**О. А. Козлитин** (Москва, ТВП). **Управляемые 2-линейные регистры сдвига.**

Пусть $R = \mathbf{Z}_2$, $m \geqslant 2$, $F(x) \in R[x]$ — многочлен максимального периода степени $m$, $S(F)$ — сопровождающая матрица, ассоциированная с многочленом $F$. Зафиксировав функцию $f$: $R^m \to R$, рассмотрим автономный автомат $\mathcal{R} = (R^m, R, \mathcal{F}_1, f)$, где $R$ — выходной алфавит, $R^m$ — множество состояний, функция перехода $\mathcal{F}_1$ определена равенством $\forall \mathbf{x} \in R^m$: $\mathcal{F}_1(\mathbf{x}) = \mathbf{x}\, S(F)$, а $f$ — функция выхода. Всюду далее будем считать, что начальное заполнение регистра $\mathcal{R}$ является ненулевым. Тогда этот регистр генерирует линейную рекуррентную последовательность (ЛРП) максимального периода ранга $m$ (см., например, [1]).

Пусть $G(x) \in R[x]$ — многочлен максимального периода степени $m$, $U = S(G)^T$, где «$T$» есть операция транспонирования, а $V = S(G)$. Зафиксировав некоторым образом функцию $\xi$: $R_{m,m} \to R$, рассмотрим внешне автономный автомат $\mathfrak{B} = (R, R_{m,m}, R, \mathcal{F}_2, \xi)$, функция перехода $\mathcal{F}_2$ которого определена равенством $\forall\, X \in R_{m,m}$, $z \in R$: $\mathcal{F}_2(X, z) = U^{1-z} X V^z$.

Последовательное соединение $\mathcal{R} \to \mathfrak{B}$ обозначим $\mathfrak{A}$. Автомат $\mathfrak{A}$ будем называть *управляемым 2-линейным регистром сдвига*.

Пусть $\tau = 2^m - 1$, и автоморфизм $\sigma$ пространства $R_{m,m}$ определен равенством $\forall\, X \in R_{m,m}$: $\sigma(X) = U^{(\tau-1)/2}\, X\, V^{(\tau+1)/2}$.

Если $\theta$ — корень многочлена $G(x)$ в поле $\mathrm{GF}(2^m)$, $a = \theta^{(\tau-1)/2}$, для всякого значения $j \in \{1, 2, \ldots, m-1\}$ многочлен $G_j(x) \in R[x]$ есть минимальный многочлен элемента $a^{2^{m-j}-1}$ над полем $R = \mathbf{Z}_2$, и $G_m(x) = (x \oplus 1)^m$, то согласно лемме 12 из работы [2] характеристический многочлен $\chi_\sigma(x)$ автоморфизма $\sigma$ представляется в виде

$$\chi_\sigma(x) = G_1(x) G_2(x) \cdots G_m(x), \tag{1}$$

причем $G_j(x)$ $(j = 1, 2, \ldots, m)$ — попарно взаимно простые многочлены степени $m$. Равенство (1) индуцирует следующее разложение пространства $R_{m,m}$ в прямую сумму ядер эндоморфизмов:

$$R_{m,m} = \operatorname{Ker} G_1(\sigma) \dot{+} \operatorname{Ker} G_2(\sigma) \dot{+} \cdots \dot{+} \operatorname{Ker} G_m(\sigma). \tag{2}$$

Разложение (2), в свою очередь, позволяет однозначно представить начальное состояние $W$ автомата $\mathfrak{B}$ в виде суммы $W = W_1 + W_2 + \cdots + W_m$, где $W_j \in \operatorname{Ker} G_j(\sigma)$, $j = 1, 2, \ldots, m$. Справедливо следующее утверждение.

**Теорема.** *Пусть выполнены следующие условия*:

1) $W_m \neq 0$, $W_j \neq 0$ *для всех* $j \in \{1, 2, \ldots, m-1\}$, *взаимно простых с* $m$;

2) $L$: $R^m \to R$ — *ненулевая линейная функция вида* $L(x_1, x_2, \ldots, x_m) = a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_m x_m$, *где* $a_i \in \{0, 1\}$;

3) *функция выхода* $\xi$ *управляемого 2-линейного регистра сдвига* $\mathfrak{A}$ *определена равенством* $\forall\, X \in R_{m,m}$: $\xi(X) = L(x_{1,1}, x_{2,1}, \ldots, x_{m,1})$, *где* $x_{i,1}$ — *элемент, стоящий в* $i$*-й строке и первом столбце матрицы* $X$, $i = 1, 2, \ldots, m$.

*Тогда выходная последовательность* $\gamma$ *автомата* $\mathfrak{A}$:

a) *имеет период* $\tau^2 = (2^m - 1)^2$;

b) *имеет ранг, удовлетворяющий двойному неравенству*

$$m + m\varphi(m)d(m) \leqslant \operatorname{rang}(\gamma) \leqslant m + m(m-1)(2^m - 1),$$

*где* $\varphi$ — *функция Эйлера, а* $d(m)$ *есть максимальное примарное число, которое делит* $2^m - 1$ *и не делит* $2^k - 1$ *ни для какого* $k \in \{1, 2, \ldots, m-1\}$.

Работа выполнена при поддержке гранта Президента РФ НШ-4.2008.10.

СПИСОК ЛИТЕРАТУРЫ

1. *Глухов М. М.*, *Елизаров В. П.*, *Нечаев А. А.* Алгебра. Т. 1, 2. М.: Гелиос–АРВ, 2003, 749 с.
2. *Козлитин О. А.* Периодические свойства простейшего 2-линейного регистра сдвига. — Дискретн. математика, 2007, т. 19, в. 3, с. 51–78.