О Б О З Р Е Н И Е
П Р И К Л А Д Н О Й И П Р О М Ы Ш Л Е Н Н О Й
Т о м 20 **М А Т Е М А Т И К И** **В ы п у с к 3**
2013

М. В. З а е ц (Москва, ТВП)**. Некоторые свойства функций с вариационно-координатной полиномиальностью над примарным кольцом вычетов.**

Пусть $\mathcal{B} = \{0, 1, \ldots, p-1\} \subset \mathbf{Z}_{p^m}$, тогда любой элемент $a \in \mathbf{Z}_{p^m}$ может быть однозначно представлен в виде $a = a^{(0)} + p\,a^{(1)} + \cdots + p^{m-1}\,a^{(m-1)}$, $a^{(j)} \in \mathcal{B}$, $j = 0, 1, \ldots, m-1$, называемом разложением элемента a в p-ичном координатном множестве $\mathcal{B}$. Отображения $\gamma_j:\ \mathbf{Z}_{p^m} \to \mathcal{B}$, $\gamma_j(a) = a^{(j)}$, $j = 0, 1, \ldots, m-1$, называются координатными функциями. Класс всех полиномиальных функций от n переменных над кольцом $\mathbf{Z}_{p^m}$ обозначим через $\mathcal{P}_{p^m}(n)$. Следующее определение для случая кольца $\mathbf{Z}_{2^m}$ также можно найти в [1].

Функцию $f(\mathbf{x})\colon\ \mathbf{Z}_{p^m}^n \to \mathbf{Z}_{p^m}$ назовем *вариационно-координатно полиномиальной* (или ВКП-*функцией*), если для любого $j \in \{0, 1, \ldots, m-1\}$ существует такая полиномиальная функция $p_j(\mathbf{x}) \in \mathcal{P}_{p^m}(n)$, что $\gamma_j(f(\mathbf{x})) = \gamma_j(p_j(\mathbf{x}))$ при всех $\mathbf{x} \in \mathbf{Z}_{p^m}^n$. Такую полиномиальную функцию $p_j(\mathbf{x})$ будем называть *j-м координатным многочленом.*

Класс всех ВКП-функций от n переменных обозначим $\mathcal{CP}_{p^m}(n)$.

Теорема 1. *Верны следующие соотношения между классами $\mathcal{P}_{p^m}(n)$ и $\mathcal{CP}_{p^m}(n)$:*

1) $\mathcal{P}_{p^2}(n) = \mathcal{CP}_{p^2}(n)$; 2) $\mathcal{P}_{p^m}(n) \subsetneq \mathcal{CP}_{p^m}(n)$ *при всех* $m \geqslant 3$.

Теорема 2. *Справедлива следующая оценка сверху мощности класса $\mathcal{CP}_{p^m}(n)$:*

$$|\mathcal{CP}_{p^m}(n)| \leqslant p^{p^n + (m-1)n\,p^n + p^n\,(p^{n(m-1)}-1)/(p^n-1)}.$$

Пусть $f(\mathbf{x}) \in \mathbf{Z}_{p^m}[\mathbf{x}]$, обозначим

$$\mathrm{grad} f(\mathbf{x}) = \left(\frac{\partial f}{\partial x_1}(\mathbf{x}), \frac{\partial f}{\partial x_2}(\mathbf{x}), \ldots, \frac{\partial f}{\partial x_n}(\mathbf{x})\right), \text{ где } \frac{\partial f}{\partial x_i}(\mathbf{x}) \text{ —}$$

формальная частная производная многочлена $f(\mathbf{x})$ по переменной x_i, $i = 1, 2, \ldots, n$. Если $f_1(\mathbf{x}), f_2(\mathbf{x}), \ldots, f_t(\mathbf{x}) \in \mathbf{Z}_{p^m}[\mathbf{x}]$, то матрица $J_{f_1,f_2,\ldots,f_t}(\mathbf{x}) = \begin{pmatrix} \mathrm{grad} f_1(\mathbf{x}) \\ \vdots \\ \mathrm{grad} f_t(\mathbf{x}) \end{pmatrix}$ называется *матрицей Якоби* системы многочленов, а ее определитель $|J_{f_1,f_2,\ldots,f_t}(\mathbf{x})|$ — *якобианом.* Следующая теорема обобщает известный из [2] результат о биективности полиномиальной вектор-функции.

Теорема 3. *Вектор-функция* $F(\mathbf{x}) = (f_1(\mathbf{x}), f_2(\mathbf{x}), \ldots, f_n(\mathbf{x}))\colon\ \mathbf{Z}_{p^m}^n \to \mathbf{Z}_{p^m}^n$, *где* $f_i \in \mathcal{CP}_{p^m}(n)$, *является биекцией тогда и только тогда, когда одновременно выполняются условия*:

1) $(p_{01}(\mathbf{x}^{(0)}), p_{02}(\mathbf{x}^{(0)}), \ldots, p_{0n}(\mathbf{x}^{(0)}))\ (\mathrm{mod}\ p)\colon\ \mathcal{B}^n \to \mathcal{B}^n$ *является биекцией;*

2) *для любого* $j \in \{1, 2, \ldots, m-1\}$ *якобиан* $|J_{p_{j1},p_{j2},\ldots,p_{jn}}(\mathbf{x}^{(0)})| \not\equiv 0\ (\mathrm{mod}\ p)$ *при всех* $\mathbf{x}^{(0)} \in \mathcal{B}^n$,

где $p_{ji}(\mathbf{x})$ — j *-й координатный многочлен функции* $f_i(\mathbf{x})$, $j = 0, 1, \ldots, m-1$, $i = 1, 2, \ldots, n$, *и* $\mathbf{x}^{(0)} = (x_1^{(0)}, x_2^{(0)}, \ldots, x_n^{(0)})$.

В частности, отсюда получим следствие — обобщение результата, изложенного, например, в работе [3].

Следствие. ВКП-*функция* $f(x) \in \mathcal{CP}_{p^m}(1)$ *с координатными многочленами* $p_0, p_1, \ldots, p_{m-1}$ *задает подстановку кольца* $\mathbf{Z}_{p^m}$ *тогда и только тогда, когда одновременно выполняются условия*:

1) $p_0(x^{(0)}) \pmod p$ *задает подстановку на* $\mathcal{B}$;

2) *для любого* $j \in \{1, 2, \ldots, m-1\}$ *частная производная* $\frac{\partial p_j}{\partial x}(x^{(0)}) \not\equiv 0 \pmod p$ *при всех* $x^{(0)} \in \mathcal{B}$.

Работа выполнена при поддержке гранта Президента РФ НШ-8.2010.10.

СПИСОК ЛИТЕРАТУРЫ

1. *Заец М. В., Никонов В. Г., Шишков А. Б.* Функции с вариационно-координатной полиномиальностью и их свойства. — Открытое образование, 2012, № 3, с. 57–61.
2. *Lausch H., Nobauer W.* Algebra of polynomials. Amsterdam: North-Holl. Publ. Co, 1973.
3. *Нечаев А. А.* Полиномиальные преобразования конечных коммутативных колец главных идеалов. — Матем. заметки, 1980, т. 27, в. 6, с. 885–899.