О. А. К о з л и т и н (Москва, ТВП). **Декомпозиция двоичного 2-ЛРС с сепарабельными элементарными характеристическими многочленами.**

Пусть $R = \mathbf{Z}_2$, $m_i \in \mathbf{N}_0$, $i = 0, 1$, F_0 и F_1 — реверсивные неприводимые над R многочлены степеней m_0 и m_1 соответственно, $F(x) \in R[x]$ — реверсивный многочлен максимального периода степени $m = [m_0, m_1]$ (квадратные скобки означают наименьшее общее кратное), θ — его корень в поле $\mathrm{GF}(2^m)$. Для всякого $\alpha \in \mathrm{GF}(2^m)$ обозначим $m_{\alpha,R}(x)$ минимальный многочлен элемента α над полем R. Существуют такие значения $k, l \in \{1, 2, \ldots, 2^m - 1\}$, что $F_0(x) = m_{\theta^k,R}(x)$ и $F_1(x) = m_{\theta^l,R}(x)$.

Для $u \in L_R(F)$, $\lambda \geqslant 0$, $t \geqslant 1$, обозначим $u[\lambda, t]$ регулярную (λ, t)-выборку из последовательности u. Для всякого $j = 1, 2, \ldots, m$ обозначим $H_j^{[k,l]}$ множество 2-линейных рекуррентных последовательностей вида

$$(u[0, l], \quad u[k\,2^j, l], \quad u[2k\,2^j, l], \quad \ldots, \quad u[ik\,2^j, l], \quad \ldots)^*$$

по всем $u \in L_R(F)$ (здесь «$*$» означает операцию транспонирования). Рассмотрим преобразования φ_0 и φ_1 семейства $L_R(F_0, F_1)$, определенные равенством $\varphi_i(\mu) = x_i\mu$, $i = 0, 1$.

Теорема. *Имеет место следующее разложение пространства $L_R(F_0, F_1)$ в сумму подпространств, инвариантных относительно φ_0 и φ_1:*

$$L_R(F_0, F_1) = \sum_{j=1}^{m} H_j^{[k,l]}. \tag{1}$$

В случае $m_0 = m_1$ сумма (1) — прямая.

Для всякого $j = 1, 2, \ldots, m$ обозначим R_j генератор «$k\,2^j - l$ шагов» с характеристическим многочленом $F(x)$, функция выхода которого выделяет содержимое крайней слева ячейки накопителя [1]. Генераторы R_j, $j = 1, 2, \ldots, m$, представляют собой регистры сдвига с неравномерным движением. Обозначим $\mathfrak{A}$ неавтономный 2-линейный регистр сдвига (2-ЛРС) с элементарными характеристическими многочленами F_0 и F_1, диаграмма Ферре которого представляет собой прямоугольник $m_0 \times m_1$, а функция выхода выделяет содержимое ячейки, стоящей в верхнем левом углу текущего состояния [2]. Такой автомат будем называть *неавтономным прямоугольным* 2-ЛРС. Пусть $||$ — операция параллельного соединения автоматов (вход — один на все компоненты, выход — сумма выходных последовательностей компонент).

Следствие 1. *Неавтономный прямоугольный 2-ЛРС $\mathfrak{A}$ представляется параллельным соединением регистров сдвига с неравномерным движением*

$$\mathfrak{B} = R_1 \,||\, R_2 \,||\, R_3 \,||\, \cdots \,||\, R_m.$$

В случае $m_0 = m_1$ автоматы $\mathfrak{A}$ и $\mathfrak{B}$ эквивалентны.

Следствие 2. *Неавтономный прямоугольный 2-ЛРС $\mathfrak{A}$ с реверсивными сепарабельными элементарными характеристическими многочленами представляется параллельным соединением регистров сдвига с неравномерным движением.*

Эти результаты в определенном смысле сводят изучение периода и ранга выходной последовательности неавтономного прямоугольного 2-ЛРС $\mathfrak{A}$ к изучению аналогичных характеристик выходных последовательностей регистров сдвига с неравномерным движением.

Работа выполнена при поддержке гранта Президента РФ НШ-4.2008.10.

СПИСОК ЛИТЕРАТУРЫ

1. *Фомичев В.М.* Дискретная математика и криптология. М.: Диалог–МИФИ, 2003, 397 с.
2. *Нечаев А. А.* Многомерные регистры сдвига и сложность мультипоследовательностей. Труды по дискретной математике. М.: Физматлит, 2003, т. 6, с. 150–165.