Таблица 2

n	Кол-во EA-классов	Кол-во аффинных функций A: $F + A \in \mathcal{DE}_F$
2	1	2^4
3	1	2^6
4	1	2^{10}
5	2	Для обоих классов: 2^{10}
6	13	Для одного класса: 2^{13}; для остальных 12 классов: 2^{12}
7	$\geqslant 487$	Для всех известных 487 классов: 2^{14}
8	$\geqslant 8179$	Для одного класса из известных 8179: 2^{20}; для остальных 8178 классов: 2^{16}

ЛИТЕРАТУРА

1. *Тужилин М. Э.* Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. №3. С. 14–20.
2. *Pott A.* Almost perfect and planar functions // Des. Codes Cryptogr. 2016. V. 78. P. 141–195.
3. *Carlet C.* Open questions on nonlinearity and on APN functions // Arithmetic of Finite Fields. LNCS. 2015. V. 9061. P. 83–107.
4. *Глухов М. М.* О матрицах переходов разностей при использовании некоторых модулярных групп // Матем. вопр. криптограф. 2013. Т. 4. №4. С. 27–47.
5. *Сачков В. Н.* Комбинаторные свойства дифференциально 2-равномерных подстановок // Матем. вопр. криптограф. 2015. Т. 6. №1. С. 159–179.
6. *Городилова А. А.* О пересечении множеств значений производных APN-функций // Прикладная дискретная математика. Приложение. 2015. №8. С. 25–27.

УДК 512.542.3 DOI 10.17223/2226308X/9/9

ФУНКЦИИ С ВАРИАЦИОННО-КООРДИНАТНОЙ ПОЛИНОМИАЛЬНОСТЬЮ НАД ГРУППОЙ

А. И. Зуева, А. В. Карпов

Определён класс функций с вариационно-координатной полиномиальностью над группой, являющийся обобщением класса ВКП-функций над примарным кольцом вычетов. Представлен алгоритм нахождения координат для элемента группы. Доказано, что класс ВКП-функций над $UT_n(\mathbb{Z}_p)$ не совпадает с классом полиномиальных функций. Указан способ обращения биективной ВКП-функции над $UT_n(\mathbb{Z}_p)$.

Ключевые слова: *функции над группой, функции с вариационно-координатной полиномиальностью, координатные функции.*

В [1] определён класс функций с вариационно-координатной полиномиальностью (ВКП-функций) над примарным кольцом вычетов, порождающий системы ВКП-уравнений, для решения которых применим метод покоординатной линеаризации.

В данной работе делается обобщение класса ВКП-функций на случай, когда полиномы рассматриваются над группой с нормальным рядом. Получающийся при этом класс ВКП-функций над группой даёт конструктивный пример дифференцируемых функций над группой, рассмотренных в [2].

Пусть задана группа $\mathbb{G}$ с нормальным рядом $\mathbb{G} = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_n = e$. Как и в случае примарного кольца вычетов, для определения класса ВКП-функций над группой необходимо определить понятие координатной функции полинома над группой.

Определение 1. *Полиномом* над группой $\mathbb{G}$ от переменной x будем называть выражение вида $p(x) = g_1 x^{\varepsilon_1} g_2 x^{\varepsilon_2} \ldots g_m x^{\varepsilon_m}$, где все «коэффициенты» g_i — элементы группы $\mathbb{G}$, а экспоненты ε_i принимают значения 1 либо -1.

Каждый полином индуцирует функцию на $\mathbb{G}$ по следующему правилу:

$$p(g) = g_1 g^{\varepsilon_1} g_2 g^{\varepsilon_2} \ldots g_m g^{\varepsilon_m}.$$

Определение 2. Функцию $p : \mathbb{G} \to \mathbb{G}$ будем называть *полиномиальной*, если она индуцирована некоторым полиномом над $\mathbb{G}$.

Определение 3. Для $k \in \{0, \ldots, n-1\}$ будем называть функции $\gamma_k : \mathbb{G} \to H_k$ *координатными функциями группы* $\mathbb{G}$ *относительно нормального ряда*, если произвольный элемент $g \in \mathbb{G}$ однозначно представляется в виде произведения

$$g = \gamma_0(g)\gamma_1(g) \cdots \gamma_{n-1}(g).$$

Элемент $g^{(k)}$ подгруппы H_k, равный $g^{(k)} = \gamma_k(g)$, будем называть *k-й координатой* элемента g. Если задана функция $f : \mathbb{G} \to \mathbb{G}$, то *$k$-й координатной функцией* функции f будем называть отображение $\gamma_k f : \mathbb{G} \to H_k$, определяемое по правилу $\gamma_k f(g) = \gamma_k(f(g))$.

Координаты элемента группы определяются способом выбора представителей в факторах ряда и могут быть найдены с помощью алгоритма 1.

Алгоритм 1. Нахождение координат элемента группы

Вход: группа $\mathbb{G} = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_n = e$ с нормальным рядом, элемент $g \in \mathbb{G}$, функции выбора представителей в факторах ряда $s_0, \ldots, s_{n-2}$ $(s_i : H_i/H_{i+1} \to H_i)$

Выход: набор координат $(\gamma_0(g), \ldots, \gamma_{n-1}(g))$, $\gamma_i(g) \in H_i$ и $g = \gamma_0(g) \cdots \gamma_{n-1}(g)$

1: **Для всех** i от 0 до $n-2$
2: $\quad \overline{g} := gH_{i+1}$, $\gamma_i(g) := s_i(\overline{g})$
3: $\quad g := \gamma_i(g)^{-1} g$
4: $\gamma_{n-1}(g) := g$, конец

Определение 4. Функцию $f : \mathbb{G} \to \mathbb{G}$ будем называть ВКП-функцией, если существуют полиномы $p_0, \ldots, p_{n-1}$, такие, что для произвольных $g \in \mathbb{G}$, $k \in \{0, \ldots, n-1\}$ выполняется

$$\gamma_k f(g) = \gamma_k p_k(g).$$

Как видно из определения, класс ВКП-функций над группой определяется нормальным рядом в группе, способом выбора представителей в факторах ряда и тем, как понимать термин полинома над группой. Например, можно отказаться от требования полиномиальности либо рассматривать иначе определённые (например, так, как в [3]) полиномы. Далее полиномы понимаются в смысле определения 1.

С практической точки зрения наибольший интерес представляют конечные группы. Известно, что конечные нильпотентные группы (интересующие нас, как относительно простые некоммутативные группы) исчерпываются прямыми произведениями конечных p-групп, каждая из которых, в свою очередь, изоморфно вкладывается в $UT_n(\mathbb{Z}_p)$ [4]. Поэтому в качестве основной интерпретации будем рассматривать группу унитреугольных матриц $UT_n(\mathbb{Z}_p)$ с центральным рядом

$$UT_n(\mathbb{Z}_p) = UT_n^1(\mathbb{Z}_p) \trianglerighteq UT_n^2(\mathbb{Z}_p) \trianglerighteq \cdots \trianglerighteq UT_n^n(\mathbb{Z}_p) = e,$$

где $n \geqslant 3$ и $UT_n^i(\mathbb{Z}_p)$ — подгруппа, состоящая из унитреугольных матриц с $i-1$ нулевыми диагоналями над главной.

Очевидно, что класс ВКП-функций над произвольной группой включает в себя класс полиномиальных функций. Обратное включение не выполняется.

Теорема 1. Пусть $\mathbb{G} = UT_n(\mathbb{Z}_p)$ и $n \geqslant 3$. Тогда класс ВКП-функций над $\mathbb{G}$ не совпадает с классом полиномиальных функций.

Следующие теоремы дают критерий биективности ВКП-функции и формулу обращения биективной ВКП-функции над $UT_n(\mathbb{Z}_p)$.

Теорема 2. Пусть $\mathbb{G} = UT_n(\mathbb{Z}_p)$; $f : \mathbb{G} \to \mathbb{G}$ — ВКП-функция, заданная полиномами $p_0, \ldots, p_{n-2}$. Тогда f биективна на $\mathbb{G}$, если и только если выполняются следующие два условия:

1) p_0 биективен по модулю $UT_n^2(\mathbb{Z}_p)$;
2) степени полиномов $p_0, \ldots, p_{n-2}$ взаимно просты с p.

Теорема 3. Пусть $\mathbb{G} = UT_n(\mathbb{Z}_p)$; $f : \mathbb{G} \to \mathbb{G}$ — биективная ВКП-функция, заданная полиномами $p_0, \ldots, p_{n-2}$; $k \in \{2, \ldots, n-1\}$; v_k — обратная в смысле композиции ВКП-функция к f по модулю $UT_n^k(\mathbb{Z}_p)$. Тогда обратной к f по модулю $UT_n^{k+1}(\mathbb{Z}_p)$ является функция

$$v_{k+1}(x) = v_k(x)(x^{-1}f(v_k(x)))^{-m},$$

где $m = \deg(p_{k-1})^{-1} \pmod p$.

Рассмотрим группу $\mathbb{G} = UT_3(\mathbb{Z}_3)$ с функцией $s_0 : UT_3(\mathbb{Z}_3)/UT_3^2(\mathbb{Z}_3) \to UT_3(\mathbb{Z}_3)$, выбирающей в качестве представителя смежного класса матрицу с нулевой верхней клеткой. Тогда, например, $\gamma_0\left(\begin{pmatrix}1&2&2\\0&1&1\\0&0&1\end{pmatrix}\right) = \begin{pmatrix}1&2&0\\0&1&1\\0&0&1\end{pmatrix}$, $\gamma_1\left(\begin{pmatrix}1&2&2\\0&1&1\\0&0&1\end{pmatrix}\right) = \begin{pmatrix}1&0&2\\0&1&0\\0&0&1\end{pmatrix}$.

Построим следующие полиномы:

$$p_0(x) = \begin{pmatrix}1&1&1\\0&1&2\\0&0&1\end{pmatrix} x \begin{pmatrix}1&0&2\\0&1&2\\0&0&1\end{pmatrix} x^{-1} \begin{pmatrix}1&1&1\\0&1&0\\0&0&1\end{pmatrix} x, \quad p_1(x) = \begin{pmatrix}1&1&2\\0&1&2\\0&0&1\end{pmatrix} x \begin{pmatrix}1&0&2\\0&1&2\\0&0&1\end{pmatrix} x.$$

Занумеруем матрицы из $UT_3(\mathbb{Z}_3)$ следующим образом:

$$I\left(\begin{pmatrix}1&a_1&a_3\\0&1&a_2\\0&0&1\end{pmatrix}\right) = 1 + a_1 + 3a_2 + 9a_3.$$

Тогда построенные полиномы индуцируют следующие перестановки номеров:

$$p_0 : (1,6,8)(2,22,18)(3,14,25)(4,27,11)(5,16,21)(7,12,23)(9,20,13)(10,15,17)(19,24,26),$$

$$p_1 : (1,5,19,14,10,23)(2,22)(3,15,12,6,21,24)(4,20)(7,17,16,8,25,26)(11,13)(18,27).$$

Построим по p_0 и p_1 ВКП-функцию $f(x) = \gamma_0 p_0(x) \gamma_1 p_1(x)$:

$$f : (1,6,26)(2,22,9)(3,14,16)(4,27,11,13,18,20)(5,25,21,23,7,12)(8,19,15,17,10,24).$$

В качестве обратной к f по модулю $UT_3^2(\mathbb{Z}_3)$ возьмём функцию, индуцированную полиномом $p(x) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} x$. Степень p_1 равна 2, значит, $m = 2$ и обратная перестановка к f получается как $g(x) = p(x)(x^{-1}f(p(x)))^{-2}$:

$$g : (1, 26, 6)(2, 9, 22)(3, 16, 14)(4, 20, 18, 13, 11, 27)(5, 12, 7, 23, 21, 25)(8, 24, 10, 17, 15, 19).$$

Таким образом, при фиксированных нормальном ряде в группе и способе выбора представителей в факторах этого ряда определён класс ВКП-функций над группой. Функции класса задаются набором полиномов и получаются как произведение их координатных функций. Класс ВКП-функций над $UT_n(\mathbb{Z}_p)$ не совпадает с классом полиномиальных функций над $UT_n(\mathbb{Z}_p)$ (теорема 1). К ВКП-функциям применимы критерий биективности и формулы обращения дифференцируемых функций, которые в случае $\mathbb{G} = UT_n(\mathbb{Z}_p)$ принимают вид теорем 2 и 3 соответственно.

ЛИТЕРАТУРА

1. *Заец М. В.* О классе вариационно-координатно-полиномиальных функций над примарным кольцом вычетов // Прикладная дискретная математика. 2014. №3. С. 12–27.
2. *Карпов А. В.* Обращение дифференцируемых перестановок над группой // Прикладная дискретная математика. Приложение. 2015. №8. С. 30–33.
3. *Anashin V. S.* Solvable groups with operators and commutative rings having transitive polynomials // Algebra. Logika. 1982. No. 21(6). С. 627–646.
4. *Меньшов А. В.* Асимптотические свойства рациональных множеств и систем уравнений в свободных абелевых группах и разрешимость регулярных уравнений в классе нильпотентных групп: дис. … канд. физ.-мат. наук. Омск, 2014.

УДК 519.7 DOI 10.17223/2226308X/9/10

О РАССТОЯНИИ ХЭММИНГА МЕЖДУ ДВУМЯ БЕНТ-ФУНКЦИЯМИ[1]

Н. А. Коломеец

Рассматривается расстояние Хэмминга между двумя бент-функциями. С использованием конструкции бент-функций на минимальном расстоянии друг от друга получен ряд возможных значений расстояния. Найдены всевозможные значения расстояния между бент-функциями из класса Мэйорана — МакФарланда.

Ключевые слова: *булевы функции, бент-функции, расстояние Хэмминга.*

Булевой функцией от n переменных называется отображение вида $f : \mathbb{F}_2^n \to \mathbb{F}_2$. *Расстоянием Хэмминга* $\mathrm{dist}(f, g)$ между двумя булевыми функциями f и g от n переменных называется количество значений аргументов, на которых значения функций различаются. Функция вида $\langle a, x\rangle \oplus c$, где $a \in \mathbb{F}_2^n$, $c \in \mathbb{F}_2$ и $\langle a, x\rangle = a_1x_1 \oplus a_2x_2 \oplus \ldots \oplus a_nx_n$, называется *аффинной* булевой функцией. *Бент-функциями* называются булевы функции от чётного числа переменных, находящиеся на максимально возможном расстоянии от множества всех аффинных функций. Они предложены О. Ротхаусом [1]. Бент-функции имеют приложения в алгебре, комбинаторике, теории кодирования, криптографии [2]. Обозначим через $\mathcal{B}_{2k}$ множество всех бент-функций от $2k$ переменных.

[1]Работа поддержана грантом РФФИ, проект №15-07-01328.