

УДК 519.716.32+519.854

DOI 10.17223/2226308X/10/5

РАЗРЯДНО-ПОЛИНОМИАЛЬНОЕ ПОСТРОЕНИЕ ПОДСТАНОВОК НАД КОЛЬЦОМ ГАЛУА

М. В. Заец

Рассматривается новый способ построения подстановок над кольцом Галуа, использующий функции с вариационно-разрядной полиномиальностью. Класс функций с вариационно-разрядной полиномиальностью над различными кольцами определялся ранее автором. Особенность данного класса в том, что он содержит класс полиномиальных функций и при определённых условиях не совпадает с ним. В данной работе обобщаются критерий биективности полиномиальной вектор-функции и критерий подстановочности полиномиальной функции. Представленные результаты позволяют, в частности, строить неполиномиальные n -квазигруппы.

Ключевые слова: подстановки, n -квазигруппы, биективные вектор-функции, функции с вариационно-разрядной полиномиальностью, разрядное множество, кольцо Галуа.

Кольцом Галуа называется конечное коммутативное локальное кольцо $R = \text{GR}(q^m, p^m)$, нильрадикал $J(R)$ которого имеет вид pR , где $p = \text{char } \bar{R}$ и $\bar{R} = R/J(R) = \text{GF}(q)$ — поле вычетов данного кольца [1]. При этом $\text{char } R = p^m$, $|R| = q^m$ и $m = \text{ind } J(R)$, $m \in \mathbb{N}$, — индекс нильпотентности нильрадикала $J(R)$. Подмножество $\mathcal{B} = \{b_0 = 0, \dots, b_{q-1}\} \subseteq R$ называется разрядным 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

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

называемом разложением элемента a в разрядном множестве $\mathcal{B}$. Функции $\kappa_i^{\mathcal{B}}: R \rightarrow \mathcal{B}$, определяемые по правилу $\kappa_i^{\mathcal{B}}(a) = a^{(i)}$, $i = 0, \dots, m-1$, называются разрядными функциями в разрядном множестве $\mathcal{B}$, а элементы $a^{(i)} = \kappa_i^{\mathcal{B}}(a)$ — разрядами i -го порядка элемента a в разрядном множестве $\mathcal{B}$.

Обозначим через $\mathcal{P}_R(n)$ класс всех полиномиальных функций от n переменных над кольцом Галуа $R = \text{GR}(q^m, p^m)$.

Определение 1. Функцию $f(\mathbf{x}): R^n \rightarrow R$, $R = \text{GR}(q^m, p^m)$, $m > 1$, назовём вариационно-разрядно полиномиальной (ВРП-функцией) в разрядном множестве $\mathcal{B}$, если для любого $i \in \{0, \dots, m-1\}$ существует полиномиальная функция $p_i(\mathbf{x}) \in \mathcal{P}_R(n)$, такая, что $\kappa_i^{\mathcal{B}}(f(\alpha)) = \kappa_i^{\mathcal{B}}(p_i(\alpha))$ при всех $\alpha \in R^n$. При этом многочлен $p_i(\mathbf{x})$, $i = 0, \dots, m-1$, будем называть i -м разрядным многочленом функции $f(\mathbf{x})$.

Класс всех ВРП-функций от n переменных над кольцом R в разрядном множестве $\mathcal{B}$ обозначим через $\mathcal{DP}_R^{\mathcal{B}}(n)$. Свойства данного класса над различными кольцами описаны автором в [2–4]. В частности, имеет место следующая

Теорема 1. Справедливы утверждения:

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

Пусть $f(\mathbf{x}) \in R[\mathbf{x}]$, обозначим $\text{grad } f(\mathbf{x}) = \left(\frac{\partial f}{\partial x_1}(\mathbf{x}), \dots, \frac{\partial f}{\partial x_n}(\mathbf{x}) \right)$, где $\frac{\partial f}{\partial x_i}(\mathbf{x})$ — формальная частная производная многочлена $f(\mathbf{x})$ по переменной x_i , $i = 1, \dots, n$. Если

$f_1(\mathbf{x}), \dots, f_t(\mathbf{x}) \in R[\mathbf{x}]$, то матрица $J_{f_1, \dots, f_t}(\mathbf{x}) = \begin{pmatrix} \text{grad } f_1(\mathbf{x}) \\ \vdots \\ \text{grad } f_t(\mathbf{x}) \end{pmatrix}$ называется матрицей

Якоби системы многочленов, а её определитель (при $t = n$) $|J_{f_1, \dots, f_n}(\mathbf{x})|$ — якобианом. Следующая теорема обобщает известный из [5] результат о биективности полиномиальной вектор-функции, а также результат о биективности ВРП-вектор-функции, полученный ранее автором в [6], со случая примарного кольца вычетов и p -ичного разрядного множества на случай произвольного кольца Галуа и его разрядного множества.

Теорема 2. Вектор-функция $F(\mathbf{x}) = (f_1(\mathbf{x}), \dots, f_n(\mathbf{x})) : R^n \rightarrow R^n$, где $f_i \in \mathcal{DP}_R^{\mathcal{B}}(n)$, является биекцией тогда и только тогда, когда одновременно выполняются следующие условия:

- 1) $(p_{01}(\mathbf{x}^{(0)}), \dots, p_{0n}(\mathbf{x}^{(0)})) \pmod{J(R)} : \mathcal{B}^n \rightarrow \mathcal{B}^n$ является биекцией;
- 2) для любого $j = 1, \dots, m-1$ якобиан $|J_{p_{j1}, \dots, p_{jn}}(\mathbf{x}^{(0)})| \not\equiv 0 \pmod{J(R)}$ при всех $\mathbf{x}^{(0)} \in \mathcal{B}^n$,

где $p_{ji}(\mathbf{x})$ — j -й разрядный многочлен функции $f_i(\mathbf{x})$, $j = 0, \dots, m-1$, $i = 1, \dots, n$, и $\mathbf{x}^{(0)} = (x_1^{(0)}, \dots, x_n^{(0)})$.

Получим отсюда следствие — обобщение результата о биективности полиномиальной функции [7].

Следствие 1. ВРП-функция $f(x) \in \mathcal{DP}_R^{\mathcal{B}}(1)$ с разрядными многочленами $p_0(x), \dots, p_{m-1}(x)$ задаёт подстановку кольца R тогда и только тогда, когда одновременно выполняются следующие условия:

- 1) $p_0(x^{(0)}) \pmod{J(R)}$ задаёт подстановку на $\mathcal{B}$;
- 2) для любого $j \in \{1, \dots, m-1\}$ частная производная $\frac{\partial p_j}{\partial x}(x^{(0)}) \not\equiv 0 \pmod{J(R)}$ при всех $x^{(0)} \in \mathcal{B}$.

Напомним [8], что пара (Q, f) , где $f : Q^n \rightarrow Q$ и Q — конечное множество, называется n -квазигруппой (или n -арной квазигруппой), если унарная операция, полученная фиксацией всех аргументов операции f , кроме одного, любыми значениями из Q , является биекцией (такая унарная операция называется элементарной трансляцией). Иногда n -квазигруппой называют саму функцию f . При $n = 1$ n -квазигруппа — это подстановка элементов Q . Если Q — кольцо и функция f является полиномиальной над Q , то такая квазигруппа также называется полиномиальной. Дадим критерий того, что ВРП-функция над кольцом Галуа задаёт n -квазигруппу. Соответственно такую n -квазигруппу будем называть ВРП n -квазигруппой.

Теорема 3. Функция $f(\mathbf{x}) \in \mathcal{DP}_R^{\mathcal{B}}(n)$ с разрядными многочленами $p_0(\mathbf{x}), \dots, p_{m-1}(\mathbf{x})$ задаёт n -квазигруппу на кольце R тогда и только тогда, когда одновременно выполняются следующие условия:

- 1) $p_0(\mathbf{x}) \pmod{J(R)}$ задаёт n -квазигруппу на $\mathcal{B}$;
- 2) для любого $j \in \{1, \dots, m-1\}$ $\text{grad } p_j(\alpha) \pmod{J(R)}$ не содержит нулевых координат при любом $\alpha \in \mathcal{B}^n$.

Следствие 2. Свойство ВРП-функции $f(\mathbf{x}) \in \mathcal{DP}_R^{\mathcal{B}}(n)$ с разрядными многочленами $p_0(\mathbf{x}), \dots, p_{m-1}(\mathbf{x})$ задавать подстановку или n -квазигруппу инвариантно относительно выбора разрядного множества $\mathcal{B}$.

Следствие 2 означает, что свойство ВРП-функции задавать подстановку или n -квазигруппу зависит лишь от разрядных многочленов, а не от выбора разрядного множества $\mathcal{B}$, относительно которого рассматривается такая функция. Это позволяет строить различные подстановки и ВРП n -квазигруппы, используя одни и те же разрядные многочлены, но разные разрядные множества.

ЛИТЕРАТУРА

1. Елизаров В. П. Конечные кольца. М.: Гелиос-АРВ, 2006.
2. Заец М. В. О классе вариационно-координатно полиномиальных функций над примарным кольцом вычетов // Прикладная дискретная математика. 2014. № 3. С. 12–28.
3. Заец М. В., Никонов В. Г., Шишков А. Б. Класс функций с вариационно-координатной полиномиальностью над кольцом $\mathbb{Z}_{2^m}$ и его обобщение // Матем. вопросы криптографии. 2013. Т. 4. № 3. С. 19–45.
4. Заец М. В. Классы полиномиальных и вариационно-координатно полиномиальных функций над кольцом Галуа // Прикладная дискретная математика. Приложение. 2013. № 6. С. 13–15.
5. Lausch H. and Nobauer W. Algebra of polynomials. Amsterdam: North-Holl. Publ. Co, 1973.
6. Заец М. В. Построение подстановок с использованием вариационно-координатно полиномиальных функций над примарным кольцом вычетов // Матем. вопросы криптографии. 2015. Т. 6. № 1. С. 5–32.
7. Нечаев А. А. Полиномиальные преобразования конечных коммутативных локальных колец главных идеалов // Матем. заметки. 1980. Т. 27. Вып. 6. С. 885–899.
8. Белоусов В. Д. n -Арные квазигруппы. Кишинев: Штиинца, 1972.

УДК 519.688

DOI 10.17223/2226308X/10/6

О ГРАФЕ КЭЛИ ОДНОЙ ПОДГРУППЫ БЕРНСАЙДОВОЙ ГРУППЫ $B_0(2, 5)^1$

А. А. Кузнецов, А. С. Кузнецова

Пусть $B_0(2, 5)$ — максимальная конечная двупорожденная бернсайдова группа периода 5, порядок которой равен 5^{34} . Определим автоморфизм φ , при котором каждый порождающий элемент отображается в другой порождающий. Пусть $C_{B_0(2,5)}(\varphi)$ — централизатор φ в $B_0(2, 5)$. Известно, что $|C_{B_0(2,5)}(\varphi)| = 5^{17}$. В работе вычислена функция роста данного централизатора для минимального порождающего множества. В результате получены диаметр и средний диаметр соответствующего графа Кэли $C_{B_0(2,5)}(\varphi)$.

Ключевые слова: функция роста группы, граф Кэли, группа Бернсайда.

Одним из важных инструментов для определения строения группы является изучение её роста относительно фиксированного порождающего множества. Пусть $G = \langle X \rangle$. Шаром K_s радиуса s группы G будем называть множество всех её элементов, которые могут быть представлены в виде групповых слов в алфавите X длиной, не превышающей s . Для каждого целого неотрицательного s можно определить функцию роста группы $F(s)$, которая равна числу элементов группы G относительно X , представимых в виде несократимых групповых слов длиной s . Таким образом,

$$F(0) = |K_0| = 1, \quad F(s) = |K_s| - |K_{s-1}| \text{ при } s \in \mathbb{N}.$$

¹Работа поддержана РФФИ и Правительством Красноярского края (проект № 17-47-240318).