причём в одной ветви может встретиться только один симметричный многочлен одной степени.

В результате исследования поликвадратичного расширения полей посредством операции A получены следующие свойства этого расширения.

1. Посредством поликвадратичного расширения можно вычислять характеристический многочлен элемента не только из расширенного поля, но и из расширяемого, т. е. движение по дереву возможно как вверх, так и вниз. Для того чтобы «опуститься» по дереву вниз, необходимо применить операцию A, а чтобы «подняться» по дереву вверх — выполнить обратную операцию $\Lambda = A^{-1}$.

2. Для вычисления расширений необходимо вычислить относительный след корня и записать уравнение, задающееся неприводимым многочленом, коэффициенты которого вычисляются в явном виде [3, 4].

Теорема 1. Если $h(x) = z$, $\deg f = n$, $f(z) = 0$, $\deg g = 2n$, $g(z) = 0$, то $\mathrm{Tr}(z) = \mathrm{Tr}(x)$, где $h(x) = x + x^{-1}$ равен относительному следу элемента x.

Теорема 2. Если в поле $\mathrm{GF}(2^m)$, $m > 1$, z — корень симметричного многочлена f, то однозначно определён периодический многочлен g, где $y = 1/(z + 1)$ — его корень. И наоборот, если g — периодический, то f — симметричный, где $z = 1/y + 1$.

Таким образом, с помощью операции A построено полное бинарное дерево неприводимых многочленов степени 2^n. Изученные в работе свойства такого поликвадратичного расширения значительно упрощают процедуру генерации многочленов и дают возможность избежать полного перебора при поиске многочленов больших степеней, что имеет особое значение для криптографии и теории кодирования.

ЛИТЕРАТУРА

1. Информационные технологии и безопасность алгоритмы разделения секрета. Предварительный государственный стандарт республики Беларусь СТБ П 34.101.44. Минск: Госстандарт, 2011.
2. *Глуско Кр. Л., Титов С. С.* Арифметический алгоритм решения квадратных уравнений в конечных полях характеристики два // Доклады ТУСУРа. 2012. №1(25). Ч. 2. С. 148–152.
3. *Болотов А. А., Гашков С. Б., Фролов А. Б.* Элементарное введение в эллиптическую криптографию: алгебраические и алгоритмические основы. М.: КомКнига, 2006.
4. *Болотов А. А., Гашков С. Б., Фролов А. Б.* Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых. М.: КомКнига, 2006.
5. *Лидл Р., Нидеррайтер Г.* Конечные поля. М.: Мир, 1988.
6. *Геут Кр. Л., Титов С. С.* О свойствах поликвадратичных расширений бинарных полей // Проблемы теоретической и прикладной математики: Труды 44-й Всерос. молодежной конф. Екатеринбург: УрО РАН, 2013. С. 17–19.

УДК 512.55

КЛАССЫ ПОЛИНОМИАЛЬНЫХ И ВАРИАЦИОННО-КООРДИНАТНО ПОЛИНОМИАЛЬНЫХ ФУНКЦИЙ НАД КОЛЬЦОМ ГАЛУА

М. В. Заец

Рассматривается новый класс функций над кольцом Галуа $R = \mathrm{GR}(q^m, p^m)$, получивший название класса функций с вариационно-координатной полиномиальностью (ВКП-функций). Рассматривается соотношение между данным классом и

классом полиномиальных функций над R, даётся верхняя оценка его мощности, а также достаточные условия отсутствия полиномиального представления ВКП-функции.

Ключевые слова: *полиномиальные функции, кольцо Галуа, координатное множество, ВКП-функции.*

Кольцом Галуа называется конечное коммутативное локальное кольцо $R = \mathrm{GR}(q^m, p^m)$, нильрадикал $J(R)$ которого имеет вид pR, где $p = \mathrm{char}\,\bar{R}$ и $\bar{R} = R/J(R) = \mathrm{GF}(q)$ — поле вычетов данного кольца [1]. При этом $\mathrm{char}\,R = p^m$, $|R| = q^m$ и $m = \mathrm{ind}\,J(R)$, $m \in \mathbb{N}$, — индекс нильпотентности нильрадикала $J(R)$. Подмножество $\mathcal{B} = \{b_0 = 0, \ldots, b_{q-1}\} \subseteq R$ называется координатным множеством кольца R, если его элементы образуют полную систему вычетов по нильрадикалу $J(R)$. В таком случае любой элемент $a \in R$ однозначно представляется в виде

$$a = a^{(0)} + p \cdot a^{(1)} + \cdots + p^{m-1} \cdot a^{(m-1)},\ a^{(i)} \in \mathcal{B},\ i = 0, \ldots, m-1,$$

называемом разложением элемента a в координатном множестве $\mathcal{B}$. Функции $\gamma_i^{\mathcal{B}}\colon R \to \mathcal{B}$, определяемые по правилу $\gamma_i^{\mathcal{B}}(a) = a^{(i)}$, $i = 0, \ldots, m-1$, называются координатными функциями в координатном множестве $\mathcal{B}$, а элементы $a^{(i)} = \gamma_i^{\mathcal{B}}(a)$ — координатами элемента a в координатном множестве $\mathcal{B}$.

Обозначим через $\mathcal{P}_R(n)$ класс всех полиномиальных функций от n переменных над кольцом Галуа $R = \mathrm{GR}(q^m, p^m)$. Следующее определение и результаты обобщают полученные ранее в [2] для случая примарного кольца вычетов $\mathbb{Z}_{2^m}$.

Определение 1. Функцию $f(x)\colon R^n \to R$, $R = \mathrm{GR}(q^m, p^m)$, $m > 1$, назовём *ВКП-функцией* в координатном множестве $\mathcal{B}$, если для любого $i \in \{0, \ldots, m-1\}$ существует полиномиальная функция $p_i(x) \in \mathcal{P}_R(n)$, такая, что $\gamma_i^{\mathcal{B}}(f(\alpha)) = \gamma_i^{\mathcal{B}}(p_i(\alpha))$ при всех $\alpha \in R^n$. При этом многочлен $p_i(x)$, $i = 0, \ldots, m-1$, будем называть i-м координатным многочленом функции $f(x)$.

Класс всех ВКП-функций от n переменных над кольцом R в координатном множестве $\mathcal{B}$ обозначим через $\mathcal{CP}_R^{\mathcal{B}}(n)$. Следующая теорема устанавливает соотношение между введённым классом и классом полиномиальных функций над тем же кольцом.

Теорема 1. Справедливы утверждения:

1) если $R = GR(q^2, p^2)$, то $\mathcal{P}_R(n) = \mathcal{CP}_R^{\mathcal{B}}(n)$;
2) если $R = GR(q^m, p^m)$, $m \geqslant 3$, то $\mathcal{P}_R(n) \subsetneq \mathcal{CP}_R^{\mathcal{B}}(n)$.

Пусть $f(x) \in R[x]$. Обозначим $\mathrm{grad}\,f(x) = \left(\dfrac{\partial f}{\partial x_1}(x), \ldots, \dfrac{\partial f}{\partial x_n}(x)\right)$, где $\dfrac{\partial f}{\partial x_i}(x)$ — формальная частная производная многочлена $f(x)$ по переменной x_i, $i = 1, \ldots, n$. Приведём достаточное условие того, что при $m \geqslant 3$ ВКП-функция не имеет полиномиального представления над R.

Теорема 2. Пусть $f(x) \in \mathcal{CP}_R^{\mathcal{B}}(n)$, $m \geqslant 3$ и для координатных многочленов $p_i(x)$, $p_j(x)$, $i, j \in \{1, \ldots, m-1\}$, $i \neq j$, существует $\alpha \in \mathcal{B}^n$, такое, что

$$\mathrm{grad}\,p_i(\alpha) \not\equiv \mathrm{grad}\,p_j(\alpha) \pmod{J(R)}.$$

Тогда $f(x) \notin \mathcal{P}_R(n)$.

Теорема 3. Справедлива следующая оценка мощности класса $\mathcal{CP}_R^{\mathcal{B}}(n)$:

$$|\mathcal{CP}_R^{\mathcal{B}}(n)| \leqslant q^{q^n + (m-1)n \cdot q^n + q^n \cdot (q^{n(m-1)}-1)/(q^n-1)},$$

при этом если $m = 2$, то в неравенстве достигается равенство.

Класс ВКП-функций во многом обобщает класс полиномиальных функций. В частности, можно показать, что системы уравнений, левые части которых являются такими функциями, могут быть решены методом покоординатной линеаризации, предложенным в работе [3] для полиномиальных функций над кольцом Галуа — Эйзенштейна.

ЛИТЕРАТУРА

1. *Елизаров В. П.* Конечные кольца. М.: Гелиос-АРВ, 2006.
2. *Заец М. В., Никонов В. Г., Шишков А. Б.* Функции с вариационно-координатной полиномиальностью и их свойства // Открытое образование. 2012. № 3. С. 57–61.
3. *Михайлов Д. А., Нечаев А. А.* Решение системы полиномиальных уравнений над кольцом Галуа — Эйзенштейна с помощью канонической системы образующих полиномиального идеала // Дискретная математика. 2004. № 1. Вып. 1. С. 21–51.

УДК 519.7

ОБ АФФИННОСТИ БУЛЕВЫХ ФУНКЦИЙ НА ПОДПРОСТРАНСТВАХ И ИХ СДВИГАХ[1]

Н. А. Коломеец

Пусть f — булева функция от n переменных и для любого аффинного подпространства L размерности $\lceil n/2 \rceil$ функция f аффинна на L тогда и только тогда, когда f аффинна на любом сдвиге L. Доказано, что тогда либо степень f не превышает 2, либо не существует ни одного аффинного подпространства размерности $\lceil n/2 \rceil$, на котором f аффинна.

Ключевые слова: *булевы функции, бент-функции, квадратичные функции.*

Рассматривается свойство булевых функций, связанное с их аффинностью на аффинных подпространствах.

Введём необходимые определения. Отображение $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ называется *булевой функцией* от n переменных. *Алгебраической степенью* или просто *степенью* булевой функции называется степень её алгебраической нормальной формы (полинома Жегалкина). Булева функция называется *аффинной*, если её алгебраическая степень не больше 1, и *квадратичной*, если её степень равна 2. Множество $U \subseteq \mathbb{Z}_2^n$ называется *аффинным подпространством*, если $U = a \oplus L$, где $a \in \mathbb{Z}_2^n$ и L является линейным подпространством в $\mathbb{Z}_2^n$. Будем называть U сдвигом подпространства L. Через Ind_D обозначим характеристическую функцию множества $D \subseteq \mathbb{Z}_2^n$. Через $\langle u, v \rangle$ обозначим скалярное произведение векторов u и v. Булева функция f от n переменных *аффинна на множестве* $D \subseteq \mathbb{Z}_2^n$, если существуют $a \in \mathbb{Z}_2^n$, $c \in \mathbb{Z}_2$, такие, что для любого $x \in D$ верно $f(x) = \langle a, x \rangle \oplus c$. Под *расстоянием* между двумя булевыми функциями подразумевается *расстояние Хэмминга* между их векторами значений.

Все квадратичные булевы функции обладают следующим свойством.

Утверждение 1. Пусть f — квадратичная булева функция от n переменных. Тогда для любого аффинного подпространства L функция f аффинна на L, если и только если f аффинна на любом сдвиге L.

Доказательство утверждения следует из неравенства $\deg(f(x) \oplus f(x \oplus s)) \leqslant 1$, верного для любого $s \in \mathbb{Z}_2^n$.

[1]Исследование выполнено при поддержке РФФИ (проект № 12-01-31097).