Д. Н. Б ы л к о в (Москва, МИРЭА)**. Усложнения линейных рекуррент над кольцом Галуа, не приводящие к потере информации.**

Пусть $R = \mathrm{GR}\,(q^n, p^n)$, $q = p^r$ — кольцо Галуа, $\mathcal{B} = \{b_0, b_1, \ldots, b_{q-1}\}$ — его координатное множество. Примерами координатных множеств являются p-адическое координатное множество $\Gamma(R)$ и p-ичное координатное множество $\{0, 1, \ldots, p-1\}$ в кольце $\mathbf{Z}_{p^n}$. В [1] показано, что каждый элемент $a \in R$ однозначно представляется в виде

$$a = a_0 + pa_1 + \ldots + p^{n-1}a_{n-1}, \quad a_s = \gamma_s^{\mathcal{B}}(a) \in \mathcal{B}, \quad s \in \{0, 1, \ldots, n-1\}, \qquad (1)$$

называемом *разложением элемента a в координатном множестве $\mathcal{B}$.*

Будем называть унитарный многочлен $F(x) \in R[x]$ степени m *многочленом максимального периода* (МП *многочленом*), если его период $T(F)$ равен $p^{n-1}(q^m - 1)$. Обозначим $L_R(F)$ множество всех линейных рекуррент над R с характеристическим многочленом $F(x)$, а $L_R(F)^*$ — подмножество линейных рекуррент $u \in L_R(F)$ периода $T(u) = T(F)$, т. е. *линейных рекуррентных последовательностей максимального периода* (МП ЛРП).

Функции $\Psi\colon\ R \to \mathrm{GF}\,(q)$ сопоставим отображение $\widehat{\Psi}\colon\ L_R(F) \to \mathrm{GF}\,(q)^\infty$ вида $\widehat{\Psi}(u)(i) = \Psi(u(i))$, $i \geqslant 0$. Для использования в криптографии последовательностей вида $\widehat{\Psi}(u)$ важно, чтобы при всех $u, v \in L_R(F)^*$, $u \neq v$, выполнялось соотношение $\widehat{\Psi}(u) \neq \widehat{\Psi}(v)$, т. е. чтобы функция $\widehat{\Psi}$ была инъективной.

Основы исследований в этом направлении заложены А. А. Нечаевым и его учениками. К настоящему времени построены большие классы инъективных отображений $\widehat{\Psi}$ [2]. В работе, представленной данным докладом, для класса МП многочленов описаны все такие отображения Ψ, что функция $\widehat{\Psi}$ инъективна.

Разложение (1) позволяет рассматривать функцию $\Psi(x)$ как функцию ψ от аргументов $x_0, x_1, \ldots, x_{n-1}$, полученных разложением x в координатном множестве $\mathcal{B}$.

Теорема. *Пусть $F(x) \in R[x]$ — МП многочлен со свойством $T(F) \geqslant q^{m/2}(q^{2n} - 1)p^{n-1}$. Тогда функция $\widehat{\Psi}$ инъективна тогда и только тогда, когда выполняются условия*:

1) *функция ψ существенно зависит от x_{n-1}*;

2) *для каждого $\lambda \in R^*$ найдется $x \in R$ со свойством $\Psi(x) \neq \Psi(\lambda x)$.*

Автор выражает глубокую признательность А. А. Нечаеву за постановку задачи и внимание к исследованию.

Работа выполнена при поддержке гранта Президента РФ НШ-4.2010.10.

СПИСОК ЛИТЕРАТУРЫ

1. *Kurakin V. L.*, *Kuzmin A. S.*, *Mikhalev A. V.*, *Nechaev A. A.* Linear Recurring Sequences over Rings and Modules. — J. Math. Sci. (New York), 1995, v. 76, № 6, p. 2793–2915.
2. *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.