Д. Н. Б ы л к о в (Москва, МИРЭА). **Инъективность сжимающих отображений, действующих на рекуррентах над кольцом Галуа.**

Пусть $R = GR(q^n, p^n)$, $q = p^r$, есть кольцо Галуа. Множество всех линейных рекуррент с характеристическим многочленом $F(x) = x^m - f_{m-1}x^{m-1} - \cdots - f_0$ над R будем обозначать $L_R(F)$. Пусть $\Psi\colon R \to \mathbf{Z}_p$, введем отображение $\widehat{\Psi}\colon L_R(F) \to \mathbf{Z}_p^\infty$ и пусть $\widehat{\Psi}(u)(i) = \Psi(u(i))$, $i \geqslant 0$.

Важной задачей является описание таких классов $(F(x), \Psi)$, что функция $\widehat{\Psi}$ инъективна. В случае, когда $F(x)$ является многочленом максимального периода, А. А. Нечаевым и А. С. Кузьминым построены большие классы инъективных отображений $\widehat{\Psi}$ [1]. В работе, представленной данным докладом, изучается случай, когда функция усложнения зависит от двух рекуррент.

Подмножество $K = \{b_0, b_1, \ldots, b_{q-1}\}$ называется *координатным множеством* кольца R, если оно образует полную систему вычетов по модулю идеала pR. Известно, что каждый элемент $a \in R$ однозначно представляется в виде

$$a = a_0 + pa_1 + p^2a_2 + \cdots + p^{n-1}a_{n-1}, \quad a_s = \gamma_s^K(a) \in K, \quad s = 0, 1, \ldots, n-1, \quad (1)$$

называемом *разложением элемента a в координатном множестве K*. Последнее свойство позволяет рассматривать произвольную функцию $\Phi\colon R^2 \to K$ от аргументов x_1, x_2 как функцию $\phi\colon K^{2n} \to K$ от аргументов $x_{i,j} = \gamma_j^K(x_i)$, $i = 1, 2$, $j = 0, 1, \ldots, n-1$.

Пусть $\Phi\colon R^2 \to K$, $F(x), G(x)$ — унитарные многочлены над R, степеней m и k. Рассмотрим отображение $\widehat{\Phi}(u, v)(i) = \Phi(u(i), v(i))$, $i \geqslant 0$.

Теорема. *Пусть функция ϕ биективна по переменным $x_{1,n-1}, x_{2,n-1}$. Пусть $F(x), G(x)$ — взаимно простые унитарные реверсивные многочлены Галуа над R со свойствами $(T(\overline{F}), T(\overline{G})) = e$ и*

$$\frac{T(F)}{(T(F), T(G))} \geqslant p^{2(n-1)}(q^n - 1)q^{m/2}, \quad \frac{T(G)}{(T(F), T(G))} \geqslant p^{2(n-1)}(q^n - 1)q^{k/2}.$$

Тогда отображение $\widehat{\Phi}$ инъективно (т. е. последовательности u, v однозначно определяются по последовательности $\widehat{\Phi}(u, v)$).

Автор выражает глубокую благодарность А. А. Нечаеву за постановку задачи и ценные советы при проведении исследования.

Работа выполнена при поддержке гранта Президента РФ НШ-4.2010.10.

СПИСОК ЛИТЕРАТУРЫ

1. *Кузьмин А. С.*, *Маршалко Г. Б.*, *Нечаев А. А.* Восстановление линейной рекурренты над примарным кольцом вычетов по ее усложнению. — Математические вопросы криптографии, 2010, т. 1, № 2, с. 31–56.