UDC 512

On Periodical Properties of 2-Linear Recurring Sequences

Oleg A. Kozlitin

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

Abstract. The cycle structure of one set of 2-linear recurring sequences is researched in this paper. The results are useful to construct a generator of pseudo-random sequences with good periodical properties.

Keywords: cycle structure; k-linear shift register; pseudo-random sequence.

Рост трафика в компьютерных сетях, наблюдающийся в последние десятилетия, ставит новые задачи в области криптографической защиты данных. Один из подходов к их решению заключается в использовании современных поточных криптосистем. Основой любой поточной криптосистемы является генератор псевдослучайных последовательностей (ПСП), свойствами которого во многом определяется качество системы в целом. Поэтому разработка и исследование генераторов ПСП, построенных на новых математических принципах, являются актуальными задачами современной криптографии.

С середины 90-х г.г. прошлого века изучается возможность использования для выработки ПСП линейных регистров сдвига размерности $k \geq 2$ ($k-$линейных регистров сдвига), вырабатывающих на основе начальной информации (начального отрезка) $k-$линейную рекуррентную последовательность ($k-$ЛРП, [1]).

Пусть $k \geq 1$ и R – кольцо с единицей 1. Всякое отображение $u: \mathrm{N}_0^k \to R$ назовем $k-$мерной последовательностью над кольцом R. Множество всех $k-$мерных последовательностей над R обозначим через $R^{\langle k \rangle}$. Если

$$R_k = R[x_0, x_1, \ldots, x_{k-1}],$$

то абелеву группу $(R^{\langle k \rangle}, +)$ можно наделить структурой левого R_k-модуля: для всякого вектора $(i_0, i_1, \ldots, i_{k-1}) \in \mathrm{N}_0^k$ положим

$$(x_0^{t_0} x_1^{t_1} \cdots x_{k-1}^{t_{k-1}} \cdot u)(i_0, i_1, \ldots, i_{k-1}) = u(i_0 + t_0, i_1 + t_1, \ldots, i_{k-1} + t_{k-1}).$$

Пусть $F_0(x_0), F_1(x_1), \ldots, F_{k-1}(x_{k-1}) \in R_k$ – унитарные (со старшим коэффициентом 1) многочлены. Последовательность $u \in R^{\langle k \rangle}$ называется $k-$линейной рекуррентной последовательностью с элементарными характеристическими многочленами (э.х.м.) $F_0, F_1, \ldots, F_{k-1}$, если

$$\forall i \in \overline{0, k-1}: \quad F_i(x_i) u = 0.$$

Семейство всех $k-$линейных рекуррент с э.х.м. $F_0, F_1, \ldots, F_{k-1}$ обозначается

$$L_R(F_0, F_1, \ldots, F_{k-1}) \tag{1}$$

и называется $k-$ЛРП$-$семейством.

Периодические свойства $k-$линейных регистров сдвига тесно связаны с цикловым типом $C_{F_0, F_1, \ldots, F_{k-1}}(y)$ семейства рекуррент (1). Если

$$\mathrm{t} = (t_0, t_1, \ldots, t_{k-1}), \quad \mathrm{x} = (x_0, x_1, \ldots, x_{k-1}), \quad \mathrm{x}^{\mathrm{t}} = x_0^{t_0} x_1^{t_1} \cdots x_{k-1}^{t_{k-1}},$$

то под циклом $C(u)$, содержащим рекурренту u из семейства (1), понимается множество

$$C(u) = \{\mathrm{x}^{\mathrm{t}} u \mid \mathrm{t} \in \mathrm{N}_0^k\},$$

а под его длиной – величина $T(u) = |C(u)|$ (период рекурренты u).

Многочлен

$$C_{F_0, F_1, \ldots, F_{k-1}}(y) = \sum_{t \geq 1} c_t y^t \in \mathbf{Z}[y],$$

где c_t – количество циклов длины t в семействе (1), называется цикловым типом семейства (1).

Описание циклового типа семейства (1) – в данный момент открытая проблема. Начинать ее решение естественно с простейших случаев. Мы вычислим цикловой тип $C_{F,F}(y)$ семейства $L_R(F,F)$ в случае, когда $R = \mathbf{Z}_2$, и

$$F(x) = x^m - f_{m-1}x^{m-1} - \ldots - f_1 x - f_0 \text{ –}$$

многочлен максимального периода $\tau = 2^m - 1.$

Пусть $S(F)$ – сопровождающая матрица многочлена $F(x)$:

$$S(F) = \begin{pmatrix} 0 & 0 & \cdots & 0 & f_0 \\ 1 & 0 & \cdots & 0 & f_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & 1 & 0 & f_{m-2} \\ 0 & \cdots & 0 & 1 & f_{m-1} \end{pmatrix},$$

$\Omega = R_{m,m}$ – пространство $m \times m-$матриц над полем $R = \mathbf{Z}_2$, φ_0 и φ_1 – автоморфизмы пространства Ω, определенные равенствами

$$\varphi_0(X) = S(F)^T X, \quad \varphi_1(X) = XS(F),$$

где T – символ операции транспонирования. Согласно [2] характеристический многочлен $\chi_\sigma(x)$ автоморфизма $\sigma = \varphi_0^{-1}\varphi_1$ имеет следующее каноническое разложение:

$$\chi_\sigma(x) = G_0(x)G_1(x)\cdots G_{m-1}(x), \tag{2}$$

где $G_0(x) = (x \oplus 1)^m$, $G_s(x)$ – попарно различные неприводимые над полем R многочлены степени m, $s = 1, 2, \ldots, m-1.$ Представление (2) индуцирует следующее однозначное разложение всякой матрицы $w \in \Omega$:

$$w = w_0 + w_1 + \cdots + w_{m-1}, \tag{3}$$

где $w_s \in \operatorname{Ker} G_s(\sigma)$, $s = 0, 1, \ldots, m-1.$

Положим $\mathsf{F} = \overline{0, m-1} \times \overline{0, m-1}.$ Если $u \in L_R(F,F)$, то матрицу $u[\mathsf{F}]$ будем называть начальным отрезком ЛРП u. Пусть w – начальный отрезок ЛРП u, и ε_s – индикатор того, что в разложении (3) слагаемое w_s – ненулевое, $s = 0, 1, \ldots, m-1.$ Вектор

$$\operatorname{typ}(u) = (\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{m-1})$$

назовем типом рекурренты u. Пусть $\tau_d = \tau / (2^d - 1)$, $d \mid m.$ Справедлива следующая теорема.

ТЕОРЕМА. Пусть $R = \mathbf{Z}_2$, $F(x) \in R[x]$ – многочлен максимального периода степени $m \geq 2$. Тогда:

1. Если $m = d_1 > d_2 > d_3 > \cdots > d_l = 1$ – все натуральные делители числа m, то длины циклов семейства $L_R(F,F)$ образуют ряд
$$1 < \tau\tau_{d_1} < \tau\tau_{d_2} < \cdots < \tau\tau_{d_l} = \tau^2.$$
2. Пусть $u \in L_R(F,F)$, и $\mathrm{typ}(u) = (\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{m-1})$. $T(u) = 1$ тогда и только тогда, когда $u = 0$. $T(u) = \tau\tau_d$ тогда и только тогда, когда
$$u \neq 0 \text{ и } (\varepsilon_1, 2\varepsilon_2, 3\varepsilon_3 \ldots, (m-1)\varepsilon_{m-1}, m) = d.$$
3. Цикловой тип $C_{F,F}(y)$ семейства $L_R(F,F)$ выражается формулой
$$y + y^{\tau} + \sum_{d|m,\, d<m} (\tau\tau_d)^{-1} \sum_{t\,|\,\frac{m}{d}} \mu\left(\frac{m}{dt}\right) 2^{mt} y^{\tau\tau_d},$$
где μ – функция Мебиуса (см., например, [3]).

Полученные результаты показывают, что почти все рекурренты из семейства $L_R(F,F)$ лежат на циклах максимально возможной длины. С точки зрения возможного использования в криптографии 2-линейный регистр сдвига с равными элементарными характеристическими многочленами максимального периода обладает хорошими периодическими свойствами.

Примечания:

1. Кузьмин А.С., Куракин В.Л., Нечаев А.А. Псевдослучайные и полилинейные последовательности // Труды по дискретной математике. М., 1997. Том 1. С. 139-202.
2. Козлитин О.А. Периодические свойства 2-линейного регистра сдвига над кольцом Галуа // Обозрение прикладной и промышленной математики. М., 2011. Том 18, вып. 4. С. 513-526.
3. Сачков В.Н. Введение в комбинаторные методы дискретной математики. М.: МЦНМО, 2004. 424 с.

УДК 512

О периодических свойствах 2-линейных рекуррентных последовательностей

Олег Алексеевич Козлитин

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

Аннотация. В работе исследуется цикловая структура одного семейства 2-линейных рекуррентных последовательностей. Полученные результаты могут быть использованы при построении генераторов псевдослучайных последовательностей с хорошими периодическими свойствами.

Ключевые слова: цикловая структура; k-линейный регистр сдвига; псевдослучайная последовательность.