functions and the minimum is taken from their transformations corresponding to various field assignments. Moreover, various types of such transformations are considered. The main results of the paper relate to two types of transformations, the description of which is given in the first section of the paper.

The paper estimates $L(q) \geq q - 2$ for the maximum minimum of the number of nonzero coefficients in the polynomial for the certain type of transformations that leave the zero field element in place.

Keywords: coefficients of polynomials, Boolean functions, polynomial of a Boolean function, table of values of a function, sagemath.