УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО УНИВЕРСИТЕТА.
СЕРИЯ ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ

2020, Т. 162, кн. 3
С. 285–299

ISSN 2541-7746 (Print)
ISSN 2500-2198 (Online)

УДК 519.714.4

doi: 10.26907/2541-7746.2020.3.285-299

СЛОЖНОСТЬ ПСЕВДОКРОНЕКЕРОВЫХ И СВОБОДНО КРОНЕКЕРОВЫХ ФОРМ ФУНКЦИЙ НАД КОНЕЧНЫМИ ПОЛЯМИ

А.С. Балюк

Иркутский государственный университет,

г. Иркутск, 664003, Россия

Аннотация

Предложен подход, позволяющий частично обобщить иерархию Грина – Сасао полиномиальных форм булевых функций на случай произвольного конечного поля.

Для сложности псевдокронекеровых и свободно кронекеровых форм n-местных функций над произвольным конечным полем $\mathbb{F}_q$ найдено точное значение функции Шеннона, которое оказывается равным q^{n-1}. Работа обобщает ранее известный результат для булевых функций.

Ключевые слова: конечное поле, сложность вычислений, свободно кронекеровы формы, псевдокронекеровы формы

Введение

В работах [1–3] предложен общий подход к классификации бинарных деревьев и соответствующих им полиномиальных представлений (форм) булевых функций. Это так называемая иерархия Грина – Сасао [4]. В частности, этот подход позволяет единообразно определить кронекеровы, псевдокронекеровы и свободно кронекеровы формы. Ранее были найдены оценки сложности кронекеровых [5], псевдокронекеровых и свободно кронекеровых [6] форм булевых функций, и кронекеровых форм функций над произвольным конечным полем [7]. В настоящей работе определение псевдокронекеровых и свободно кронекеровых форм булевых функций обобщается на случай произвольного конечного поля, а также устанавливаются верхние и эффективные нижние оценки сложности этих форм.

Введем некоторые обозначения, которые будут использоваться на протяжении всей статьи.

Обозначим через q целую положительную степень простого числа, через $\mathbb{F}_q$ конечное поле порядка q, через $\alpha_0, \alpha_1, \ldots, \alpha_q$ все элементы поля $\mathbb{F}_q$, взятые в фиксированном порядке, который закрепляется отображением $\kappa : \mathbb{F}_q \to \{0, 1, \ldots, q-1\}$, так что $\kappa(\alpha_i) = i$ для всех i, $0 \leqslant i \leqslant q-1$.

Введем в рассмотрение одноместные функции $\psi_0, \psi_1, \ldots, \psi_{q-1}$ над полем $\mathbb{F}_q$, которые задаются формулой $\psi_i(x) = 1 - (x - \alpha_i)^{q-1}$, $0 \leqslant i \leqslant q-1$. Поскольку по [8, лемма 2.1.16] для всех ненулевых элементов $b \in \mathbb{F}_q$ выполняется $b^{q-1} = 1$, то каждая из функций ψ_i обращается в нуль на всех значениях, кроме α_i, на котором она обращается в единицу.

Далее, n будет обозначать целое положительное число. Введем также обозначения $N = q^n$ и $Q = (q^n - 1)/(q-1) = q^0 + q^1 + \cdots + q^{n-1}$. Сразу обратим внимание, что $qQ + 1 = (q^{n+1} - 1)/(q-1)$ и $(Q-1)/q = (q^{n-1} - 1)/(q-1)$. Обозначим через $\sigma^1, \ldots, \sigma^N$ все n-ки (упорядоченные наборы длины n) с элементами из $\mathbb{F}_q$,

упорядоченные лексикографически следующим образом. Пусть j, $1 \leqslant j \leqslant N$, представлено в системе счисления с основанием q как $j = 1 + j_1 q^0 + j_2 q^1 + \cdots + j_n q^{n-1}$, где $0 \leqslant j_i \leqslant q-1$ при $1 \leqslant i \leqslant n$. Тогда $\sigma^j = (\sigma_1^j, \sigma_2^j, \ldots, \sigma_n^j)$, где $\sigma_i^j = \alpha_{j_i}$, и, как следствие, $\kappa(\sigma_i^j) = j_i$.

Множество n-местных функций над $\mathbb{F}_q$ с операциями сложения и умножения на константы из $\mathbb{F}_q$ образует линейное векторное пространство размерности N, которое будем обозначать как $\mathbb{F}_q^N$. Если задана n-местная функция $f : \mathbb{F}_q^n \to \mathbb{F}_q$, то компоненты ее векторного представления в пространстве $\mathbb{F}_q^N$ будут обозначаться как $f_1, f_2, \ldots, f_N$, где $f_j = f(\sigma^j)$, $1 \leqslant j \leqslant N$. В дальнейшем будем отождествлять функцию f с ее векторным представлением $(f_1, f_2, \ldots, f_N)$ и считать, что $f \in \mathbb{F}_q^N$.

1. Полные q-нарные деревья и полиномиальные формы.

Пусть T – корневое дерево с корневой вершиной v_0. Обозначим через V_T множество его вершин, а через E_T множество его ребер. Высотой вершины $v \in V_T$ будем называть число $h(v)$ ребер в пути от v_0 до v. Определим множество $C_v = \{u \in V_T \mid (v,u) \in E_T,\ h(v) < h(u)\}$ дочерних вершин вершины v.

Рассмотрим полное корневое q-нарное дерево T высоты n. Оно содержит $qQ+1$ вершину.

Пронумеруем его вершины следующим образом: v_0 – корневая вершина, если v_j – нелистовая вершина, то множество ее дочерних вершин $C_{v_j} = \{v_{qj+1}, v_{qj+2}, \ldots, v_{qj+q}\}$. Нетрудно убедиться, что при такой нумерации $\{v_0, v_1, \ldots, v_{qQ}\} = V_T$, то есть множество всех вершин дерева T, $\{v_0, v_1, \ldots, v_{Q-1}\}$ – множество всех нелистовых вершин, $\{v_Q, v_{Q+1}, \ldots, v_{qQ}\}$ – множество всех листовых вершин дерева T, $\{v_{(Q-1)/q}, v_{(Q-1)/q+1}, \ldots, v_{Q-1}\}$ – множество всех вершин с высотой $n-1$.

С каждой нелистовой вершиной v_j, где $0 \leqslant j \leqslant Q-1$, ассоциируем переменную x_{v_j} из множества $\{x_1, \ldots, x_n\}$. С каждым ребром $(v_j, v_{qj+i}) \in E_T$, где $0 \leqslant j \leqslant Q-1$ и $1 \leqslant i \leqslant q$, ассоциируем одноместную функцию $t_{qj+i} : \mathbb{F}_q \to \mathbb{F}_q$.

Дерево T задает преобразование из $\mathbb{F}_q^N$ в $\mathbb{F}_q^N$ следующим образом. Пусть $c = (c_1, c_2, \ldots, c_N) \in \mathbb{F}_q^N$. Припишем константы $c_1, c_2, \ldots, c_N$ листовым вершинам $v_Q, v_{Q+1}, \ldots v_{qQ}$ соответственно и будем считать, что в каждой листовой вершине v_j, где $Q \leqslant j \leqslant qQ$, вычисляется константная функция $f_{v_j}(x_1, \ldots, x_n) = c_{j-Q+1}$. Фактически, функции f_{v_j} не зависят ни от одной из переменных при $Q \leqslant j \leqslant qQ$. Для каждой нелистовой вершины v_j, $0 \leqslant j \leqslant Q-1$, рекурсивно определим функцию $f_{v_j} \in \mathbb{F}_q^n \to \mathbb{F}_q$ так, что

$$f_{v_j}(x_1, \ldots, x_n) = \sum_{i=1}^{q} t_{qj+i}(x_{v_j}) f_{v_{qj+i}}(x_1, \ldots, x_n). \tag{1}$$

Таким образом, дерево T преобразует вектор $c \in \mathbb{F}_q^N$ в функцию $f_{v_0} : \mathbb{F}_q^n \to \mathbb{F}_q$, а поскольку n-местная функция f_{v_0} может быть представлена в виде вектора из пространства $\mathbb{F}_q^N$, то дерево T задает преобразование из $\mathbb{F}_q^N$ в $\mathbb{F}_q^N$.

Если рекурсивно раскрыть все скобки в выражении (1) для $f_{v_0}(x_1, \ldots, x_n)$ вплоть до одноместных функций t_{qj+i} и констант $c_1, \ldots, c_N$, получим полиномиальную форму, соответствующую данному дереву T, которая представляет функцию f_{v_0}.

2. Пример

На рис. 1 приведен пример полного тернарного дерева высоты 2 для случая конечного поля $\mathbb{F}_3$. В этом дереве с вершинами v_0 и v_3 ассоциирована переменная x_1,

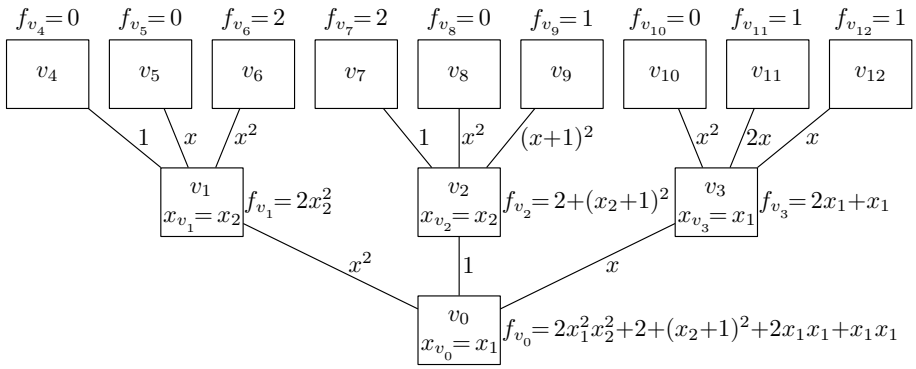

Рис. 1. Вычисление функции на примере полного тернарного дерева глубины 2

а с вершинами v_1 и v_2 – переменная x_2. С каждым ребром ассоциирована одноместная функция. Например, с ребром (v_1, v_4) ассоциирована константная одноместная функция $t_4(x) = 1$, а с ребром (v_2, v_9) – функция $t_9(x) = (x+1)^2$. Дерево преобразует вектор $c = (0, 0, 2,\ 2, 0, 1,\ 0, 1, 1)$ в функцию f_{v_0} следующим образом. Сначала листовым вершинам приписываются константы — компоненты вектора c, и определяются константные функции $f_{v_i}(x_1, x_2) = c_{i-4+1}$, $4 \leqslant i \leqslant 12$. Затем, по формуле (1) вычисляются функции f_{v_1}, f_{v_2}, f_{v_3}. При этом в функции t_{qj+i} из формулы (1) подставляется переменная, ассоциированная с соответствующей вершиной v_j. Например, с вершиной v_2 ассоциирована переменная x_2, значит, функция f_{v_2} будет вычисляться по формуле

$$t_7(x_2)f_{v_7}(x_1, x_2) + t_8(x_2)f_{v_8}(x_1, x_2) + t_9(x_2)f_{v_9}(x_1, x_2) = 1 \cdot 2 + x_2 \cdot 0 + (x_2 + 1)^2 \cdot 1.$$

Аналогично определяется функция f_{v_0}, которая в нашем случае равна

$$f_{v_0}(x_1, x_2) = x_1^2 \cdot f_{v_1}(x_1, x_2) + 1 \cdot f_{v_2}(x_1, x_2) + x_1 \cdot f_{v_3}(x_1, x_2).$$

После рекурсивного раскрытия скобок, получим следующую полиномиальную форму для f_{v_0}:

$$x_1^2{\cdot}1{\cdot}0{+}x_1^2{\cdot}x_2{\cdot}0{+}x_1^2{\cdot}x_2^2{\cdot}2{+}1{\cdot}1{\cdot}2{+}1{\cdot}x_2^2{\cdot}0{+}1{\cdot}(x_2{+}1)^2{\cdot}1{+}x_1{\cdot}x_1^2{\cdot}0{+}x_1{\cdot}2x_1{\cdot}1{+}x_1{\cdot}x_1{\cdot}1,$$

или после исключения нулевых слагаемых

$$f_{v_0}(x_1, x_2) = 2x_1^2x_2^2 + 2 + (x_2{+}1)^2 + 2x_1x_1 + x_1x_1.$$

Подставляя вместо (x_1, x_2) все пары с элементами из $\mathbb{F}_3$ в лексикографическом порядке, то есть $(0,0)$, $(0,1)$, $(0,2)$, $(1,0)$, $(1,1)$, $(1,2)$, $(2,0)$, $(2,1)$, $(2,2)$, и, произведя вычисления в конечном поле $\mathbb{F}_3$ (то есть по модулю три), получим векторное представление функции $f_{v_0} = (0, 0, 2,\ 0, 2, 1,\ 0, 2, 1)$.

Легко видеть, что дерево на рис. 1 будет преобразовывать произвольный вектор $c = (c_1, \ldots, c_9)$ в функцию (полиномиальную форму)

$$c_1x_1^2 + c_2x_1^2x_2 + c_3x_1^2x_2^2 + c_4 + c_5x_2^2 + c_6(x_2{+}1)^2 + c_7x_1x_1^2 + c_8x_1 \cdot 2x_1 + c_9x_1x_1.$$

Фактически, при изменении вектора c в полиномиальной форме меняются только коэффициенты $c_1, \ldots, c_9$, а произведения одноместных функций остаются без изменений. В частности, вектор $c = (0, 0, 2,\ 2, 0, 1,\ 0, 2, 2)$ будет преобразован в функцию $2x_1^2x_2^2 + 2 + (x_2{+}1)^2 + x_1x_1 + 2x_1x_1$, которая представляется вектором $(0, 0, 2,\ 0, 2, 1,\ 0, 2, 1)$. Таким образом, дерево на рис. 1 преобразует два различных вектора в один. Это означает, что преобразование в общем случае не является взаимооднозначным.

3. Канонические деревья и полиномиальные формы

Определение 1. Полное q-нарное дерево высоты n вместе с ассоциированными с его нелистовыми вершинами переменными из упорядоченного множества $(x_1, \ldots, x_n)$ и ассоциированными с его ребрами одноместными функциями над конечным полем $\mathbb{F}_q$ называется *каноническим деревом высоты* n, если оно задает взаимооднозначное отображение из $\mathbb{F}_q^N$ в $\mathbb{F}_q^N$.

Каноническому дереву высоты n естественным образом ставится в соответствие каноническая полиномиальная форма. Канонической она называется в том смысле, что каждая n-местная функция над конечным полем $\mathbb{F}_q$ представляется в виде этой полиномиальной формы единственным образом.

Определение 2. Количество ненулевых элементов в векторе c, компоненты которого нужно приписать листовым вершинам канонического дерева T, так чтобы оно вычисляло функцию f, называется *сложностью* представления функции f деревом T и обозначается $L_T(f)$. Эта же величина будет называться *сложностью* представления функции f *полиномиальной формой*, соответствующей дереву T.

Теорема 1. *Для того чтобы полное q-нарное дерево T высоты n было каноническим, достаточно, чтобы выполнялись следующие условия:*

(а) одноместные функции, ассоциированные с ребрами, исходящими из произвольной нелистовой вершины к ее дочерним вершинам, линейно независимы;

(б) в любом пути от корневой вершины до листовой переменные, ассоциированные с нелистовыми вершинами, встречаются во множестве переменных $\{x_1, \ldots, x_n\}$ ровно по одному разу.

Доказательство. Доказательство достаточности проведем индукцией по высоте n дерева T.

При $n = 1$ условие (б) выполнено для любого дерева автоматически, поскольку множество переменных состоит из единственной переменной x_1. Если функции $t_1(x), \ldots, t_q(x)$, соответственно приписанные ребрам, соединяющим корневую вершину v_0 с листовыми вершинами $v_1, \ldots, v_q$, линейно независимы, они образуют базис линейного пространства $\mathbb{F}_q^q$, поскольку его размерность совпадает с числом функций $t_1(x), \ldots, t_q(x)$. Значит, любая одноместная функция $f : \mathbb{F}_q \to \mathbb{F}_q$ может быть выражена некоторой линейной комбинацией $f(x_1) = c_1 t_1(x_1) + \cdots + c_q t_q(x_1)$. Таким образом, дерево T вычисляет функцию f, если его листовым вершинам $v_1, \ldots, v_q$ приписать константы $c_1, \ldots, c_q$. Поскольку одноместная функция f была выбрана произвольно, значит, дерево T может вычислить любую функцию и потому является каноническим.

При $n \geqslant 2$ с корневой вершиной v_0 дерева T ассоциирована некоторая переменная x_k из упорядоченного множества $(x_1, \ldots, x_n)$, а с ребрами, соединяющими вершину v_0 с вершинами $v_1, \ldots, v_q$, – функции $t_1(x), \ldots, t_q(x)$. Поскольку вершина v_0 встречается в любом пути от корневой вершины к листовой, то условие (б) означает, что с некорневыми нелистовыми вершинами ассоциированы переменные, отличные от x_k. Это, в свою очередь, означает, что функции $f_{v_1}, \ldots, f_{v_q}$, вычисляемые деревом T в вершинах $v_1, \ldots, v_q$, смежных с корневой, не зависят от переменной x_k.

Для каждого i, $1 \leqslant i \leqslant q$, рассмотрим полное q-нарное поддерево T_i дерева T, высоты $n-1$ с корнем в вершине v_i, смежной с v_0. Это поддерево удовлетворяет условиям (а) и (б), если в качестве множества вершин взять $\{x_1, \ldots, x_n\} \setminus \{x_k\}$. Тогда по предположению индукции для произвольной функции $g : \mathbb{F}_q^{n-1} \to \mathbb{F}_q$ найдется такой вектор $c_1, \ldots, c_{N/q} \in \mathbb{F}_q^{N/q}$, что, если приписать листовым

вершинам дерева T_i константы $c_1, \ldots, c_{N/q}$, оно будет вычислять функцию g, а значит, в вершине v_i дерева T будет вычисляться функция $f_{v_i}(x_1, \ldots, x_n) = g(x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n)$, фактически не зависящая от переменной x_k, то есть произвольная $(n-1)$-местная функция.

Пусть теперь $f : \mathbb{F}_q^n \to \mathbb{F}_q$ – произвольная функция. Для упрощения дальнейших выкладок будем считать, что с корневой вершиной v_0 дерева T ассоциирована переменная x_1, то есть будем считать, что $k = 1$. Определим функцию $g_i(x_2, \ldots, x_n) = b_{i1} f(\alpha_0, x_2, \ldots, x_n) + \cdots + b_{iq} f(\alpha_{q-1}, x_2, \ldots, x_n)$, где $1 \leqslant i \leqslant q$ и

$$\begin{bmatrix} b_{11} & b_{12} & \ldots & b_{1q} \\ b_{21} & b_{22} & \ldots & b_{2q} \\ \vdots & \vdots & \ddots & \vdots \\ b_{q1} & b_{q2} & \ldots & b_{qq} \end{bmatrix} = \begin{bmatrix} t_1(\alpha_0) & t_2(\alpha_0) & \ldots & t_q(\alpha_0) \\ t_1(\alpha_1) & t_2(\alpha_1) & \ldots & t_q(\alpha_1) \\ \vdots & \vdots & \ddots & \vdots \\ t_1(\alpha_{q-1}) & t_2(\alpha_{q-1}) & \ldots & t_q(\alpha_{q-1}) \end{bmatrix}^{-1}. \tag{2}$$

Матрица в правой части (2) обратима, поскольку функции $t_1(x), \ldots, t_q(x)$ по условию (а) линейно независимы, а значит, образуют базис линейного пространства $\mathbb{F}_q^q$. Тогда для каждого j, $1 \leqslant j \leqslant q$, имеем

$$f(\alpha_{j-1}, x_2, \ldots, x_n) = t_1(\alpha_{j-1}) g_1(x_2, \ldots, x_n) + \cdots + t_q(\alpha_{j-1}) g_q(x_2, \ldots, x_n).$$

Поскольку функция g_i является $(n-1)$-местной, найдутся такие константы $c_{(i-1)N/q+1}, \ldots, c_{iN/q}$, что, если их приписать листовым вершинам поддерева T_i, это поддерево будет вычислять функцию $f_{v_i}(x_1, \ldots, x_n) = g_i(x_2, \ldots, x_n)$. Это справедливо для всех i, $1 \leqslant i \leqslant q$. Поэтому выполняется

$$f(x_1, \ldots, x_n) = t_1(x) f_{v_1}(x_1, \ldots, x_n) + \cdots + t_q(x) f_{v_q}(x_1, \ldots, x_n),$$

следовательно, функция f вычисляется деревом T. Это завершает доказательство, поскольку функция $f : \mathbb{F}_q^n \to \mathbb{F}_q$ была выбрана произвольно. □

4. Классификация канонических деревьев и полиномиальных форм

В работах [1–3, 9] были введены различные классы (множества) канонических деревьев и соответствующих им канонических полиномиальных форм булевых функций. В данном разделе обобщим некоторые из них на случай произвольного конечного поля. Классы канонических деревьев и соответствующих им полиномиальных форм будут получаться путем наложения ограничений на ассоциированные с вершинами дерева переменные и ассоциированные с его ребрами одноместные функции. Для класса канонических деревьев $\mathfrak{M}$ и соответствующих им полиномиальных форм определим функцию Шеннона

$$L_{\mathfrak{M}}(n) = \max_{f \in \mathbb{F}_q^N} \min_{T \in \mathfrak{M}_n} L_T(f),$$

где $\mathfrak{M}_n$ обозначает множество всех деревьев высоты n, входящих в класс $\mathfrak{M}$.

4.1. Дерево Шеннона и совершенная полиномиальная нормальная форма. Каноническое q-нарное дерево высоты n будем называть деревом Шеннона, если выполнены два условия:

(а) для любой нелистовой вершины одноместными функциями, ассоциированными с ребрами, соединяющими эту вершину с дочерними, являются функции $\psi_0(x), \psi_1(x), \ldots, \psi_{q-1}(x)$;

(б) со всеми вершинами высоты h, $0 \leqslant h \leqslant n-1$, ассоциирована одна и та же переменная x_{h+1}.

Соответствующая дереву Шеннона полиномиальная форма называется совершенной полиномиальной нормальной формой.

Для каждой n-местной функции над полем $\mathbb{F}_q$ существует единственная совершенная полиномиальная нормальная форма с точностью до перестановки слагаемых. Поэтому всегда найдется функция, сложность которой будет равна q^n.

4.2. Деревья Рида – Маллера и поляризованные полиномы. Каноническое q-нарное дерево высоты n будем называть деревом Рида – Маллера, если выполнены два условия:

(а) существует такая n-ка $(b_1, \ldots, b_n)$ с элементами из $\mathbb{F}_q$, что для любой нелистовой вершины высоты h множество одноместных функций, ассоциированных с ребрами, соединяющими эту вершину с дочерними, совпадает с множеством функций $\{(x + b_{h+1})^j \mid 0 \leqslant j \leqslant q-1\}$;

(б) со всеми вершинами высоты h, $0 \leqslant h \leqslant n-1$, ассоциирована одна и та же переменная x_{h+1}.

Соответствующая дереву Рида – Маллера полиномиальная форма называется формой Рида – Маллера, или поляризованным полиномом.

Точное значение функции Шеннона для поляризованных полиномов булевых функций (поляризованных полиномов Жегалкина) было найдено в работе [10]. Точное значение функции Шеннона для конечных полей, отличных от поля $\mathbb{F}_2$, в настоящее время неизвестно. Первые оценки функции Шеннона для простых конечных полей нечетной характеристики были получены в [11, 12]. Наилучшие на текущий момент верхние оценки найдены в работах [13, 14], нижние оценки для трехзначных функций, то есть для поля $\mathbb{F}_3$, найдены в работе [15], нижние оценки для произвольного конечного поля – в работе [7].

4.3. Кронекеровы деревья и кронекеровы полиномиальные формы. Каноническое q-нарное дерево высоты n будем называть кронекеровым деревом, если выполнены два условия:

(а) существуют такие множества $S_1, \ldots, S_n$, каждое из которых состоит из q линейно независимых одноместных функций над полем $\mathbb{F}_q$, что для любой нелистовой вершины высоты h множество одноместных функций, ассоциированных с ребрами, соединяющими эту вершину с дочерними, совпадает с множеством S_{h+1};

(б) со всеми вершинами высоты h, $0 \leqslant h \leqslant n-1$, ассоциирована одна и та же переменная x_{h+1}.

Соответствующая кронекерову дереву полиномиальная форма называется кронекеровой.

Точное значение функции Шеннона для кронекеровых полиномиальных форм булевых функций, по-видимому, впервые приведено в [5]. Первые оценки функции Шеннона для кронекеровых форм функций над простыми конечными полями нечетной характеристики были найдены в работе [16]. Наилучшие на текущий момент верхние оценки для произвольных конечных полей получены в работе [17]. Нижние оценки исследовались, например, в работе [18].

4.4. Псевдокронекеровы и свободно кронекеровы деревья и полиномиальные формы. Каноническое q-нарное дерево высоты n будем называть псевдокронекеровым, если выполнены два условия:

(а) для любой нелистовой вершины одноместные функции, ассоциированные с ребрами, соединяющими эту вершину с ее дочерними вершинами, линейно независимы;

(б) со всеми вершинами высоты h, $0 \leqslant h \leqslant n-1$, ассоциирована одна и та же переменная x_{h+1}.

Соответствующая полиномиальная форма называется псевдокронекеровой.

Каноническое q-нарное дерево высоты n будем называть свободно кронекеровым, если выполнено два условия:

(а) для любой нелистовой вершины одноместные функции, ассоциированные с ребрами, соединяющими эту вершину с ее дочерними вершинами, линейно независимы;

(б) в любом пути от корневой вершины до листовой переменные, ассоциированные с нелистовыми вершинами, встречаются во множестве переменных $\{x_1, \ldots, x_n\}$ ровно по одному разу.

Соответствующая полиномиальная форма называется свободно кронекеровой.

Точное значение функции Шеннона для псевдокронекеровых и свободно кронекеровых форм булевых функций найдено в [6].

Исследование функции Шеннона для случая произвольного конечного поля является темой разд. 5. настоящей статьи.

4.5. Другие классы полиномиальных форм. Исследовались также и другие классы полиномиальных форм. Одни из них, например псевдополяризованные полиномы [2] или классы HPD и HDE [5], получаются путем наложения ограничений на канонические деревья. Другие, например обобщенные формы Рида – Маллера [2], расширенные полиномиальные формы [5] или полиномиальные нормальные формы [2], не могут быть построены из канонических деревьев высоты n, поскольку нелистовые вершины соответствующих таким формам деревьев должны содержать более q дочерних вершин.

5. Функция Шеннона для классов псевдокронекеровых и свободно кронекеровых полиномиальных форм

Теорема 2. *Для любой функции $f : \mathbb{F}_q^n \to \mathbb{F}_q$, где $n \geqslant 1$, найдется такое псевдокронекерово дерево T высоты n, что $L_T(f) \leqslant q^{n-1}$.*

Доказательство. Пусть T – полное q-нарное дерево высоты n. Пусть $v_0, v_1, \ldots, v_{qQ}$ – все вершины дерева T, взятые таким образом, что v_0 – корневая вершина, и для каждой нелистовой вершины v_j, $0 \leqslant j \leqslant Q-1$, вершины $v_{qj+1}, \ldots, v_{qj+q}$ являются ее дочерними. Напомним, что листовыми вершинами при таком порядке являются вершины $v_Q, v_{Q+1}, \ldots, v_{qQ}$, высоту $n-1$ имеют вершины $v_{(Q-1)/q}, v_{(Q-1)/q+1}, \ldots, v_{Q-1}$, а все остальные вершины составляют множество $\{v_0, v_1, \ldots, v_{(Q-1)/q-1}\}$, которое может оказаться пустым, если $n = 1$.

С каждой нелистовой вершиной высоты h, $0 \leqslant h \leqslant n-1$, ассоциируем переменную x_{h+1}.

С каждым ребром, соединяющим вершину v_j высоты не более $n-2$ и v_{qj+k}, где $1 \leqslant k \leqslant q$ и $0 \leqslant j \leqslant (Q-1)/q-1$, ассоциируем одноместную функцию $\psi_{k-1}(x)$. Фактически, если удалить из дерева T все вершины высоты n и инцидентные им ребра, оставшаяся часть будет представлять собой дерево Шеннона.

Прежде чем перейти к ассоциированию одноместных функций с ребрами, инцидентными листовым вершинам, посмотрим, какие функции должны вычисляться в вершинах дерева, чтобы в корневой вершине вычислялась функция $f_{v_0}(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$. Согласно формуле (1) имеем

$$f_{v_j}(x_1, x_2, \ldots, x_n) = \sum_{k=1}^{q} \psi_{k-1}(x_{v_j}) f_{v_{qj+k}}(x_1, x_2, \ldots, x_n) \tag{3}$$

при $0 \leqslant j \leqslant (Q-1)/q-1$. В случае $j=0$ в (3) вместо переменной $x_{v_0}=x_1$ подставим σ_1^1. Сразу заметим, что $\sigma_1^1=\alpha_0$. Тогда

$$f(\sigma_1^1,x_2,\ldots,x_n)=$$
$$=f_{v_0}(\alpha_0,x_2,\ldots,x_n)=\sum_{k=1}^{q}\psi_{k-1}(\alpha_0)f_{v_k}(\alpha_0,x_2,\ldots,x_n)=f_{v_1}(\alpha_0,x_2,\ldots,x_n),$$

поскольку все $\psi_{k-1}(\alpha_0)$ при $k\geqslant 2$ обращаются в 0, а $\psi_0(\alpha_0)=1$. Далее заметим, что функция $f_{v_1}(x_1,x_2,\ldots,x_n)$ фактически не зависит от переменной x_1, так как эта переменная не ассоциирована ни с одной вершиной, высота которой не меньше 1, то есть не меньше, чем высота вершины v_1. Таким образом,

$$f_{v_1}(x_1,x_2,\ldots,x_n)=f_{v_1}(\alpha_0,x_2,\ldots,x_n)=f(\sigma_1^1,x_2,\ldots,x_n).$$

Рассуждая аналогично для всех вершин высоты 1, то есть для случая $1\leqslant j\leqslant q$ получим, что $f_{v_j}(x_1,x_2,\ldots,x_n)=f(\sigma_1^j,x_2,\ldots,x_n)$. Проводя последовательно подобные рассуждения для вершин высоты $2,3,\ldots,n-1$, обнаружим, что $f_{v_{j-1+(Q-1)/q}}(x_1,\ldots,x_{n-1},x_n)=f(\sigma_1^j,\ldots,\sigma_{n-1}^j,x_n)$, для всех j, $1\leqslant j\leqslant q^{n-1}=N/q$. Другими словами, в вершинах дерева на высоте $n-1$ должны вычисляться функции $f(\sigma_1^1,\ldots,\sigma_{n-1}^1,x_n),\ldots,f(\sigma_1^{N/q},\ldots,\sigma_{n-1}^{N/q},x_n)$.

Для каждого j, $1\leqslant j\leqslant N/q$, введем в рассмотрение одноместную функцию $g_j:\mathbb{F}_q\to\mathbb{F}_q$, определяемую как $g_j(x)=f(\sigma_1^j,\ldots,\sigma_{n-1}^j,x)$. Зададим множество $J=\{j\mid 1\leqslant j\leqslant N/q,\ g_j(x)\not\equiv 0\}$ таких индексов j, для которых функция g_j не является тождественно нулевой. Определим вектор $(c_1,c_2,\ldots,c_N)$, в котором все компоненты равны 0, кроме компонентов c_{qj-q+1}, где $j\in J$, которые равны 1.

Для каждого $j\in J$ из множества $\{g_j(x),1,x,x^2,\ldots,x^{q-1}\}$ выберем q функций, так чтобы они были линейно независимыми и чтобы одной из них была функция $g_j(x)$. Это всегда возможно сделать, поскольку $g_j(x)$ не равна тождественно нулю, а функции 1, x, $x^2,\ldots,x^{q-1}$ линейно независимы, так как образуют так называемый полиномиальный базис. С ребром, соединяющим вершины v_i и v_{qi+1}, где $i=j-1+(Q-1)/q$, ассоциируем одноместную функцию $g_j(x)$, а с ребрами, соединяющими вершину v_i с вершинами $v_{qi+2},\ldots,v_{qi+q}$, – остальные из выбранных q функций в произвольном порядке. Так как $f_{v_{qi+1}}$ – это константная функция, значение которой равно $c_{qj-q+1}=1$, а функции $f_{v_{qi+2}},\ldots,f_{v_{qi+q}}$ тождественно равны нулю, поскольку $c_{qj-q+2}=\cdots=c_{qj-q+q}=0$, то по формуле (1)

$$f_{v_i}(x_1,\ldots,x_n)=\sum_{k=1}^{q}t_{qi+k}(x_n)f_{v_{qi+k}}(x_1,\ldots,x_n)=g_j(x_n)=f(\sigma_1^j,\ldots,\sigma_{n-1}^j,x_n).$$

Для каждого из остальных j, $1\leqslant j\leqslant N/q$, то есть для не входящих во множество J, ассоциируем с ребрами, соединяющими листовые вершины с вершиной v_i, где снова $i=j-1+(Q-1)/q$, одноместные функции $1,x,x^2,\ldots,x^{q-1}$ в любом порядке. Как уже упоминалось выше, эти функции линейно независимые. Тогда, поскольку константы $c_{qi+1},\ldots,c_{qi+q}$ все равны нулю, функции $f_{v_{qi+1}},\ldots,f_{v_{qi+q}}$ тождественно равны нулю и

$$f_{v_i}(x_1,\ldots,x_n)=\sum_{k=1}^{q}t_{qi+k}(x_n)f_{v_{qi+k}}(x_1,\ldots,x_n)=0=g_j(x_n)=f(\sigma_1^j,\ldots,\sigma_{n-1}^j,x_n).$$

Таким образом, в вершинах дерева на высоте $n-1$ вычисляются функции $f(\sigma_1^1,\ldots,\sigma_{n-1}^1,x_n),\ldots,f(\sigma_1^{N/q},\ldots,\sigma_{n-1}^{N/q},x_n)$, а следовательно, дерево T вычисляет

функцию $f(x_1,\dots,x_n)$. При этом по построению дерево T является псевдокронекеровым, а сложность представления функции f деревом T равняется $L_T(f) = |\{i \mid 1 \leqslant i \leqslant N,\ c_i \neq 0\}| = |J| \leqslant N/q = q^{n-1}$, поскольку множество J содержит не более N/q элементов. □

Определение 3. Пусть $\mathbb{F}_{q^k}$ – расширение конечного поля $\mathbb{F}_q$. *Следом* элемента $\beta \in \mathbb{F}_{q^k}$ называется значение выражения $\beta + \beta^q + \beta^{q^2} + \dots + \beta^{q^{k-1}}$, которое будем обозначать $\mathrm{Tr}_q^k(\beta)$.

След удовлетворяет следующим свойствам (см. [8, теорема 2.1.83]):
(а) $\mathrm{Tr}_q^k(\beta) \in \mathbb{F}_q$ для любого $\beta \in \mathbb{F}_{q^k}$;
(б) $\mathrm{Tr}_q^k(b\beta + d\delta) = b\mathrm{Tr}_q^k(\beta) + d\mathrm{Tr}_q^k(\delta)$ для любых $\beta,\ \delta \in \mathbb{F}_{q^k}$ и любых $b,\ d \in \mathbb{F}_q$.

Определение 4. Пусть $b_0, b_1, \dots, b_{k-1}$ – некоторые элементы конечного поля $\mathbb{F}_q$. Бесконечная последовательность $s_0, s_1, s_2, \dots$ элементов из поля $\mathbb{F}_q$, удовлетворяющая соотношению

$$s_{i+k} = b_{k-1}s_{i+k-1} + b_{k-2}s_{i+k-2} + \dots + b_0 s_i \tag{4}$$

для всех $i \geqslant 0$, называется *линейной рекуррентной последовательностью порядка* k, а многочлен $p(x) = x^k - b_{k-1}x^{k-1} - \dots - b_1 x - b_0$ – ее *характеристическим многочленом.*

Определение 5. Пусть $s_0, s_1, s_2, \dots$ – бесконечная последовательность элементов из некоторого множества S. Если существуют такие целые $m \geqslant 0$ и $r > 0$, что для всех $i \geqslant m$ выполняется $s_{i+r} = s_i$, то последовательность $s_0, s_1, s_2, \dots$ называется *периодической*, а число r – ее периодом. Наименьший из всех возможных периодов периодической последовательности называется ее *минимальным периодом.* В случае $m = 0$ периодическая последовательность называется *чисто периодической.*

Определение 6. Линейная рекуррентная последовательность порядка $k \geqslant 1$ над полем $\mathbb{F}_q$ называется *m-последовательностью порядка k*, если она чисто периодическая, содержит хотя бы один ненулевой элемент и ее минимальный период равен $q^k - 1$.

Из [19, теорема 7] следует, что для всякого конечного поля $\mathbb{F}_q$ и для всякого целого $k \geqslant 1$ найдется m-последовательность порядка k над полем $\mathbb{F}_q$, при этом ее характеристический многочлен является примитивным, то есть его корни – примитивные элементы расширения $\mathbb{F}_{q^k}$ поля $\mathbb{F}_q$.

Сформулируем и докажем обращение следствия 10.2.17 из [8] для m-последовательностей.

Лемма 1. *Пусть ξ — примитивный элемент поля $\mathbb{F}_{q^k}$. Тогда для любого ненулевого $\beta \in \mathbb{F}_{q^k}$ последовательность $s_0, s_1, s_2, \dots$, где $s_i = \mathrm{Tr}_q^k(\beta\xi^i)$, $i \geqslant 0$, является m-последовательностью порядка k.*

Доказательство. Пусть $p(x)$ – многочлен степени k над $\mathbb{F}_q$, корнем которого является ξ. По [19, теореме 7] существует m-последовательность $s_0, s_1, s_2, \dots$ порядка k над $\mathbb{F}_q$, характеристическим многочленом которой является $p(x)$. Из [8, следствие 10.2.17] следует, что существует такое $\beta_0 \in \mathbb{F}_{q^k}$, что $s_i = \mathrm{Tr}_q^k(\beta_0\xi^i)$, $i \geqslant 0$. При этом $\beta_0 \neq 0$, ибо в противном случае последовательность содержала бы только нули.

Для каждого m, $1 \leqslant m \leqslant q^k - 2$, рассмотрим последовательность b_0^m, b_1^m, $b_2^m, \ldots$, в которой $b_i^m = s_{i+m}$ для всех $i \geqslant 0$. Все эти последовательности, включая $s_0, s_1, s_2, \ldots$, имеют один и тот же минимальный период, то есть $q^k - 1$, поскольку «хвосты» у них совпадают. Характеристический многочлен у них тоже один и тот же, то есть $p(x)$.

Обозначив для удобства последовательность $s_0, s_1, s_2, \ldots$ как $b_0^0, b_1^0, b_2^0, \ldots$, проверим, могут ли совпадать последовательности $b_0^m, b_1^m, b_2^m, \ldots$ и $b_0^l, b_1^l, b_2^l, \ldots$ при $0 \leqslant m < l \leqslant q^k - 2$. Допустим, что могут. Тогда для любого $i \geqslant 0$ выполняется $s_{i+m} = s_{i+l}$ или, что то же, для любого $i \geqslant m$ выполняется $s_i = s_{i+r}$, где $r = l - m$, то есть r – период последовательности $s_0, s_1, s_2, \ldots$. При этом $r \leqslant q^k - 2$, что противоречит тому, что минимальный период последовательности $s_0, s_1, s_2, \ldots$ равен $q^k - 1$.

Итак, мы имеем $q^k - 1$ различных m-последовательностей, для каждой из которых найдется соответствующее ненулевое $\beta_m \in \mathbb{F}_{q^k}$ такое что $b_i^m = \mathrm{Tr}_q^k(\beta_m \xi^i)$ для всех $i \geqslant 0$ и $0 \leqslant m \leqslant q^k - 2$.

Но в поле $\mathbb{F}_{q^k}$ всего $q^k - 1$ различных ненулевых элементов, что совпадает с числом построенных m-последовательностей. Значит, для любого ненулевого $\beta \in \mathbb{F}_{q^k}$ последовательность $s_0, s_1, s_2, \ldots$, где $s_i = \mathrm{Tr}_q^k(\beta \xi^i)$ для всех $i \geqslant 0$, является m-последовательностью порядка k. □

Теорема 3. *Пусть* $f(x_1, \ldots, x_n) = \mathrm{Tr}_q^q\big(\beta \cdot \xi_1^{\kappa(x_1)} \cdot \ldots \cdot \xi_n^{\kappa(x_n)}\big)$, *где* β – *ненулевой, а* $\xi_1, \ldots, \xi_n$ – *примитивные элементы поля* $\mathbb{F}_{q^q}$. *Тогда* $L_T(f) \geqslant q^{n-1}$ *для любого свободно кронекерова дерева* T *высоты* n.

Доказательство. Для начала заметим, что m-последовательность $s_0, s_1, s_2, \ldots$ порядка k не может содержать k подряд идущих нулевых элементов. Ибо если $s_m = s_{m+1} = \cdots = s_{m+k-1} = 0$, то по формуле (4) выполняется $s_{m+k} = b_{k-1}s_{m+k-1} + \cdots + b_0 s_m = 0$, а следовательно и $s_{m+k+1} = 0$, и вообще $s_{m+i} = 0$ для всех $i \geqslant 0$. Это противоречит определению m-последовательности.

Пусть T – свободно кронекерово дерево высоты $n \geqslant 1$. Доказательство будем вести индукцией по высоте дерева T.

Базис индукции при $n = 1$. Напомним, что $\alpha_0, \alpha_1, \ldots, \alpha_{q-1} \in \mathbb{F}_q$ таковы, что $\kappa(\alpha_i) = i$ при $0 \leqslant i \leqslant q - 1$. Последовательные значения функции f, а именно $f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{q-1})$, являются q-мя первыми членами последовательности $s_0, s_1, s_2, \ldots$, где $s_i = \mathrm{Tr}_q^q(\beta \xi_1^{\kappa(\alpha_i)}) = \mathrm{Tr}_q^q(\beta \xi_1^i)$, которая по лемме 1 является m-последовательностью порядка q, а значит, не содержит q подряд идущих нулевых значений. Следовательно, среди $f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{q-1})$ найдется хотя бы одно ненулевое значение, то есть функция $f(x)$ не равна тождественно нулю. Тогда для ее вычисления в дереве T хотя бы одной листовой вершине должна быть приписана ненулевая константа. Тогда $L_T(f) \geqslant 1 = q^{n-1}$, и базис индукции выполняется.

Шаг индукции при $n \geqslant 2$. Пусть с корневой вершиной v_0 дерева T ассоциирована переменная x_k, а с ребрами, соединяющими вершину v_0 с вершинами $v_1, \ldots, v_q$, – одноместные функции $t_1(x), \ldots, t_q(x)$ соответственно. Выясним, какие функции должны вычисляться в вершинах $v_1, \ldots, v_q$, для того чтобы в вершине v_0 вычислялась функция $f(x_1, \ldots, x_n) = \mathrm{Tr}_q^q\big(\beta \cdot \xi_1^{\kappa(x_1)} \cdot \ldots \cdot \xi_n^{\kappa(x_n)}\big)$. Обозначим, как и раньше, эти функции через $f_{v_1}, \ldots, f_{v_q}$ соответственно, и, поскольку по определению свободно кронекерова дерева переменная x_k не ассоциирована ни с какой другой вершиной, кроме корневой, можно считать, что эти функции не зависят от переменной x_k.

В выражение (1) последовательно подставим вместо переменной x_k значения $\alpha_0, \alpha_1, \ldots, \alpha_{q-1}$ (чтобы не загромождать выкладки, будем считать, что $k = 1$):

$$\begin{aligned}
f(\ \alpha_0\ , x_2, \ldots, x_n) &= t_1(\ \alpha_0\ ) f_{v_1}(x_2, \ldots, x_n) + \cdots + t_q(\ \alpha_0\ ) f_{v_q}(x_2, \ldots, x_n),\\
f(\ \alpha_1\ , x_2, \ldots, x_n) &= t_1(\ \alpha_1\ ) f_{v_1}(x_2, \ldots, x_n) + \cdots + t_q(\ \alpha_1\ ) f_{v_q}(x_2, \ldots, x_n),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
f(\alpha_{q-1}, x_2, \ldots, x_n) &= t_1(\alpha_{q-1}) f_{v_1}(x_2, \ldots, x_n) + \cdots + t_q(\alpha_{q-1}) f_{v_q}(x_2, \ldots, x_n).
\end{aligned}$$

Как видно, здесь выполняется линейное преобразование, и, поскольку по определению свободно кронекерова дерева функции $t_1(x), \ldots, t_q(x)$ линейно независимы, можно найти матрицу, обратную к данному преобразованию. Обозначим ее B, а ее элементы b_{ji}:

$$\begin{bmatrix} b_{11} & b_{12} & \ldots & b_{1q} \\ b_{21} & b_{22} & \ldots & b_{2q} \\ \vdots & \vdots & \ddots & \vdots \\ b_{q1} & b_{q2} & \ldots & b_{qq} \end{bmatrix} = \begin{bmatrix} t_1(\alpha_0) & t_2(\alpha_0) & \ldots & t_q(\alpha_0) \\ t_1(\alpha_1) & t_2(\alpha_1) & \ldots & t_q(\alpha_1) \\ \vdots & \vdots & \ddots & \vdots \\ t_1(\alpha_{q-1}) & t_2(\alpha_{q-1}) & \ldots & t_q(\alpha_{q-1}) \end{bmatrix}^{-1}.$$

Тогда функции f_{v_j}, $1 \leqslant j \leqslant q$, определяются следующим выражением:

$$\begin{aligned}
f_{v_j}(x_2, \ldots, x_n) &= \sum_{i=1}^{q} b_{ji} f(\alpha_{i-1}, x_2, \ldots, x_n) = \\
&= \sum_{i=1}^{q} b_{ji} \mathrm{Tr}_q^q\bigl(\beta \xi_1^{\kappa(\alpha_{i-1})} \xi_2^{\kappa(x_2)} \ldots \xi_n^{\kappa(x_n)}\bigr) = \mathrm{Tr}_q^q\Bigl(\beta \xi_2^{\kappa(x_2)} \ldots \xi_n^{\kappa(x_n)} \sum_{i=1}^{q} b_{ji} \xi_1^{i-1}\Bigr).
\end{aligned}$$

Введем обозначение: $\delta_j = \sum_{i=1}^{q} b_{ji} \xi_1^{i-1}$. Поскольку $\xi_1^0, \xi_1^1, \ldots, \xi_1^{q-1}$ образуют полиномиальный базис (см. [8, определение 2.1.96]) расширения $\mathbb{F}_{q^q}$ над $\mathbb{F}_q$ в том смысле, что линейная комбинация $d_0\xi^0 + d_1\xi^1 + \cdots + d_{q-1}\xi^{q-1}$, где $d_i \in \mathbb{F}_q$ при $1 \leqslant i \leqslant q-1$, обращается в нуль, только если $d_0 = d_1 = \cdots = d_{q-1} = 0$, то $\delta_j \neq 0$, так как строка $b_{j1}, b_{j2}, \ldots, b_{jq}$ невырожденной матрицы B не может состоять из одних лишь нулей.

Значит, для всех j, $1 \leqslant j \leqslant q$, $f_{v_j}(x_2, \ldots, x_n) = \mathrm{Tr}_q^q\bigl(\beta\delta_j \xi_2^{\kappa(x_2)} \ldots \xi_n^{\kappa(x_n)}\bigr)$, то есть функции f_{v_j} имеют тот же вид, что и функция f в условиях леммы. По индуктивному предположению $L_{T_j}(f_{v_j}) \geqslant q^{n-2}$, где T_j означает полное q-нарное поддерево дерева T высоты $n-1$ с корнем в вершине v_j с унаследованными от дерева T ассоциациями переменных нелистовым вершинам и одноместных функций ребрам. Тогда $L_T(f) = L_{T_1}(f_{v_1}) + \cdots + L_{T_q}(f_{v_q}) \geqslant q q^{n-2} = q^{n-1}$. □

Следствие 1. *Пусть элементы $f_1, f_2, \ldots, f_N$ векторного представления функции $f : \mathbb{F}_q^n \to \mathbb{F}_q$ представляют собой начальный отрезок m-последовательности порядка q над полем $\mathbb{F}_q$. Тогда для любого свободно кронекерова дерева T высоты n выполняется $L_T(f) \geqslant q^{n-1}$.*

Доказательство. Пусть $s_0, s_1, s_2, \ldots$ – такая m-последовательность порядка q над $\mathbb{F}_q$, что $s_i = f_{i+1}$ для всех i, $0 \leqslant i \leqslant N-1$. По [8, следствие 10.2.17] существует примитивный элемент ξ в расширении $\mathbb{F}_{q^q}$ поля $\mathbb{F}_q$ и ненулевое $\beta \in \mathbb{F}_{q^q}$, что $s_i = \mathrm{Tr}_q^q(\beta\xi^i)$ для всех $i \geqslant 0$. Тогда $f_j = f(\sigma^j) = \mathrm{Tr}_q^q(\beta\xi^{j-1})$ при $1 \leqslant j \leqslant N$.

По [8, теорема 2.1.73] для каждого $i \geqslant 0$ элементы ξ^{q^i} также являются примитивными в поле $\mathbb{F}_{q^q}$. Рассмотрим функцию $g(x_1, \ldots, x_n) = \mathrm{Tr}_q^q\bigl(\beta\xi_1^{\kappa(x_1)} \ldots \xi_n^{\kappa(x_n)}\bigr)$,

где $\xi_i = \xi^{q^{i-1}}$ при $1 \leqslant i \leqslant n$. Вычислим ее значение на наборе σ^j, где $1 \leqslant j \leqslant N$. Для этого представим j в системе счисления по основанию q, то есть в виде $j = 1 + j_1 + j_2 q + j_3 q^2 + \cdots + j_n q^{n-1}$, где $0 \leqslant j_i \leqslant q-1$ при $1 \leqslant i \leqslant n$. Тогда

$$g(\sigma^j) = \mathrm{Tr}_q^q\big(\beta\xi_1^{\kappa(\sigma_1^j)} \dots \xi_n^{\kappa(\sigma_n^j)}\big) = \mathrm{Tr}_q^q\big(\beta\xi_1^{j_1} \dots \xi_n^{j_n}\big) =$$
$$= \mathrm{Tr}_q^q\big(\beta\xi^{j_1 q^0} \dots \xi^{j_n q^{n-1}}\big) = \mathrm{Tr}_q^q\big(\beta\xi^{j_1 q^0 + \ldots + j_n q^{n-1}}\big) = \mathrm{Tr}_q^q\big(\beta\xi^{j-1}\big).$$

Таким образом функция g совпадает с функцией f и ее можно представить в виде, подходящем для применения теоремы 3. □

Следствие 2. *Точное значение функции Шеннона для классов псевдокронекеровых и свободно кронекеровых полиномиальных форм (деревьев) равно* q^{n-1}.

Доказательство. Обозначим через $\mathfrak{P}$ класс псевдокронекеровых, а через $\mathfrak{F}$ класс свободно кронекеровых деревьев. Поскольку $\mathfrak{P} \subset \mathfrak{F}$, для любой функции $f : \mathbb{F}_q^n \to \mathbb{F}_q$ выполняется $\min\{L_T(f) \mid T \in \mathfrak{F}_n\} \leqslant \min\{L_T(f) \mid T \in \mathfrak{P}_n\}$. По теореме 2 имеем $\min\{L_T(f) \mid T \in \mathfrak{P}_n\} \leqslant q^{n-1}$ также для любой $f : \mathbb{F}_q^n \to \mathbb{F}_q$. По следствию 1 найдется функция $g : \mathbb{F}_q^n \to \mathbb{F}_q$, что $\min\{L_T(g) \mid T \in \mathfrak{F}_n\} \geqslant q^{n-1}$. Объединяя все вместе, получим следующую цепочку неравенств:

$$q^{n-1} \leqslant \min_{T \in \mathfrak{F}_n} L_T(g) \leqslant L_{\mathfrak{F}}(n) =$$
$$= \max_{f \in \mathbb{F}_q^N} \min_{T \in \mathfrak{F}_n} L_T(f) \leqslant L_{\mathfrak{P}}(n) = \max_{f \in \mathbb{F}_q^N} \min_{T \in \mathfrak{P}_n} L_T(f) \leqslant q^{n-1}.$$

Значит, все неравенства в этом выражении обращаются в равенства, и, следовательно, функции Шеннона для классов псевдокронекеровых и свободно кронекеровых деревьев равны между собой и равны q^{n-1}. □

Благодарности. Работа выполнена при поддержке РФФИ (проект № 19-01-00200).

Литература

1. *Green D.H.* Families of Reed-Muller canonical forms // Int. J. Electron. – 1991. – V. 70, No 2. – P. 259–280. – doi: 10.1080/00207219108921277.
2. *Sasao T.* Representations of logic functions using EXOR operators // Representations of Discrete Functions. – Boston: Kluwer Acad. Publ., 1996. – P. 29–54. – doi: 10.1007/978-1-4613-1385-4_2.
3. *Ho P., Perkowski M.* Free Kronecker decision diagrams and their application to Atmel 6000 series FPGA mapping // Proc. Conf. on European Design Automation. – Grenoble, France, 1994. – P. 8–13. – doi: 10.1145/198174.198180.
4. *Al-Rabadi A.N.* An extended Green-Sasao hierarchy of canonical ternary Galois forms and Universal Logic Modules // Facta Univ., Ser.: Electron. Energ. – 2017. – V. 30, No 1, P. 49–66. – doi: 10.1080/00207219108921277.
5. Избранные вопросы теории булевых функций / Под ред. С.Ф. Винокурова, Н.А. Перязева. – М.: Физматлит, 2001. – 192 р.
6. *Балюк А.С., Винокуров С.Ф.* Функция Шеннона для некоторых классов операторных полиномиальных форм // Оптимизация, управление, интеллект. – 2000. – Т. 5, № 1. – С. 111–121.

7. *Балюк А.С., Зинченко А.С.* Нижние оценки сложности поляризованных полиномов над конечными полями // Сиб. матем. журн. – 2019. – V. 60, No 1. – P. 3–13. – doi: 10.1134/S0037446619010014.

8. *Mullen G.L., Panarino D.* Handbook of Finite Fields. – N. Y.: Chapman and Hall/CRC, 2013. – 1068 p. – doi: 10.1201/b15006.

9. *Baluck A.S., Vinokurov S.F.* Classes of operator forms // 5th Int. Workshop on Boolean Problems. – Freiberg, Germany, 2002. – P. 76–83.

10. *Перязев Н.А.* Сложность булевых функций в классе полиномиальных поляризованных форм // Алгебра и логика. – 1995. – Т. 34, № 3. – С. 323–326.

11. *Селезнева С.Н.* О сложности представления функций многозначных логик поляризованными полиномами // Дискрет. матем. – 2002. – Т. 14, № 2. – С. 48–53.

12. *Алексеев В.Б., Вороненко А.А., Селезнева С.Н.* О сложности реализации функций k-значной логики поляризованными полиномами // Труды V Междунар. конференции «Дискретные модели в теории управляющих систем». – Ратмино, 2003. – С. 8–9.

13. *Балюк А.С., Янушковский Г.В.* Верхние оценки сложности функций над конечными полями в некоторых классах кронекеровых форм // Изв. Иркут. гос. ун-та. Сер. «Математика». – 2015. – № 14. – С. 3–17.

14. *Казимиров А.С., Реймеров С.Ю.* Верхние оценки сложности функций над непростыми конечными полями в классе поляризованных полиномов // Изв. Иркут. гос. ун-та. Сер.«Математика». – 2016. – № 17. – С. 37–45.

15. *Маркелов Н.К.* Нижняя оценка сложности функций трехзначной логики в классе поляризованных полиномов // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем и кибернетика. – 2012. – № 3. – С. 40–45.

16. *Селезнева С.Н.* О сложности k-значных функций в одном классе полиномов // Проблемы теоретической кибернетики: Материалы XVI Междунар. конф. – Н. Новгород, 2011. – С. 430–434.

17. *Балюк А.С.* О верхней оценке сложности задания квазиполиномами функций над конечными полями //Изв. Иркут. гос. ун-та. Сер.«Математика». – 2014. – № 10. – С. 3–12.

18. *Балюк А.С.* Методы получения оценок сложности кронекеровых форм функций над конечными полями // Труды X Междунар. конф. «Дискретные модели в теории управляющих систем». – Москва и Подмосковье, 2018. – С. 46–49.

19. *Цирлер Н.* Линейные возвратные последовательности // Кибернетический сб. – М.: Изд-во иностр. лит., 1963. – Вып. 6. – С. 55–79.

Поступила в редакцию
18.08.2020

Балюк Александр Сергеевич, кандидат физико-математических наук, доцент Института математики и информационных технологий

Иркутский государственный университет
ул. Карла Маркса, д. 1, г. Иркутск, 664003, Россия

E-mail: *sacha@hotmail.ru*

ISSN 2541-7746 (Print)
ISSN 2500-2198 (Online)

**UCHENYE ZAPISKI KAZANSKOGO UNIVERSITETA.
SERIYA FIZIKO-MATEMATICHESKIE NAUKI
(Proceedings of Kazan University. Physics and Mathematics Series)**

2020, vol. 162, no. 3, pp. 285–299

doi: 10.26907/2541-7746.2020.3.285-299

The Complexity of Pseudo-Kronecker and Free-Kronecker Forms of Functions over Finite Fields

A.S. Baliuk

Irkutsk State University, Irkutsk, 664003 Russia
E-mail: *sacha@hotmail.ru*

Received August 18, 2020

Abstract

An approach enabling partial generalization of the Green–Sasao hierarchy for polynomial forms of Boolean functions to the case of an arbitrary finite field was introduced.

The exact value of the Shannon function was obtained for the class of pseudo-Kroneker and free-Kronecker forms of n-ary functions over an arbitrary finite field $\mathbb{F}_q$. The value found is equal to q^{n-1}. The previously known result for Boolean functions was generalized.

Keywords: finite field, computational complexity, free-Kronecker forms, pseudo-Kronecker forms

Acknowledgments. The study was supported by the Russian Foundation for Basic Research (project no. 19-01-00200).

Figure Captions

Fig. 1. Computation of the function as illustrated by the complete ternary tree with depth 2.

References

1. Green D.H. Families of Reed-Muller canonical forms. *Int. J. Electron.*, 1991, vol. 70, no. 2, pp. 259–280. doi: 10.1080/00207219108921277.
2. Sasao T. Representations of logic functions using EXOR operators. In: *Representations of Discrete Functions*. Boston, Kluwer Acad. Publ., 1996, pp. 29–54. doi: 10.1007/978-1-4613-1385-4_2.
3. Ho P., Perkowski M. Free Kronecker decision diagrams and their application to Atmel 6000 series FPGA mapping. *Proc. Conf. on European Design Automation*. Grenoble, France, 1994, pp. 8–13. doi: 10.1145/198174.198180.
4. Al-Rabadi A.N. An extended Green-Sasao hierarchy of canonical ternary Galois forms and Universal Logic Modules. *Facta Univ., Ser.: Electron. Energ.*, 2017, vol. 30, no. 1, pp. 49–66. doi: 10.1080/00207219108921277.
5. *Izbrannye voprosy teorii bulevykh funktsii* [Selected Problems in the Theory of Boolean Functions]. Vinokurov S.F., Peryazev N.A. (Eds.). Moscow, Fizmatlit, 2001. 192 p. (In Russian)

6. Baliuk A.S., Vinokurov S.F. The Shannon function for some classes of operator polynomial forms. *Optim., Upr., Intellekt*, 2000, vol. 5, no. 1, pp. 111–121. (In Russian)

7. Baliuk A.S., Zinchenko A.S. Lower bounds of complexity for polarized polynomials over finite fields. *Sib. Math. J.*, 2019, vol. 60, no. 1, pp. 1–9. doi: 10.1134/S0037446619010014.

8. Mullen G.L., Panarino D. *Handbook of Finite Fields*. New York, Chapman and Hall/CRC, 2013. 1068 p. doi: 10.1201/b15006.

9. Baluck A.S., Vinokurov S.F. Classes of operator forms. *Proc. 5th Int. Workshop on Boolean Problems*. Freiberg, Germany, 2002, pp. 76–83.

10. Peryazev N.A. Complexity of Boolean functions in the class of polarized polynomial forms. *Algebra Logic*, 1995, vol. 34, no. 3, pp. 177–179. doi: 10.1007/BF02341875.

11. Selezneva S.N. On the complexity of the representation of functions of many-valued logics by polarized polynomials. *Discrete Math. Appl.*, 2002, vol. 12, no. 3, pp. 229–234.

12. Alekseev V.B., Voronenko A.A., Selezneva S.N. On the complexity of realization of functions of a k-valued logic with polarized polynomials. *Trudy V Mezhdunar. konferentsii "Diskretnye modeli v teorii upravlyayushchikh sistem"* [Poc. 5th Int. Conf. "Discrete Models in Theory of Control Systems"]. Ratmino, 2003, pp. 8–9. (In Russian)

13. Baliuk A.S., Yanushkovsky G.V. Upper bounds of the complexity of functions over finite fields in some classes of Kroneker forms. *Izv. Irkutsk. Gos. Univ. Ser. "Mat."*, 2015, no. 14, pp. 3–17. (In Russian)

14. Kazimirov A.S., Reymerov S.Yu. On upper bounds of the complexity of functions over non-prime finite fields in some classes of polarized polynomials. *Izv. Irkutsk. Gos. Univ. Ser. "Mat.'*, 2016, no. 17, pp. 37–45. (In Russian)

15. Markelov N.K. A lower estimate of the complexity of three-valued logic functions in the class of polarized polynomials. *Moscow Univ. Comput. Math. Cybern.*, 2012, vol. 36, no. 3, pp. 150–154. doi: 10.3103/S0278641912030041.

16. Selezneva S.N. On the complexity of k-valued functions in a class of polynomials. *Problemy teoreticheskoi kibernetiki: Materialy XVI Mezhdunar. konf.* [Problems of Theoretical Cybernetics: Proc. XVI Int. Conf.]. Nizhny Novgorod, 2011, pp. 430–434. (In Russian)

17. Baliuk A.S. On upper bound of the complexity of quasi polynomial representations of functions over finite fields. *Izv. Irkutsk. Gos. Univ. Ser. "Mat."*, 2014, no. 10, pp. 3–12. (In Russian)

18. Baliuk A.S. Methods for assessing the complexity of Kronecker forms of functions over finite fields. *Trudy X Mezhdunar. konf. "Diskretnye modeli v teorii upravlyayushchikh sistem"* [Proc. X Int. Conf. "Discrete Models in the Theory of Control Systems"]. Moscow and Moscow Region, 2018, pp. 46–49. (In Russian)

19. Zierler N. Linear recurring sequences. *J. Soc. Ind. Appl. Math.*, 1959, vol. 7, no. 1, pp. 31–48. doi: 10.1137/0107003.

⟨ ***Для цитирования:*** *Балюк А.С.* Сложность псевдокронекеровых и свободно кронекеровых форм функций над конечными полями // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки. – 2020. – Т. 162, кн. 3. – С. 285–299. – doi: 10.26907/2541-7746.2020.3.285-299. ⟩

⟨ ***For citation:*** Baliuk A.S. The complexity of pseudo-Kronecker and free-Kronecker forms of functions over finite fields. *Uchenye Zapiski Kazanskogo Universiteta. Seriya Fiziko-Matematicheskie Nauki*, 2020, vol. 162, no. 3, pp. 285–299. doi: 10.26907/2541-7746.2020.3.285-299. (In Russian) ⟩