UDC 512

RANK OF OUTPUT SEQUENCE OF SELF-CONTROLLED 2-LINEAR SHIFT REGISTER

Oleg A. Kozlitin

Laboratory TVP
111141, Moscow, Perovskaya st., 40.
PhD
E-mail: okozlitin@yandex.ru

The use of a self-controlled 2-linear shift register to generate pseudo-random sequences of high rank is considered in this paper. The upper and lower borders of rank of output sequence are received.

Keywords: self-controlled 2-linear shift register, pseudo-random sequence, rank.

Пусть $r \geq 1, \quad n \geq 1, \quad q = 2^r, \quad R = GR(q^n, 2^n)$ – кольцо Галуа мощности q^n и характеристики 2^n, $F(x) \in R[x]$ – многочлен максимального периода степени $m \geq 2$, $S(F)$ – его сопровождающая матрица, автоморфизмы φ_i бимодуля $R_{m,m}$ определены равенствами

$$\varphi_0(X) = S(F)^t \cdot X, \quad \varphi_1(X) = X \cdot S(F), \quad (1)$$

где t – символ транспонирования. Зададим функцию самоуправления $\beta : R_{m,m} \to \{0,1\}$ и функцию выхода $\psi : R_{m,m} \to R$. Используя автоморфизмы (1), построим автономный автомат

$$A = (R_{m,m}, R, h_\beta, \psi) \quad (2)$$

функция перехода h_β которого определена равенством $h_\beta(X) = \varphi_{\beta(X)}(X)$. Следуя [1], назовем автомат (2) самоуправляемым 2-линейным регистром сдвига.

Рассмотрим автоморфизм σ $R-$бимодуля $R_{m,m}$, заданный соотношением

$$\sigma = \varphi_0^{2^{n-2}(\tau-1)} \varphi_1^{2^{n-2}(\tau+1)},$$

где $\tau = q^m - 1$. Если θ – корень многочлена $F(x)$ в кольце $S = R[x]/F(x)$, $\alpha = \theta^{2^{n-2}(\tau-1)}$, $\overline{\alpha}$ – образ элемента α под действием естественного эпиморфизма $S \to \overline{S} = S / 2S$ и $m_j(x)$ – минимальный многочлен элемента $\overline{\alpha}^{q^j-1}$ над полем $\overline{R} = R/2R$, то характеристический многочлен $\chi_\sigma(x)$ автоморфизма σ имеет следующее каноническое разложение:

$$\chi_\sigma(x) = G_0(x) G_1(x) \cdots G_{m-1}(x),$$

где $G_0(x) = (x-1)^m, \quad \overline{G}_j(x) = m_j(x), \quad j = 1,2,\ldots,m-1.$ Это разложение индуцирует однозначное представление всякого состояния X автомата (2):

$$X = X_0 + X_1 + \ldots + X_{m-1}, \quad (3)$$

где $X_j \in \operatorname{Ker} G_j(\sigma), \quad j = 0,1,\ldots,m-1.$ Пусть функция выхода ψ возвращает элемент, находящийся в первой строке и первом столбце матрицы-аргумента, а

функция самоуправления β определена равенством $\beta(X) = \mathrm{tr}_{\mathbf{Z}_2}^{\bar{R}}(\overline{\psi(X_0)})$, где tr – функция «след», действующая из поля $\bar{R} = GF(2^r)$ в поле $\mathbf{Z}_2$.

Будем рассматривать лишь те начальные заполнения X, в разложении (3) которых $\bar{X}_0 \neq 0$. Для всякой матрицы $M \in R_{m,m}$ обозначим через $\|M\|$ максимальное значение $k \in \overline{0,n}$, для которого $M \in 2^k R_{m,m}$. Положим $s = \min\{\|X_j\| : j \in \overline{1,m-1}\}$. Усложним выходную последовательность γ автомата (2) путем выделения разряда γ_s в ее 2-адическом разложении:

$$\gamma = \gamma_0 + 2\gamma_1 + \cdots + 2^{n-1}\gamma_{n-1}.$$

Теорема. Если $J_s = \min\{j \in \overline{1,m-1} : \|X_j\| = s\}$ и $\tau_j = \tau/(q^{(m,j)} - 1)$, $j \in J_s$, то для некоторой линейной рекуррентной последовательности (ЛРП) максимального периода u с характеристическим многочленом $F(x)$ имеет место двойное неравенство

$$m \cdot \sum_{j \in J_s} \tau_j \leq \mathrm{rank}\, \gamma_s - \mathrm{rank}\, u_s \leq m \cdot |J_s| \cdot \tau,$$

где u_s есть s-ая координата в 2-адическом разложении ЛРП u. Таким образом,

$$\mathrm{rank}\, \gamma_s = O(m^2 q^m), \quad m \to \infty.$$

Работа выполнена при поддержке гранта Президента РФ НШ-4.2010.10.

Примечания:

1. Нечаев А.А. Многомерные регистры сдвига и сложность мультипоследовательностей. // Труды по дискретной математике. 2002. Том 6. С. 150-164.

УДК 512

РАНГ ВЫХОДНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ САМОУПРАВЛЯЕМОГО 2-ЛИНЕЙНОГО РЕГИСТРА СДВИГА

Олег Алексеевич Козлитин

Лаборатория ТВП
111141, Москва, Перовская ул., 40.
кандидат физико-математических наук.
E-mail: okozlitin@yandex.ru

В работе рассматривается возможность использования самоуправляемого 2-линейного регистра сдвига для выработки псевдослучайных последовательностей большого ранга. Получены верхняя и нижняя оценки ранга выходной последовательности.

Ключевые слова: самоуправляемый 2-линейный регистр сдвига, псевдослучайная последовательность, ранг.