Math-Net.Ru

Общероссийский математический портал

О. А. Козлитин, Свойства выходной последовательности простейшего 2-линейного регистра сдвига над кольцом $\mathbf{Z}_{2^n}$, *Дискрет. матем.*, 2007, том 19, выпуск 4, 70–96

DOI: <https://doi.org/10.4213/dm978>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.84.234.179

26 апреля 2023 г., 12:29:21

Свойства выходной последовательности простейшего 2-линейного регистра сдвига над кольцом $\mathbb{Z}_2^n$

© 2007 г. О. А. Козлитин

Изучаются свойства выходной последовательности простейшего самоуправяемого 2-линейного регистра сдвига над кольцом вычетов $R = \mathbb{Z}_2^n$. Для конкретной функции выхода исследуются период и ранг выходной последовательности. В некоторых частных случаях изучаются частоты знаков на цикле выходной последовательности, усложненной путем выделения первого разряда. Показано, что ранг выходной последовательности двумерного регистра сдвига значительно больше ранга выходной последовательности одномерного регистра с тем же объемом накопителя.

Работа выполнена при поддержке программой Президента Российской Федерации поддержки ведущих научных школ, грант НШ-8564.2006.10.

1. Введение

Пусть $R = \mathbb{Z}_2^n$, $n \geq 2$. Для каждого унитарного (со старшим коэффициентом 1) многочлена

$$F(x) = x^m - f_{m-1}x^{m-1} - f_{m-2}x^{m-2} - \dots - f_1x - f_0 \in R[x]$$

обозначим через $S(F)$ соответствующую сопровождающую матрицу

$$S(F) = \begin{pmatrix} 0 & \dots & 0 & 0 & f_0 \\ 1 & \dots & 0 & 0 & f_1 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 1 & 0 & f_{m-2} \\ 0 & \dots & 0 & 1 & f_{m-1} \end{pmatrix}.$$

Напомним, что многочлен $F(x) \in R[x]$ является периодическим, то есть существуют числа $d \in \mathbb{N}_0$, $t \in \mathbb{N}$ такие, что

$$F(x) \mid x^d(x^t - 1). \quad (1)$$

При этом существуют параметры $T(F) \in \mathbb{N}$, период многочлена $F(x)$, и $D(F) \in \mathbb{N}_0$, дефект многочлена $F(x)$ такие, что

$$\forall t \in \mathbb{N}, d \in \mathbb{N}_0 \quad (1) \iff T(F) \mid t, \quad D(F) \leq d.$$

Унитарный периодический многочлен $F(x) \in R[x]$ такой, что $D(F) = 0$, назовем реверсивным. Согласно [1], унитарный многочлен $F(x) \in R[x]$ реверсивен тогда и только тогда, когда обратим свободный коэффициент, то есть $F(0) \in R^*$.

Реверсивный многочлен $F(x) \in R[x]$ степени m называется многочленом максимального периода, если $T(F) = 2^{n-1}(2^m - 1)$. Всюду далее $F(x) \in R[x]$ — многочлен максимального периода степени $m \geq 2$. Пусть обратимые матрицы U и V над кольцом R определены равенствами

$$U = S(F)^T, \quad V = S(F), \quad (2)$$

где верхний индекс T обозначает операцию транспонирования. Обозначим через M кольцо квадратных $m \times m$ матриц над R . Семейство M является свободным левым модулем над R . Зададим автоморфизмы φ_0 и φ_1 модуля ${}_R M$ равенствами

$$\varphi_0(X) = UX, \quad \varphi_1(X) = XV, \quad X \in M. \quad (3)$$

Используя эти автоморфизмы как частичные функции перехода, построим автономный автомат

$$\mathfrak{A}^\beta = \langle M, R, h, \psi \rangle,$$

где M — множество состояний, $\psi: M \rightarrow R$ — функция выхода, а функция перехода $h: M \rightarrow M$ задается с помощью некоторой индексирующей функции $\beta: M \rightarrow \{0, 1\} \subset \mathbb{Z}$ равенством

$$\forall X \in M: \quad h(X) = \varphi_{\beta(X)}(X).$$

Следуя [2], построенный автомат $\mathfrak{A}^\beta$ будем называть простейшим самоуправляемым 2-линейным регистром сдвига (2-ЛРС) или просто регистром.

Свойства регистра $\mathfrak{A}^\beta$ во многом определяются свойствами индексирующей функции β . Рассмотрим естественный эпиморфизм

$$R \rightarrow \bar{R} = R/2R = \mathbb{Z}_2.$$

Для каждого элемента $a \in R$ (матрицы $X \in M$, последовательности $u \in R^\infty$, многочлена $F(x) \in R[x]$) будем обозначать через $\bar{a}$ (соответственно, через $\bar{X}$, $\bar{u}$, $\bar{F}(x)$) образы этих объектов при указанном естественном эпиморфизме. Пусть $\bar{x}_{1,1}$ — элемент, стоящий в первой строке и первом столбце матрицы $\bar{X}$. Всюду далее предполагается, что индексирующая функция β определена равенством

$$\forall X \in M: \quad \beta(X) = \bar{x}_{1,1}. \quad (4)$$

Рассмотрим последовательность состояний

$$W = (W(0), W(1), \dots, W(i), \dots) \in M^\infty, \quad (5)$$

полученную по правилу

$$\forall i \geq 0: \quad W(i+1) = h(W(i)) = \varphi_{\beta(W(i))}(W(i)).$$

Эта последовательность является периодической. Согласно [2], ее период $T(W)$ и длина подхода (дефект) $D(W)$ удовлетворяют неравенству

$$T(W) + D(W) \leq 2^{n-1}(2^m - 1)^2. \quad (6)$$

Состояния $W(0) \in M$, для которых $D(W(0)) = 0$ и неравенство (6) обращается в равенство, называются основными. Существование основных состояний доказано в [2]. Их число $N(\mathfrak{A}^\beta)$ выражается формулой

$$N(\mathfrak{A}^\beta) = (2^m - 1) \sum_{d|m} \mu(m/d) 2^{m(n-1)d},$$

где μ — функция Мебиуса. В этой статье будет исследована выходная последовательность y регистра $\mathfrak{A}^\beta$, функция выхода ψ которого определена равенством

$$\forall X \in M: \quad \psi(X) = x_{1,1} \in R. \quad (7)$$

Пусть множество состояний 1-ЛРС (2-ЛРС) над кольцом R есть R^m (соответственно, $R_{m \times m}$). Будем говорить, что регистр имеет накопитель объема nm (соответственно, nm^2). Объем накопителя одномерного двоичного регистра назовем также длиной накопителя. Объем накопителя отражает количество битов памяти, необходимых для хранения его заполнения.

Основные результаты о свойствах выходной последовательности y состоят в следующем.

- (1) Показано, что если $W(0)$ — основное состояние, то

$$T(y) = T(W), \quad \text{rank}(y) \leq m^2(2^m - 1) - m(2^m - 2).$$

(теорема 1 и следствие 1). Среди основных состояний есть матрицы $W(0)$, для которых

$$\text{rank}(y) \geq md(m)\varphi(m) + (m+1)(m - \varphi(m)) - 1,$$

где φ есть функция Эйлера, а $d(m)$ есть максимальное простое число, которое делит $2^m - 1$ и не делит $2^k - 1$ для всех $k \in \{1, 2, \dots, m-1\}$. Доля таких матриц $W(0)$ среди всех основных состояний стремится к 1 при $m \rightarrow \infty$ (теорема 3).

- (2) Пусть $\nu = \|UW(0) - W(0)V\|$ — максимальное $k \in \{0, 1, \dots, n\}$, для которого

$$UW(0) - W(0)V \in 2^k R_{m \times m}.$$

Для основных состояний $W(0)$ изучается возможность усложнения выходной последовательности y путем выделения координатной последовательности y_ν в двоичном разложении

$$y = y_0 + 2y_1 + 2^2y_2 + \dots + 2^{n-1}y_{n-1}.$$

Найдены оценки ранга последовательности y_ν ; в случае, когда $R = \mathbf{Z}_4$ и $2^m - 1$ — простое число, найдено точное значение $\text{rank}(y_1)$ (теорема 5).

- (3) Пусть $R = \mathbf{Z}_4$. Обозначим $\mathfrak{A}_1^\beta$ результат усложнения регистра $\mathfrak{A}^\beta$ путем выделения первого разряда из выходной последовательности y . В одном частном случае исследуются частотные характеристики выходной последовательности y_1 автомата $\mathfrak{A}_1^\beta$. Получена нетривиальная оценка относительной частоты p_z появления знака $z \in \{0, 1\}$ на цикле последовательности y_1 (теорема 7). Найденная оценка, в частности, показывает, что если $W(0)$ — основное состояние, то последовательность y_1 асимптотически равномерна при $m \rightarrow \infty$.

- (4) Полученные результаты позволяют сравнить усложненные путем выделения старшего разряда 1-ЛРС и 2-ЛРС над кольцом $\mathbf{Z}_4$. Пусть 1-ЛРС имеет характеристический многочлен максимального периода степени m^2 . Тогда длина максимального цикла 2-ЛРС $\mathfrak{X}^\beta$ существенно меньше длины максимального цикла 1-ЛРС, однако, если $2^m - 1$ — простое число, ранг вырабатываемой последовательности в двумерном случае значительно больше, чем в одномерном. Рассмотрен вопрос о том, какова должна быть степень нелинейности функции Φ , чтобы усложненный ею 1-ЛРС вырабатывал последовательность, ранг которой не меньше ранга выходной последовательности самоуправляемого 2-ЛРС.
- (5) Ранг выходной последовательности $y_1 \in \mathbf{Z}_2^\infty$ автомата $\mathfrak{X}_1^\beta$ можно также сравнить с рангом выходной последовательности фильтрующего генератора [8] над полем $\mathbf{Z}_2$. Если такая схема представляет собой 1-ЛРС с длиной накопителя $2m^2$ и характеристическим многочленом максимального периода $4^{m^2} - 1$, а выходная последовательность γ получается путем усложнения текущего заполнения двоичной функцией Φ степени r , то максимальный возможный ранг выходной последовательности (при подходящем выборе функции усложнения) есть

$$\text{rank}(\gamma) = \sum_{j=1}^r \binom{2m^2}{j}.$$

В работе исследован вопрос, какова должна быть степень нелинейности r функции усложнения Φ , чтобы выполнялось неравенство $\text{rank}(\gamma) \geq \text{rank}(y_1)$.

2. Период выходной последовательности простейшего самоуправляемого 2-ЛРС

Чтобы изучить свойства выходной последовательности y регистра $\mathfrak{X}^\beta$, понадобятся некоторые понятия, обозначения и результаты работы [2]. Пусть $\tau = 2^m - 1$. Определим автоморфизм σ модуля ${}_R M$ равенством

$$\forall X \in M: \quad \sigma(X) = U^{(\tau-1)/2} X V^{(\tau+1)/2}.$$

Если ϑ — некоторый корень многочлена $\bar{F}$ в поле разложения $GF(2^m)$, $w = \vartheta^{(\tau-1)/2}$, и $\mu_{w^{2^l-1}}(x)$ — минимальный многочлен элемента w^{2^l-1} над полем $\mathbf{Z}_2$, то согласно [2] существуют попарно взаимно простые унитарные многочлены степени m $G_0(x), G_1(x), \dots, G_{m-1}(x) \in R[x]$ такие, что

$$\bar{G}_0(x) = (x-1)^m, \quad \bar{G}_l(x) = \mu_{w^{2^l-1}}(x), \quad l \in \{1, 2, \dots, m-1\}, \quad (8)$$

и для характеристического многочлена $\chi_\sigma(x)$ автоморфизма σ верно равенство

$$\chi_\sigma(x) = \prod_{l=0}^{m-1} G_l(x). \quad (9)$$

Обозначим N_l подмодуль $\text{Ker } G_l(\sigma)$ модуля M . Тогда из равенства (9) вытекает справедливость разложения

$${}_R M = {}_R N_0 \dot{+} {}_R N_1 \dot{+} \dots \dot{+} {}_R N_{m-1}, \quad (10)$$

и всякая матрица $X \in M$ однозначно представляется в виде

$$X = P + Q_1 + Q_2 + \dots + Q_{m-1}, \quad (11)$$

где $P \in N_0$, $Q_l \in N_l$, $l = 1, 2, \dots, m-1$.

Для каждой пары чисел $i, j \in \{1, \dots, m\}$ обозначим $E^{(i,j)}$ матрицу размеров $m \times m$, у которой в строке i и столбце j стоит 1, а на остальных позициях 0. Система матриц $E^{(1,1)}, \dots, E^{(1,m)}, E^{(2,1)}, \dots, E^{(2,m)}, \dots, E^{(m,1)}, \dots, E^{(m,m)}$ есть базис свободного модуля ${}_R M$. Эту систему будем записывать в виде столбца $e^\downarrow$ матриц

$$e^\downarrow = (E^{(1,1)}, \dots, E^{(1,m)}, E^{(2,1)}, \dots, E^{(2,m)}, \dots, E^{(m,1)}, \dots, E^{(m,m)})^T. \quad (12)$$

Для всякой матрицы $X \in M$ будем обозначать $\vec{X}$ строку коэффициентов матрицы X в базисе $e^\downarrow$:

$$X = \vec{X} e^\downarrow.$$

Тогда если E — единичная матрица размеров $m \times m$, а $\otimes$ — операция тензорного произведения матриц, то

$$\varphi_0(X) = \vec{X}(S(F) \otimes E)e^\downarrow, \quad \varphi_1(X) = \vec{X}(E \otimes S(F))e^\downarrow, \quad (13)$$

и

$$\sigma(X) = \vec{X}(S(F)^{(\tau-1)/2} \otimes S(F)^{(\tau+1)/2})e^\downarrow$$

для каждой матрицы $X \in M$. Из равенств (13) следует, что если $\circ$ есть операция композиции, то для любого $i \in \{0, 1\}$

$$\varphi_i \circ \sigma = \sigma \circ \varphi_i.$$

Следовательно, если $X \in N_l$, то для любого $i \in \{0, 1\}$

$$G_l(\sigma)(\varphi_i(X)) = \varphi_i(G_l(\sigma)(X)) = 0,$$

то есть $\varphi_i(X) \in N_l$. Таким образом, все подмодули N_l инвариантны относительно функции перехода h регистра $\mathfrak{A}^\beta$. Обозначим δ управляющую последовательность регистра $\mathfrak{A}^\beta$, определенную равенством

$$\forall i \geq 0: \quad \delta(i) = \beta(W(i)). \quad (14)$$

Для изучаемой последовательности W вида (5) зададим последовательность $\mathbf{s}$ управляющих векторов равенствами

$$\forall j \geq 0: \quad \mathbf{s}(j) = (s_0(j), s_1(j)) = \left(\sum_{i=0}^{j-1} (1 - \delta(i)), \sum_{i=0}^{j-1} \delta(i) \right) \in \mathbf{N}_0^2, \quad (15)$$

при этом будем считать, что $\mathbf{s}(0) = (0, 0)$. Тогда для всех $i \geq 0$ справедливо равенство

$$W(i) = U^{s_0(i)} W(0) V^{s_1(i)}. \quad (16)$$

Пусть матрица $W(0) \in M$ обладает следующими свойствами:

$$\bar{W}(0) \neq 0, \quad \bar{U} \bar{W}(0) = \bar{W}(0) \bar{V}, \quad U W(0) \neq W(0) V. \quad (17)$$

В [2] показано, что матрица $W(0)$ обладает свойствами (17) тогда и только тогда, когда ее разложение (11) имеет вид

$$W(0) = P + Q_{l_1} + Q_{l_2} + \dots + Q_{l_s}, \quad (18)$$

где $\bar{P} \neq 0$, $s \geq 1$, $1 \leq l_1 < l_2 < \dots < l_s \leq m-1$, и $\bar{Q}_l = 0$, $Q_l \neq 0$ для всех $l \in \{l_1, l_2, \dots, l_s\}$.

Введем обозначения

$$\forall i \geq 0, \quad l \in \{l_1, l_2, \dots, l_s\}: \quad P(i) = PV^i, \quad Q_l(i) = U^{s_0(i)} Q_l V^{s_1(i)}.$$

Пусть $\|X\|$ есть максимальное $k \in \{0, 1, \dots, n\}$ такое, что $X \in 2^k R_{m \times m}$. Согласно (16), (18) и в силу инвариантности N_l относительно функции перехода h имеет место разложение

$$\forall i \geq 0: \quad W(i) = P(i) + Q_{l_1}(i) + Q_{l_2}(i) + \dots + Q_{l_s}(i), \quad (19)$$

где

$$\forall i \geq 0, \quad l \in \{l_1, l_2, \dots, l_s\}: \quad P(i) \in N_0, \quad \bar{P}(i) \neq 0,$$

и

$$Q_l(i) \in N_l, \quad \|Q_l(i)\| = \|Q_l\| \in \{1, 2, \dots, n-1\}.$$

Выходная последовательность y автомата $\mathfrak{A}^\beta$ удовлетворяет равенству

$$\forall i \geq 0: \quad y(i) = \psi(P(i)) + \psi(Q(i)), \quad (20)$$

где

$$Q(i) = Q_{l_1}(i) + Q_{l_2}(i) + \dots + Q_{l_s}(i). \quad (21)$$

Поскольку для матрицы P из разложения (11) справедливо включение $P \in N_0$, согласно п. 2 леммы 4.12 в [2] верно равенство $UP = PV$. Из п. 1 леммы 4.9 в [2] следует, что если $\bar{P} \neq 0$ и $UP = PV$, то первая строка матрицы P является ненулевой по модулю радикала. Поэтому

$$\forall i \geq 0: \quad \psi(P(i)) = \psi(PV^i) = u(i),$$

где $u \in L_R(F)$, $\bar{u} \neq 0$. Пусть последовательность λ определена соотношением

$$\forall i \geq 0: \quad \lambda(i) = \psi(Q(i)).$$

Тогда разложение (20) приобретает вид

$$\forall i \geq 0: \quad y(i) = u(i) + \lambda(i), \quad (22)$$

причем $F(x)$ — минимальный многочлен (см. [1]) линейной рекуррентной последовательности (ЛРП) u и $T(u) = 2^{n-1}\tau$. Таким образом, вопрос о периоде выходной последовательности y сводится к вопросу о периоде последовательности λ .

Знаки 0 и 1 управляющей последовательности δ можно рассматривать как элементы поля $\mathbf{Z}_2$. Согласно лемме 4.1 в [2], если матрица $W(0)$ обладает свойствами (17), то δ есть ЛРП максимального периода τ над полем $\mathbf{Z}_2$ с минимальным многочленом $\bar{F}(x)$. Поэтому для всех $d \in \{0, 1, \dots, \tau-1\}$ и $j \geq 0$ имеет место цепочка равенств

$$\begin{aligned} s(d+j\tau) &= \left(\sum_{k=0}^{d+j\tau-1} (1-\delta(k)), \sum_{k=0}^{d+j\tau-1} \delta(k) \right) = s(d) + j \left(\sum_{k=d}^{d+\tau-1} (1-\delta(k)), \sum_{k=d}^{d+\tau-1} \delta(k) \right) \\ &= s(d) + j((\tau-1)/2, (\tau+1)/2). \end{aligned}$$

Отсюда

$$Q(d + j\tau) = U^{j(\tau-1)/2} Q(d) V^{j(\tau+1)/2} = \sigma^j(Q(d)) \quad (23)$$

для всех $d \in \{0, 1, \dots, \tau - 1\}$ и $j \geq 0$. Обозначим через λ_d последовательность, определенную равенством

$$\forall j \geq 0: \quad \lambda_d(j) = \psi(\sigma^j(Q(d))).$$

Последовательность λ_d является регулярной (d, τ) -выборкой из λ . Поскольку функция ψ линейна, а σ – автоморфизм, для всех $j \geq 0$ справедливы равенства

$$\lambda_d(j) = \lambda_d^{(1)}(j) + \lambda_d^{(2)}(j) + \dots + \lambda_d^{(s)}(j), \quad (24)$$

где

$$\forall i \in \{1, 2, \dots, s\}: \quad \lambda_d^{(i)}(j) = \psi(\sigma^j(Q_{l_i}(d))). \quad (25)$$

Из соотношения (24) следует, что периодические свойства последовательности λ определяются периодическими свойствами последовательностей $\lambda_d^{(i)}$, которые и будут изучаться в дальнейшем.

Введем ряд обозначений. Пусть $k \geq 1$. Сопоставим матрице $X \in R_{k \times k}$ левый $R[x]$ -модуль $M(X)$, получающийся из R -модуля R^k , если определить умножение многочлена $G(x) \in R[x]$ на вектор-строку $\gamma \in R^k$ по правилу

$$G(x) \circ \gamma = \gamma G(X).$$

Пусть $A = S(F)^{(\tau-1)/2} \otimes S(F)^{(\tau+1)/2}$. Согласно [2] для некоторой матрицы $A_0 \in R_{m \times m}$ с характеристическим многочленом $G_0(x)$ имеет место следующий изоморфизм левых $R[x]$ -модулей:

$$M(A) \cong M(A_0) \oplus M(S(G_1)) \oplus \dots \oplus M(S(G_{m-1})). \quad (26)$$

Отсюда и из теоремы 1 раздела 1 в [6] следует, что существует матрица $Z \in R_{m^2 \times m^2}^*$ такая, что

$$Z^{-1}AZ = \text{Diag}(A_0, S(G_1), \dots, S(G_{m-1})).$$

Напомним, что для всякой матрицы $X \in M$ через $\vec{X}$ обозначена строка коэффициентов при разложении X по базису $e^\downarrow$, определенному равенством (12). Справедливо следующее утверждение.

Лемма 1. *Отображение $\zeta: R^{m^2} \rightarrow R^{m^2}$, действующее по правилу*

$$\forall X \in M: \quad \zeta(\vec{X}) = \vec{X}Z,$$

задает изоморфизм (26).

Доказательство. Достаточно показать, что

$$\forall G(x) \in R[x], \quad \alpha \in R^{m^2}: \quad \zeta(G(x) \circ \alpha) = G(x) \circ \alpha Z.$$

Справедлива цепочка равенств

$$\begin{aligned} \zeta(G(x) \circ \alpha) &= \alpha G(A)Z = (\alpha Z) \text{Diag}(G(A_0), G(S(G_1)), \dots, G(S(G_{m-1})))Z^{-1}Z \\ &= G(x) \circ \alpha Z. \end{aligned}$$

Лемма доказана.

В [2] доказано, что $\zeta(\vec{X}) \in \{0\} \oplus \dots \oplus \{0\} \oplus M(S(G_l)) \oplus \{0\} \oplus \dots \oplus \{0\}$ для всех $l \in \{1, \dots, m-1\}$ и $X \in \text{Ker } G_l(\sigma)$, где ненулевое слагаемое стоит на $(l+1)$ -й позиции. Для всех $i \in \{1, \dots, s\}$ и $d \in \{0, 1, \dots, \tau-1\}$ справедливо включение $Q_{l_i}(d) \in N_{l_i} = \text{Ker } G_{l_i}(\sigma)$, поэтому вектор $\zeta(\vec{Q}_{l_i}(d))$ имеет вид

$$\zeta(\vec{Q}_{l_i}(d)) = (0, \dots, 0, \gamma_{i,d}(0), \gamma_{i,d}(1), \dots, \gamma_{i,d}(m-1), 0, \dots, 0), \quad (27)$$

где элемент $\gamma_{i,d}(0)$ стоит на $(ml_i + 1)$ -й позиции.

Пусть первый столбец матрицы Z^{-1} имеет вид $(*, \dots, *, c_0^{(i)}, c_1^{(i)}, \dots, c_{m-1}^{(i)}, *, \dots, *)^T$, где элемент $c_0^{(i)}$ стоит на $(ml_i + 1)$ -й позиции. Рассмотрим многочлен $C^{(i)}(x) \in R[x]$, определенный равенством

$$C^{(i)}(x) = c_0^{(i)} + c_1^{(i)}x + c_2^{(i)}x^2 + \dots + c_{m-1}^{(i)}x^{m-1}.$$

Обозначим через $\mathbf{1}_1$ вектор-столбец длины m^2 , в котором на первой позиции стоит единица, а на остальных позициях нули.

Лемма 2. Если начальный вектор $\gamma_{i,d}(0, 1, \dots, m-1)$ рекурренты $\gamma_{i,d} \in L_R(G_{l_i})$ определен соотношением (27), то верно равенство

$$\lambda_d^{(i)} = C^{(i)}(x)\gamma_{i,d}.$$

Доказательство. В силу (25), (27) и леммы 1, для всякого $j \geq 0$ имеет место цепочка соотношений

$$\begin{aligned} \lambda_d^{(i)}(j) &= \psi(\sigma^j(Q_{l_i}(d))) = \psi((x^j \circ \vec{Q}_{l_i}(d))e^\downarrow) = (x^j \circ \vec{Q}_{l_i}(d))\mathbf{1}_1 \\ &= (x^j \circ \zeta^{-1}(0, \dots, 0, \gamma_{i,d}(0, 1, \dots, m-1), 0, \dots, 0))\mathbf{1}_1 \\ &= \zeta^{-1}(0, \dots, 0, \gamma_{i,d}(j, \dots, j+m-1), 0, \dots, 0)\mathbf{1}_1 \\ &= (0, \dots, 0, \gamma_{i,d}(j, \dots, j+m-1), 0, \dots, 0)Z^{-1}\mathbf{1}_1 \\ &= (0, \dots, 0, \gamma_{i,d}(j, \dots, j+m-1), 0, \dots, 0)(*, \dots, *, c_0^{(i)}, c_1^{(i)}, \dots, c_{m-1}^{(i)}, *, \dots, *)^T \\ &= \sum_{t=0}^{m-1} c_t^{(i)} \gamma_{i,d}(j+t) = (C^{(i)}(x)\gamma_{i,d})(j). \end{aligned}$$

Лемма доказана.

Лемма 3. Для всех $i \in \{1, \dots, s\}$, $j \geq 0$, $d \in \{0, 1, \dots, \tau-1\}$ верно равенство

$$Q_{l_i}(d + j\tau) = \sigma^j(Q_{l_i}(d)).$$

Доказательство. Согласно (23) справедливо соотношение

$$Q(d + j\tau) = \sigma^j(Q(d)).$$

В силу (21),

$$\sum_{i=1}^s Q_{l_i}(d + j\tau) = \sigma^j \left(\sum_{i=1}^s Q_{l_i}(d) \right) = \sum_{i=1}^s \sigma^j(Q_{l_i}(d)). \quad (28)$$

Для каждого $l \in \{l_1, l_2, \dots, l_s\}$ модуль $N_l = \text{Ker } G_l(\sigma)$ инвариантен относительно σ . Сумма (10) является прямой, поэтому из (28) вытекает доказываемое соотношение. Лемма доказана.

Лемма 2 сводит изучение периодических свойств последовательности $\lambda_d^{(i)}$ к изучению свойств многочлена $C^{(i)}(x) \in R[x]$. Чтобы изучить эти свойства, введем ряд обозначений. Для чисел $a \in \mathbf{Z}$, $b \in \mathbf{N}$ обозначим через $\text{res}_b(a)$ остаток от деления a на b . Рассмотрим отображение $\xi: \mathbf{Z} \oplus \mathbf{Z} \rightarrow \mathbf{Z}_\tau \oplus \mathbf{Z}_\tau$, действующее по правилу

$$\xi(z_0, z_1) = (\text{res}_\tau(z_0), \text{res}_\tau(z_1)).$$

Для каждого $j \geq 0$ обозначим через $\tilde{\mathbf{s}}(j)$ упорядоченную пару $\xi(\mathbf{s}(j))$, где вектор $\mathbf{s}(j)$ определен соотношениями (15), а через $\tilde{s}_0(j)$ и $\tilde{s}_1(j)$ — соответственно первую и вторую компоненту вектора $\tilde{\mathbf{s}}(j)$.

Лемма 4. Если матрица $W(0) \in M$ обладает свойствами (17), то последовательность $\tilde{\mathbf{s}}$ реверсивна, на ее цикле все элементы попарно различны и $T(\tilde{\mathbf{s}}) = \tau^2$.

Доказательство. Согласно лемме 4.1 из [2], управляющая последовательность $\delta \in \mathbf{Z}_2^\infty$ является ЛРП ранга m и периода $\tau = 2^m - 1$. Поэтому в силу (15) для всех $i \geq 0$

$$\begin{aligned} \tilde{\mathbf{s}}(i + \tau^2) &= \xi \left(\sum_{j=0}^{i+\tau^2-1} (1 - \delta(i)), \sum_{j=0}^{i+\tau^2-1} \delta(i) \right) = \tilde{\mathbf{s}}(i) + \xi \left(\sum_{j=i}^{i+\tau^2-1} (1 - \delta(i)), \sum_{j=i}^{i+\tau^2-1} \delta(i) \right) \\ &= \tilde{\mathbf{s}}(i) + \xi \left(\tau \sum_{j=i}^{i+\tau-1} (1 - \delta(i)), \tau \sum_{j=i}^{i+\tau-1} \delta(i) \right) = \tilde{\mathbf{s}}(i). \end{aligned}$$

Отсюда следует, что последовательность $\tilde{\mathbf{s}}$ реверсивна и $T(\tilde{\mathbf{s}}) \mid \tau^2$.

Заметим, что наименьшее общее кратное периодов всех τ -выборок из $\tilde{\mathbf{s}}$ равно $T(\tilde{\mathbf{s}})/(T(\tilde{\mathbf{s}}), \tau)$. Поэтому для того чтобы доказать, что $\tau^2 \mid T(\tilde{\mathbf{s}})$, достаточно показать, что период некоторой τ -выборки из последовательности $\tilde{\mathbf{s}}$ кратен τ . Пусть $\mathbf{v}$ есть регулярная $(0, \tau)$ -выборка из $\tilde{\mathbf{s}}$, то есть $\mathbf{v}(i) = \tilde{\mathbf{s}}(\tau i)$ для всех $i \geq 0$.

Управляющая последовательность δ имеет $(\tau + 1)/2$ единиц и $(\tau - 1)/2$ нулей на своем цикле. Если $t = T(\mathbf{v})$, то для всех $i \geq 0$ справедлива цепочка равенств

$$\begin{aligned} \mathbf{v}(i) &= \mathbf{v}(i + t) = \xi \left(\sum_{j=0}^{\tau(i+t)-1} (1 - \delta(i)), \sum_{j=0}^{\tau(i+t)-1} \delta(i) \right) \\ &= \mathbf{v}(i) + \xi \left(\sum_{j=\tau i}^{\tau(i+t)-1} (1 - \delta(i)), \sum_{j=\tau i}^{\tau(i+t)-1} \delta(i) \right) = \mathbf{v}(i) + \xi(t(\tau - 1)/2, t(\tau + 1)/2). \end{aligned}$$

Таким образом, t есть натуральное решение системы сравнений

$$\begin{aligned} t(\tau - 1)/2 &\equiv 0 \pmod{\tau}, \\ t(\tau + 1)/2 &\equiv 0 \pmod{\tau}, \end{aligned}$$

и следовательно, $\tau \mid t = t(\mathbf{v})$.

Итак, $T(\tilde{\mathbf{s}}) = \tau^2$. Равенство $\tilde{\mathbf{s}}(i) = \tilde{\mathbf{s}}(j)$ в силу (16) влечет равенство $\bar{W}(i) = \bar{W}(j)$. Но тогда в силу (14) выполняется равенство $\delta(i) = \delta(j)$, и справедлива цепочка равенств

$$\tilde{\mathbf{s}}(i + 1) = \tilde{\mathbf{s}}(i) + (1 - \delta(i), \delta(i)) = \tilde{\mathbf{s}}(j) + (1 - \delta(j), \delta(j)) = \tilde{\mathbf{s}}(j + 1).$$

Таким образом, на цикле реверсивной последовательности $\tilde{\mathbf{s}}$ все элементы попарно различны. Лемма доказана.

Согласно (19) $\|Q_{l_i}(j)\| = \|Q_{l_i}\|$ для всех $j \geq 0$, $i \in \{1, \dots, s\}$. Пусть $\eta_i = \|Q_{l_i}\|$. Тогда для всех $j \geq 0$, $i \in \{1, \dots, s\}$

$$Q_{l_i}(j) \equiv U^{\tilde{s}_0(j)} Q_{l_i} V^{\tilde{s}_1(j)} \pmod{2^{\eta_i+1} R_{m \times m}}. \quad (29)$$

Для произвольной последовательности $v \in R^\infty$ обозначим $\|v\|$ максимальное число $k \in \{0, 1, \dots, n\}$ такое, что $v \in 2^k R^\infty$. Для каждой вектор-строки $\alpha \in R^t$ обозначим $\|\alpha\|$ максимальное число $k \in \{0, 1, \dots, n\}$ такое, что $\alpha \in 2^k R^t$.

Лемма 5. Для каждого $i \in \{1, \dots, s\}$ верно соотношение $\bar{C}^{(i)}(x) \neq 0$.

Доказательство. Выберем и зафиксируем $i \in \{1, \dots, s\}$. Пусть последовательность $\lambda^{(i)}$ определена равенством

$$\forall j \geq 0: \quad \lambda^{(i)}(j) = \psi(Q_{l_i}(j)). \quad (30)$$

В силу (25) и леммы 3 последовательности $\lambda_0^{(i)}, \lambda_1^{(i)}, \dots, \lambda_{\tau-1}^{(i)}$ суть соответственно регулярные $(0, \tau), (1, \tau), \dots, (\tau-1, \tau)$ -выборки из последовательности $\lambda^{(i)}$. Согласно введенным обозначениям,

$$\forall d \in \{0, 1, \dots, \tau-1\}: \quad \|Q_{l_i}(d)\| = \eta_i.$$

Поскольку матрица $\bar{Z}$ обратима,

$$\forall \alpha \in R^{m^2}: \quad \|\alpha Z\| = \|\alpha\|.$$

Так как $\gamma_{i,d}$ — ЛРП порядка m , в силу (27) и леммы 1 для каждого $d \in \{0, 1, \dots, \tau-1\}$ справедлива цепочка равенств

$$\|\gamma_{i,d}\| = \|\gamma_{i,d}(0, 1, \dots, m-1)\| = \|\zeta(\bar{Q}_{l_i}(d))\| = \|\bar{Q}_{l_i}(d)Z\| = \|Q_{l_i}(d)\| = \eta_i. \quad (31)$$

Пусть $\bar{C}^{(i)}(x) = 0$. Тогда, в силу леммы 2 и (31), справедливо соотношение

$$\forall d \in \{0, 1, \dots, \tau-1\}: \quad \|\lambda_d^{(i)}\| \geq \eta_i + 1.$$

Отсюда получаем неравенство

$$\|\lambda^{(i)}\| \geq \eta_i + 1. \quad (32)$$

Выберем и зафиксируем пару $(j_0, j_1) \in \{1, \dots, m\} \times \{1, \dots, m\}$. Согласно лемме 4, последовательность $\tilde{s}$ реверсивна, имеет период τ^2 , и на ее цикле все элементы попарно различны. Поэтому любой вектор $(a, b) \in \{0, 1, \tau-1\} \times \{0, 1, \tau-1\}$ встречается на цикле $\tilde{s}$. В частности, существует $j \in \{0, 1, \dots, \tau^2-1\}$ такое, что

$$\tilde{s}(j) = (j_0 - 1, j_1 - 1). \quad (33)$$

Для каждого $k \in \{1, \dots, m\}$ обозначим через $\mathbf{1}_k$ вектор-строку длины m вида $(0, \dots, 0, 1, 0, \dots, 0)$, где 1 стоит на k -й позиции. В силу (29), (30), (32) и (33), справедлива цепочка равенств и сравнимостей по модулю $2^{\eta_i+1} R$

$$\begin{aligned} \mathbf{1}_{j_0} Q_{l_i} \mathbf{1}_{j_1}^T &= \mathbf{1}_1 U^{j_0-1} Q_{l_i} V^{j_1-1} \mathbf{1}_1^T = \mathbf{1}_1 U^{\tilde{s}_0(j)} Q_{l_i} V^{\tilde{s}_1(j)} \mathbf{1}_1^T \\ &\equiv \mathbf{1}_1 Q_{l_i}(j) \mathbf{1}_1^T = \psi(Q_{l_i}(j)) = \lambda^{(i)}(j) \equiv 0, \end{aligned}$$

где символ T означает операцию транспонирования. Поскольку j_0 и j_1 были произвольно выбраны из множества $\{1, \dots, m\}$, получаем, что $\|Q_{l_i}\| \geq \eta_i + 1$. Это противоречит определению величины η_i . Лемма доказана.

Из леммы 1.1 раздела 1 в [7] вытекает следующее утверждение.

Лемма 6. Пусть $R = \mathbf{Z}_{2^n}$, $n \geq 1$, $m \geq 1$, $A \in R_{m \times m}^*$, характеристический многочлен $\chi_A(x)$ матрицы A есть многочлен Галуа. Тогда если для ненулевого вектора $\alpha \in R^m$ через $T_A(\alpha)$ обозначен период последовательности $\alpha, \alpha A, \alpha A^2, \dots, \alpha A^i, \dots$, то для некоторого $c \in \{0, 1, \dots, n - \|\alpha\| - 1\}$ справедливо равенство

$$T_A(\alpha) = 2^c T(\chi_{\bar{A}}(x)).$$

Теперь можно описать периодические свойства последовательности $\lambda_d^{(i)} \in R^\infty$ и указать один из ее минимальных многочленов.

Лемма 7. Для всех $d \in \{0, 1, \dots, \tau - 1\}$, $i \in \{1, \dots, s\}$ последовательность $\lambda_d^{(i)}$ имеет минимальный многочлен $G_{l_i}(x)$ и период

$$T(\lambda_d^{(i)}) = 2^{c_{i,d}} \frac{\tau}{2^{(m, l_i)} - 1},$$

где $0 \leq c_{i,d} \leq n - \eta_i - 1$.

Доказательство. Выберем и зафиксируем $d \in \{0, 1, \dots, \tau - 1\}$, $i \in \{1, \dots, s\}$. Согласно (8), многочлен $G_{l_i}(x)$ является многочленом Галуа, и по лемме 5 справедливо двойное неравенство

$$0 \leq \deg \bar{C}^{(i)}(x) < \deg \bar{G}_{l_i}(x) = m.$$

Следовательно, многочлены $C^{(i)}(x)$ и $G_{l_i}(x)$ взаимно просты, то есть существуют многочлены $A_i(x), B_i(x) \in R[x]$ такие, что $A_i(x)C^{(i)}(x) + B_i(x)G_{l_i}(x) = 1$. Домножая справа обе части последнего равенства на $\gamma_{i,d}$ и пользуясь леммой 2, находим, что

$$\forall d \in \{0, 1, \dots, \tau - 1\}, \quad i \in \{1, \dots, s\}: \quad \gamma_{i,d} = A_i(x)\lambda_d^{(i)}. \quad (34)$$

Применяя (34) и лемму 2, получаем, что для каждого унитарного многочлена $K(x) \in R[x]$

$$K(x)\lambda_d^{(i)} = 0 \iff K(x)\gamma_{i,d} = 0. \quad (35)$$

В частности, отсюда следует, что

$$T(\lambda_d^{(i)}) = T(\gamma_{i,d}). \quad (36)$$

Многочлен $\bar{G}_{l_i}(x)$ неприводим, $\gamma_{i,d} \in L_R(G_{l_i})$, согласно (19) и (31) справедливы равенства

$$\|\gamma_{i,d}\| = \eta_i = \|\mathcal{Q}_{l_i}\| \in \{1, \dots, n - 1\}.$$

Ввиду (36), (8) и леммы 6

$$T(\lambda_d^{(i)}) = T(\gamma_{i,d}) = 2^{c_{i,d}} T(\bar{G}_{l_i}(x)) = 2^{c_{i,d}} T(\mu_{w^{2^{l_i}-1}}(x)) = 2^{c_{i,d}} \frac{\tau}{2^{(m, l_i)} - 1},$$

где $0 \leq c_{i,d} \leq n - \eta_i - 1$. Докажем, что $G_{l_i}(x)$ — минимальный многочлен последовательности $\gamma_{i,d}$. В самом деле, если унитарный многочлен $L(x) \in R[x]$ таков, что

$$0 \leq \deg L(x) < \deg G_{l_i}(x) = m,$$

то многочлены $L(x)$ и $G_{l_i}(x)$ взаимно просты, и аналогично тому, как это было сделано выше, получаем, что

$$T(L(x)\gamma_{i,d}) = T(\gamma_{i,d}) = 2^{c_{i,d}} \frac{\tau}{2^{(m,l_i)} - 1} > 1.$$

Последнее неравенство справедливо, так как $l_i \in \{1, \dots, m-1\}$. Следовательно, $L(x)\gamma_{i,d} \neq 0$ и многочлен $G_{l_i}(x)$ является минимальным для ЛРП $\gamma_{i,d}$. В силу (35) он является минимальным и для ЛРП $\lambda_d^{(i)}$. Лемма доказана.

Всюду далее в этой работе, за исключением раздела 5, считаем, что $W(0)$ — основное состояние. Согласно следствию 4.16 в [2], матрица $W(0) \in M$ является основным состоянием тогда и только тогда, когда она обладает свойствами (17) и

$$(m, l_1, l_2, \dots, l_s) = 1. \quad (37)$$

Введем обозначение

$$v = \min\{\eta_1, \eta_2, \dots, \eta_s\}. \quad (38)$$

Центральным результатом этого раздела является следующее утверждение.

Теорема 1. Если $W(0)$ — основное состояние регистра $\mathfrak{A}^B$ и функция выхода ψ определена равенством (7), то выходная последовательность y есть ЛРП с характеристическим многочленом $F(x)G_{l_1}(x^\tau)G_{l_2}(x^\tau) \dots G_{l_s}(x^\tau)$, где $(l_1, l_2, \dots, l_s)$ — набор чисел из разложения (18) матрицы $W(0)$. При этом

$$T(y) = T(W) = 2^{n-1}\tau^2,$$

где $\tau = 2^m - 1$.

Доказательство. Состояние $W(0)$ является основным, поэтому справедливо соотношение (37). Многочлены $G_{l_1}(x), G_{l_2}(x), \dots, G_{l_s}(x)$ попарно взаимно просты. Используя (24), (37), лемму 7 и лемму 4.14 из [2], для любого $d \in \{0, 1, \dots, \tau-1\}$ получаем цепочку равенств

$$\begin{aligned} T(\lambda_d) &= [T(\lambda_d^{(1)}), T(\lambda_d^{(2)}), \dots, T(\lambda_d^{(s)})] = 2^{c_d} \left[\frac{\tau}{2^{(m,l_1)} - 1}, \frac{\tau}{2^{(m,l_2)} - 1}, \dots, \frac{\tau}{2^{(m,l_s)} - 1} \right] \\ &= 2^{c_d} \frac{\tau}{2^{(m,l_1,l_2,\dots,l_s)} - 1} = 2^{c_d} \tau, \end{aligned}$$

где $c_d = \max\{c_{1,d}, c_{2,d}, \dots, c_{s,d}\}$, $0 \leq c_d \leq n - v - 1$.

Наименьшее общее кратное периодов всех регулярных τ -выборок из λ равно величине $T(\lambda)/(T(\lambda), \tau)$. Отсюда получаем цепочку равенств

$$\frac{T(\lambda)}{(T(\lambda), \tau)} = [T(\lambda_0), T(\lambda_1), \dots, T(\lambda_{\tau-1})] = 2^c \tau,$$

где $c = \max\{c_0, c_1, \dots, c_{\tau-1}\}$, $0 \leq c \leq n - v - 1$. Поэтому $T(\lambda) = 2^c \tau^2$.

Многочлен $G_{l_1}(x)G_{l_2}(x) \dots G_{l_s}(x)$ является характеристическим для последовательности λ_d . Этот многочлен не зависит от d , поэтому он является общим характеристическим многочленом для всех регулярных τ -выборок из λ . Следовательно, многочлен $G_{l_1}(x^\tau)G_{l_2}(x^\tau) \dots G_{l_s}(x^\tau)$ является характеристическим для λ .

Заметим, что многочлены $F(x)$ и $G_{l_1}(x^\tau)G_{l_2}(x^\tau)\dots G_{l_s}(x^\tau)$ взаимно просты. Действительно, пусть у многочленов $\bar{F}(x)$ и $\bar{G}_{l_1}(x^\tau)\bar{G}_{l_2}(x^\tau)\dots\bar{G}_{l_s}(x^\tau)$ в их общем поле разложения есть общий корень ϑ . Тогда $\vartheta^\tau = 1$, и $(x-1) \mid \bar{G}_{l_1}(x)\bar{G}_{l_2}(x)\dots\bar{G}_{l_s}(x)$ по теореме Безу (см. [1]). Это невозможно, так как для каждого $l \in \{l_1, l_2, \dots, l_s\}$ многочлен $\bar{G}_l(x)$ неприводим и имеет степень $m \geq 2$.

Согласно (22), выходная последовательность y представляется в виде $y = u + \lambda$, причем $F(x)$ — минимальный многочлен ЛРП u . Следовательно,

$$T(y) = T(u + \lambda) = [T(u), T(\lambda)] = [2^{n-1}\tau, 2^c\tau^2] = 2^{n-1}\tau^2 = T(W),$$

и многочлен $F(x)G_{l_1}(x^\tau)G_{l_2}(x^\tau)\dots G_{l_s}(x^\tau)$ является характеристическим для выходной последовательности y . Теорема доказана.

Следствие 1. В условиях теоремы 1 справедливо неравенство

$$\text{rank}(y) \leq m^2(2^m - 1) - m(2^m - 2). \quad (39)$$

Доказательство. Из теоремы 1 и того факта, что для каждого $l \in \{1, \dots, m-1\}$ выполняется равенство $\deg G_l(x) = m$, вытекает следующая оценка ранга выходной последовательности y :

$$\text{rank}(y) \leq \deg F(x)G_{l_1}(x^\tau)G_{l_2}(x^\tau)\dots G_{l_s}(x^\tau) = m(\tau s + 1). \quad (40)$$

Учитывая, что $\tau = 2^m - 1$ и $s \leq m - 1$, получаем, что неравенство (40) влечет неравенство (39). Следствие доказано.

Теорема 1 утверждает, что если состояние $W(0)$ основное, а функция выхода ψ определена равенством (7), то период выходной последовательности регистра $\mathfrak{A}^\beta$ совпадает с периодом последовательности его состояний. Изучению ранга выходной последовательности посвящен следующий параграф.

3. Оценки ранга выходной последовательности простейшего самоуправляемого 2-ЛРС

В предыдущем параграфе была найдена верхняя оценка (39) ранга выходной последовательности y . Теперь получим нижнюю оценку ранга последовательности y . С этой целью введем ряд обозначений.

Выберем и зафиксируем $d \in \{0, 1, \dots, \tau - 1\}$, $i \in \{1, \dots, s\}$. В силу леммы 2, $\|\lambda_d^{(i)}\| \geq \|\gamma_{i,d}\|$. Из равенства (34) следует, что $\|\gamma_{i,d}\| \geq \|\lambda_d^{(i)}\|$. Поэтому, принимая во внимание (31), находим, что $\|\lambda_d^{(i)}\| = \eta_i \in \{1, \dots, n-1\}$ для всех $d \in \{0, 1, \dots, \tau - 1\}$ и $i \in \{1, \dots, s\}$. Это означает, что существует ненулевая по модулю радикала последовательность $\mu_d^{(i)} \in R^\infty$ такая, что

$$\lambda_d^{(i)} = 2^{\eta_i} \mu_d^{(i)}. \quad (41)$$

Рассмотрим последовательность $\lambda^{(i)}$, определенную равенством (30). Последовательности $\lambda_d^{(i)}$, $0 \leq d \leq \tau - 1$, суть регулярные τ -выборки из $\lambda^{(i)}$, поэтому существует последовательность $\mu^{(i)} \in R^\infty$ такая, что

$$\lambda^{(i)} = 2^{\eta_i} \mu^{(i)}, \quad (42)$$

и последовательности $\mu_d^{(i)}$, $0 \leq d \leq \tau - 1$, суть регулярные τ -выборки из $\mu^{(i)}$.

Легко показать, что многочлены $F(x)$, $G_{l_1}(x^\tau)$, $G_{l_2}(x^\tau), \dots, G_{l_s}(x^\tau)$ попарно взаимно просты. В силу леммы 7 и поскольку последовательность $\lambda_d^{(i)}$ есть (d, τ) -выборка из $\lambda^{(i)}$, $d = 0, 1, \dots, \tau - 1$, многочлен $G_{l_i}(x^\tau)$ является характеристическим многочленом для последовательности $\lambda^{(i)}$, $i = 1, 2, \dots, s$. Если

$$G(x) = G_{l_1}(x^\tau)G_{l_2}(x^\tau) \dots G_{l_s}(x^\tau),$$

то последовательность $\lambda = \lambda^{(1)} + \lambda^{(2)} + \dots + \lambda^{(s)}$ принадлежит семейству $L_R(G)$, а последовательность $y = u + \lambda$ принадлежит семейству $L_R(FG)$. Рассмотрим разложение

$$L_R(F(x)G(x)) = L_R(F(x)) \dot{+} L_R(G_{l_1}(x^\tau)) \dot{+} L_R(G_{l_2}(x^\tau)) \dot{+} \dots \dot{+} L_R(G_{l_s}(x^\tau)).$$

Пусть $K(x)$ — некоторый минимальный многочлен последовательности y . Для всех $i \in \{1, \dots, s\}$ справедливы равенства $K(x)\lambda^{(i)} = 0$ и $\bar{K}(x)\bar{\mu}^{(i)} = 0$. Для каждого $i \in \{1, \dots, s\}$ обозначим через $g_i(x)$ минимальный многочлен последовательности $\bar{\mu}^{(i)}$. Тогда $g_i(x) \mid \bar{K}(x)$. Поскольку $\bar{K}(x)\bar{u} = 0$, получаем, что $\bar{F}(x) \mid \bar{K}(x)$. Для каждого $i \in \{1, 2, \dots, s\}$ выполняется соотношение $g_i(x) \mid \bar{G}_{l_i}(x^\tau)$. Следовательно, многочлены $\bar{F}(x), g_1(x), g_2(x), \dots, g_s(x)$ попарно взаимно просты. Поэтому верно соотношение $\bar{F}(x)g_1(x)g_2(x) \dots g_s(x) \mid \bar{K}(x)$, и справедлива цепочка

$$\text{rank}(y) = \deg K(x) \geq m + \sum_{i=1}^s \deg g_i(x). \quad (43)$$

Выберем и зафиксируем $i \in \{1, \dots, s\}$. Рассмотрим естественный эпиморфизм

$$R \rightarrow \tilde{R} = R/2^{\eta_i+1}R.$$

Индекс нильпотентности кольца $\tilde{R}$ равен $\eta_i + 1$. Пусть $\tilde{\lambda}_d^{(i)}$ есть образ последовательности $\lambda_d^{(i)}$ под действием указанного эпиморфизма. Тогда согласно лемме 7 и в силу равенства (41) для всех $d \in \{0, 1, \dots, \tau - 1\}$

$$T(\bar{\mu}_d^{(i)}) = T(\tilde{\lambda}_d^{(i)}) = \frac{\tau}{2^{(m, l_i)} - 1}. \quad (44)$$

Последовательности $\bar{\mu}_d^{(i)}$, $0 \leq d \leq \tau - 1$, суть все регулярные τ -выборки из последовательности $\bar{\mu}^{(i)}$. В силу (44),

$$\frac{\tau}{2^{(m, l_i)} - 1} = \frac{T(\bar{\mu}^{(i)})}{(T(\bar{\mu}^{(i)}), \tau)},$$

откуда вытекают следующие оценки для периода последовательности $\bar{\mu}^{(i)}$:

$$\frac{\tau^2}{(2^{(m, l_i)} - 1)^2} \left| T(\bar{\mu}^{(i)}) \right| \frac{\tau^2}{2^{(m, l_i)} - 1}. \quad (45)$$

Эти соотношения позволяют оценить снизу степень многочлена $g_i(x)$ и, следовательно, найти нижнюю оценку ранга выходной последовательности y .

Пусть $l_i \in \{l_1, l_2, \dots, l_s\} \cap \mathbf{Z}_m^*$. Из цепочки соотношений (45) следует, что в этом случае $T(\bar{\mu}^{(i)}) = \tau^2$. В [5] приведен следующий факт, известный в теории чисел как теорема Гжегорчика.

Теорема 2. Если $m \geq 2$, $b \geq 2$ и каждый простой делитель числа $b^m - 1$ делит число $b^k - 1$ при некотором $k \in \{1, \dots, m-1\}$, то либо $m = 2$ и $b + 1$ есть натуральная степень 2, либо $m = 6$ и $b = 2$.

Доказательство можно найти, например, в [11]. Из теоремы 2 вытекает следующее утверждение.

Следствие 2. Для любого $m \geq 2$ существуют простое p и натуральное c такие, что $p^c \mid 2^m - 1$, и для всех натуральных $k < m$ выполняется соотношение $p^c \nmid 2^k - 1$.

Максимальное из чисел p^c , о которых идет речь в следствии 2, обозначим через $d(m)$. Справедлива следующая лемма.

Лемма 8. Если $l_i \in \{l_1, l_2, \dots, l_s\} \cap \mathbf{Z}_m^*$, то

$$\deg g_i(x) \geq md(m).$$

Доказательство. Пусть $d(m) = p^c$, и каноническое разложение многочлена $g_i(x)$ имеет вид $g_i(x) = h_1(x)^{\alpha_1} h_2(x)^{\alpha_2} \dots h_t(x)^{\alpha_t}$, где $h_1, h_2, \dots, h_t$ — попарно различные неприводимые многочлены над $\mathbf{Z}_2$, и для всех $j \in \{1, \dots, t\}$ выполняется неравенство $\alpha_j \geq 1$. Справедливы соотношения $p^{2^c} \mid \tau^2 = T(\bar{\mu}^{(i)}) = T(g_i) = [T(h_1), T(h_2), \dots, T(h_t)]$. Следовательно, существует $j \in \{1, \dots, t\}$ такое, что $p^{2^c} \mid T(h_j)$. Многочлен $h_j(x)$ неприводим, поэтому $T(h_j) \mid 2^k - 1$, где $k = \deg h_j$. Отсюда $2^k \equiv 1 \pmod{p^{2^c}}$. Тогда $p^c \mid (2^m - 1, 2^k - 1) = 2^{(m,k)} - 1$, и по определению величины $d(m) = p^c$ справедливо равенство $(m, k) = m$, то есть $k = mz$ для некоторого $z \in \mathbf{N}$. Ясно, что

$$2^{mz} \equiv 1 \pmod{p^{2^c}}. \quad (46)$$

С другой стороны, $2^{mz} = (1 + \tau)^z \equiv 1 + \tau z \pmod{\tau^2}$, откуда

$$2^{mz} - 1 = \tau z + p^{2^c} w$$

для некоторого $w \in \mathbf{Z}$. Тогда в силу (46) $d(m)^2 = p^{2^c} \mid \tau z$. Согласно определению величины $d(m)$ число p^{c+1} не делит τ . Следовательно, $d(m) = p^c \mid z$. Поэтому справедливо неравенство

$$\deg g_i \geq \deg h_j = k = mz \geq md(m).$$

Лемма доказана.

Пусть теперь $l_i \in \{l_1, l_2, \dots, l_s\} \cap (\mathbf{Z}_m \setminus \mathbf{Z}_m^*)$, $\Delta = (m, l_i)$, $k = \deg g_i(x)$. Тогда в силу (45)

$$\frac{\tau^2}{(2^\Delta - 1)^2} \mid T(\bar{\mu}^{(i)}) = T(g_i) \leq 2^k - 1.$$

Поскольку $l_i \neq 0$, справедливо неравенство $2\Delta \leq m$, и следовательно, $(2^\Delta - 1)^2 < \tau$. Отсюда следует, что $2^k - 1 > \tau = 2^m - 1$, и верна оценка $\deg g_i = k \geq m + 1$. Комбинируя эту оценку с леммой 8 и неравенством (43), получаем, что

$$\text{rank}(y) \geq m + (m + 1)(s - s') + md(m)s',$$

где $s' = |\{l_1, l_2, \dots, l_s\} \cap \mathbf{Z}_m^*|$.

Теорема 3. Во введенных обозначениях для всякого основного состояния $W(0)$ регистра $\mathcal{A}^\beta$ справедливо неравенство

$$\text{rank}(y) \geq m + (m + 1)(s - s') + md(m)s'. \quad (47)$$

Если основное состояние $W(0)$ таково, что в его разложении (18) параметр s равен $m - 1$, то

$$\text{rank}(y) \geq md(m)\varphi(m) + (m + 1)(m - \varphi(m)) - 1, \quad (48)$$

где φ есть функция Эйлера. При $m \rightarrow \infty$ доля таких состояний $W(0)$ среди всех основных состояний стремится к 1. Если состояние $W(0)$ основное и m — простое число, то

$$\text{rank}(y) \geq m(p^c s + 1), \quad (49)$$

где p^c — максимальный простой делитель числа $2^m - 1$. Если состояние $W(0)$ основное и τ — простое число, то

$$\text{rank}(y) = m(\tau s + 1). \quad (50)$$

Доказательство. Если $s = m - 1$, то $s' = \varphi(m)$. Подставляя эти значения в доказанную оценку (47), получаем неравенство (48). Из результатов работы [2] следует, что число основных состояний $W(0)$ не превосходит величины $(2^m - 1)2^{m(n-1)}2^{m(n-1)(m-1)}$, а число основных состояний $W(0)$, у которых $s = m - 1$, выражается формулой $(2^m - 1)2^{m(n-1)}(2^{m(n-1)} - 1)^{m-1}$. Следовательно, доля основных состояний $W(0)$, у которых $s = m - 1$, не менее $(1 - 2^{-m(n-1)})^{m-1}$ и при $m \rightarrow \infty$ она стремится к единице.

Пусть теперь m — простое число. Тогда $s' = s$, и для любого натурального $k < m$ числа $2^m - 1$ и $2^k - 1$ взаимно просты. Поэтому $d(m) = p^c$ есть максимальный простой делитель числа $2^m - 1$. Следовательно, из (47) вытекает (49). Равенство (50) следует из (49) и неравенства (40). Теорема доказана.

Доказанная теорема свидетельствует о том, что ранг выходной последовательности у самоуправляемого регистра $\mathcal{A}^\beta$ достаточно велик. Далее будет изучаться ранг некоторого фиксированного разряда последовательности y в ее двоичном разложении.

4. Усложнение выходной последовательности путем выделения одного из разрядов

Рассмотрим возможность усложнения выходной последовательности y путем выделения некоторого разряда в двоичном разложении

$$y = y_0 + 2y_1 + 2^2y_2 + \dots + 2^{n-1}y_{n-1}.$$

Пусть параметр $\nu \in \{1, \dots, n - 1\}$ определен равенством (38). Из п.2 леммы 4.12 в [2] следует, что для всякой матрицы $X \in M$ включение $X \in N_0$ справедливо тогда и только тогда, когда $UX = XV$. Имеет место следующий факт, позволяющий вычислять параметр ν , не прибегая к разложению (18) матрицы $W(0)$.

Теорема 4. Справедливо равенство

$$\nu = \|UW(0) - W(0)V\|.$$

Доказательство. В силу (18) справедливо равенство

$$UW(0) - W(0)V = \sum_{i=1}^s (UQ_{l_i} - Q_{l_i}V)$$

Как отмечалось в разделе 2, подмодули N_l , $l = 1, 2, \dots, m-1$, инвариантны относительно автоморфизмов φ_0 и φ_1 . Поэтому для каждого $i \in \{1, \dots, s\}$ справедливо включение $UQ_{l_i} - Q_{l_i}V \in N_{l_i}$, и поскольку сумма (10) прямая, верно равенство

$$\|UW(0) - W(0)V\| = \min\{\|UQ_{l_i} - Q_{l_i}V\| \mid 1 \leq i \leq s\}. \quad (51)$$

Пусть $i \in \{1, \dots, s\}$. Напомним, что $\eta_i = \|Q_{l_i}\|$. Существует ненулевая по модулю радикала матрица R_i такая, что $Q_{l_i} = 2^{\eta_i} R_i$. Докажем, что

$$\bar{U}\bar{R}_i - \bar{R}_i\bar{V} \neq 0. \quad (52)$$

Проведем доказательство от противного. Если (52) не выполняется, то

$$UQ_{l_i} \equiv Q_{l_i}V \pmod{2^{\eta_i+1}R_{m \times m}}.$$

Пусть $\tilde{Q}_{l_i}, \tilde{N}_l$ — образы соответственно матрицы Q_{l_i} и подмодуля N_l при естественном эпиморфизме $R \rightarrow R/2^{\eta_i+1}R$. Тогда в силу п. 2 леммы 4.12 в [2]

$$\tilde{Q}_{l_i} \in \tilde{N}_0 \cap \tilde{N}_{l_i}. \quad (53)$$

Так как $\bar{R}_i \neq 0$, матрица $\tilde{Q}_{l_i}$ ненулевая. Поэтому соотношение (53) противоречит тому, что сумма (10) прямая.

Из неравенства (52) следует, что для любого $i \in \{1, \dots, s\}$

$$\|UQ_{l_i} - Q_{l_i}V\| = \eta_i.$$

Отсюда, а также из (38) и (51) следует утверждение теоремы. Теорема доказана.

Изучим свойства координатной последовательности $y_v \in \mathbf{Z}_2^\infty$. В силу (38), для каждого $l \in \{l_1, l_2, \dots, l_s\}$ существует матрица $Z_l \in M$ такая, что $Q_l = 2^v Z_l$. Число ненулевых матриц в ряду

$$\bar{Z}_{l_1}, \bar{Z}_{l_2}, \dots, \bar{Z}_{l_s} \quad (54)$$

обозначим через s_v . Справедливо включение $s_v \in \{1, \dots, s\}$. Пусть ненулевые матрицы в ряду (54) имеют индексы $j_1, j_2, \dots, j_{s_v} \in \{l_1, l_2, \dots, l_s\}$. Введем обозначение

$$s'_v = |\{j_1, j_2, \dots, j_{s_v}\} \cap \mathbf{Z}_m^*|.$$

Очевидно, что $0 \leq s'_v \leq s_v \leq s$. Если m — простое число, то $1 \leq s'_v = s_v \leq s$.

Согласно (22), справедливо равенство $y = u + \lambda$. Рассмотрим образ $\hat{W}(0)$ матрицы $W(0)$ при естественном эпиморфизме $R \rightarrow \hat{R} = R/2^{v+1}R$. Параметры s_v и s'_v суть соответственно параметры s и s' для матрицы $\hat{W}(0)$, и разряд y_v выходной последовательности y выражается формулой

$$y_v = u_v \oplus \bar{\mu}^{(i_1)} \oplus \bar{\mu}^{(i_2)} \oplus \dots \oplus \bar{\mu}^{(i_{s_v})},$$

где $\oplus$ — символ сложения по модулю 2, u_v — разряд с номером v последовательности u , для каждого $k \in \{1, \dots, s_v\}$ число i_k определено равенством $l_{i_k} = j_k$. Как уже отмечалось (см. раздел 2), ЛРП u имеет период $2^{n-1}\tau$, и $F(x)$ — ее минимальный многочлен. Тогда, согласно [3], минимальный многочлен $m_v(x)$ последовательности u_v имеет вид

$$m_v(x) = \bar{F}^{2^{v-1}+1}(x) f_{v,1}^{2^{v-1}}(x) \dots f_{v,j}^{2^{v-1}-j+1}(x) \dots f_{v,2^{v-1}}(x),$$

где $\bar{F}(x) f_{v,1}(x) \dots f_{v,j}(x) \dots f_{v,2^{v-1}}(x) \mid x^\tau - 1$. В частности, это означает, что если a есть некоторый корень многочлена $m_v(x)$ в его поле разложения, то $a^\tau = 1$, и следовательно, a не является корнем ни одного из многочленов $\bar{G}_{j_1}(x^\tau), \bar{G}_{j_2}(x^\tau), \dots, \bar{G}_{j_{s_v}}(x^\tau)$. В разделе 3 было показано, что $g_{i_k}(x) \mid \bar{G}_{j_k}(x^\tau)$ для любого $k \in \{1, \dots, s_v\}$. Поэтому многочлены $m_v(x), g_{i_1}(x), g_{i_2}(x), \dots, g_{i_{s_v}}(x)$ попарно взаимно просты, и минимальный многочлен $\mu_v(x)$ последовательности y_v выражается формулой

$$\mu_v(x) = m_v(x) g_{i_1}(x) g_{i_2}(x) \dots g_{i_{s_v}}(x).$$

Отсюда

$$\text{rank}(y_v) = \text{rank}(u_v) + \sum_{i \in \{i_1, i_2, \dots, i_{s_v}\}} \deg g_i(x).$$

Воспользуемся оценками степеней многочленов $g_i(x)$, полученными в разделе 3. Если $(j_k, m) = 1$, то $\deg g_{i_k} \geq md(m)$, а если $(j_k, m) > 1$, то $\deg g_{i_k} \geq m + 1$. При этом в любом случае

$$\deg g_{i_k}(x) \leq \deg \bar{G}_{j_k}(x^\tau) = m\tau.$$

Отсюда вытекает следующая теорема.

Теорема 5. Во введенных обозначениях для всякого основного состояния $W(0)$ регистра $\mathcal{A}^\beta$ справедливо двойное неравенство

$$(m+1)(s_v - s'_v) + md(m)s'_v \leq \text{rank}(y_v) - \text{rank}(u_v) \leq m\tau s_v. \quad (55)$$

Если основное состояние $W(0)$ таково, что $s_v = m - 1$, то

$$md(m)\varphi(m) + (m+1)(m - \varphi(m) - 1) \leq \text{rank}(y_v) - \text{rank}(u_v) \leq m(m-1)\tau, \quad (56)$$

где φ — функция Эйлера. Если состояние $W(0)$ основное, и m — простое число, то

$$mp^c s_v \leq \text{rank}(y_v) - \text{rank}(u_v) \leq m\tau s_v, \quad (57)$$

где p^c — максимальный примарный делитель числа $2^m - 1$. Если состояние $W(0)$ основное, и τ — простое число, то

$$\text{rank}(y_v) = \text{rank}(u_v) + m\tau s_v, \quad (58)$$

а если к тому же $R = \mathbf{Z}_4$, то

$$\text{rank}(y_1) = m(2^m - 1)s_1 + \frac{m(m+3)}{2}, \quad (59)$$

где $s_1 \in \{1, \dots, m-1\}$.

Доказательство состоит в дословном повторении обоснования теоремы 3 с заменой s на s_v , s' на s'_v и учетом того, что ранг первого разряда ЛРП максимального периода над кольцом $\mathbf{Z}_4$ равен $m(m+3)/2$, где m есть степень любого минимального многочлена этой ЛРП (см. [3]).

Согласно теореме 5, вопрос о ранге последовательности y_v тесно связан с вопросом о ранге последовательности u_v . Для этого последнего ранга в [3] получена оценка

$$\text{rank}(u_v) \geq m(2^{v-1} + 1) + \sum_{t=1}^d \binom{m}{2^{t+1} + 1} (2^{v-1} - 2^t + 1) + \binom{m}{2^v},$$

где $d = \lfloor \log_2(m-2) - 1 \rfloor$. Здесь $\lfloor \cdot \rfloor$ означают целую часть числа (снизу).

5. Частотные характеристики выходной последовательности простейшего самоуправяемого 2-ЛРС над кольцом $\mathbf{Z}_4$

Пусть $R = \mathbf{Z}_4$, автомат $\mathcal{A}_1^\beta$ получен из регистра $\mathcal{A}^\beta$ путем выделения первого разряда выходной последовательности y , и разложение (11) матрицы $W(0) \in M$ имеет вид

$$W(0) = P + Q_l, \quad (60)$$

где $l \in \{1, \dots, m-1\}$, $\bar{P} \neq 0$, $Q_l \neq 0$, $\bar{Q}_l = 0$. Матрица $W(0)$ вида (60) в общем случае не является основным состоянием. Согласно [2], последовательность состояний W имеет в этой ситуации период

$$T(W) = \frac{2\tau^2}{2^{(m,l)} - 1}. \quad (61)$$

Рассмотрим выходную последовательность y_1 автомата $\mathcal{A}_1^\beta$. В силу (22), последовательность $y_1 \in \mathbf{Z}_2^\infty$ представляется в виде

$$y_1 = u_1 \oplus \varepsilon, \quad (62)$$

где u_1 и ε суть первые разряды последовательностей u и λ соответственно, $\oplus$ есть символ сложения по модулю 2. Цель этого параграфа — оценить число нулей и единиц на цикле последовательности (62).

Пусть $d \in \{0, 1, \dots, \tau-1\}$. Для каждой последовательности $v \in \mathbf{Z}_2^\infty$ обозначим через $v^{(d,\tau)}$ регулярную (d, τ) -выборку из v . Тогда из (62) следует соотношение

$$y_1^{(d,\tau)} = u_1^{(d,\tau)} \oplus \varepsilon^{(d,\tau)}, \quad (63)$$

причем в силу равенства $\lambda = 2\varepsilon$, леммы 7 и соотношений (8), последовательность $\varepsilon^{(d,\tau)} \in \mathbf{Z}_2^\infty$ имеет минимальный многочлен $\bar{G}_l(x) = \mu_{w^{2^l-1}}(x)$. Этот многочлен имеет степень $m \geq 2$ и, очевидно, неприводим.

Изучим сначала частотные характеристики $\varepsilon^{(d,\tau)}$. В [10] доказана следующая теорема.

Теорема 6. Пусть $P = GF(q)$, $f(x) \in P[x]$ — унитарный неприводимый многочлен степени $m \geq 2$, $v \in L_P(f) \setminus \{0\}$, $T = T(v)$, $h = [T, q-1]$, $\Delta = (q^m - 1)/T$, $N_z(v)$ — число знаков z на цикле последовательности v , $z \in P$. Тогда

$$\left| N_0(v) - \frac{q^{m-1} - 1}{q^m - 1} T \right| \leq \frac{q-1}{q} \left(\frac{T}{h} - \frac{1}{\Delta} \right) q^{m/2},$$

а при $z \neq 0$

$$\left| N_z(v) - \frac{q^{m-1}}{q^m - 1} T \right| \leq \left(\frac{T}{h} - \frac{1}{\Delta} + \frac{h-T}{h} \sqrt{q} \right) q^{m/2-1}.$$

В качестве последовательности v , о которой идет речь в теореме 6, возьмем последовательность $\varepsilon^{(d,\tau)}$. Тогда $q = 2$, $h = T$, и в силу леммы 7 верны равенства

$$T = \frac{\tau}{2^{(m,l)} - 1}, \quad \Delta = 2^{(m,l)} - 1.$$

Подставив эти значения в формулы теоремы 6, получим, что справедливо следующее утверждение.

Лемма 9. Во введенных обозначениях справедливы неравенства

$$\begin{aligned} \left| N_0(\varepsilon^{(d,\tau)}) - \frac{2^{m-1} - 1}{2^{(m,l)} - 1} \right| &\leq \frac{1}{2} \left(1 - \frac{1}{2^{(m,l)} - 1} \right) 2^{m/2}, \\ \left| N_1(\varepsilon^{(d,\tau)}) - \frac{2^{m-1}}{2^{(m,l)} - 1} \right| &\leq \frac{1}{2} \left(1 - \frac{1}{2^{(m,l)} - 1} \right) 2^{m/2}. \end{aligned}$$

Рассмотрим теперь последовательность $u_1^{(d,\tau)} \in \mathbf{Z}_2^\infty$. Поскольку $T(u_1) = 2\tau$, а $u_1^{(d,\tau)}$ есть регулярная τ -выборка из u_1 , справедливо включение $T(u_1^{(d,\tau)}) \in \{1, 2\}$, то есть для каждого $d \in \{0, 1, \dots, \tau-1\}$ имеет место одна из следующих ситуаций:

- (а) $u_1^{(d,\tau)} = (0, 0, 0, 0, \dots)$,
- (б) $u_1^{(d,\tau)} = (1, 1, 1, 1, \dots)$,
- (в) $u_1^{(d,\tau)} = (0, 1, 0, 1, \dots)$,
- (г) $u_1^{(d,\tau)} = (1, 0, 1, 0, \dots)$.

Ближайшая задача — оценить число знаков 0 и 1 на цикле последовательности $u_1^{(d,\tau)}$ в каждой из этих ситуаций. Выберем и зафиксируем произвольную регулярную 2-выборку v из последовательности $\varepsilon^{(d,\tau)}$. Если $\theta = w^{2^l-1}$, то существует $\alpha \in GF(2^m)$ такое, что для всех $i \geq 0$

$$\varepsilon^{(d,\tau)}(i) = \text{tr}_2^{2^m}(\alpha \theta^i), \quad (64)$$

где $\text{tr}_2^{2^m}$ есть функция след из $GF(2^m)$ в $\mathbf{Z}_2$. Поскольку величина

$$T(\varepsilon^{(d,\tau)}) = \frac{2^m - 1}{2^{(m,l)} - 1}$$

нечетна, 2-выборка ν является ненулевой. Если ν есть $(k, 2)$ -выборка, а $\alpha_1 = \alpha \theta^k$, то в силу (64) справедлива цепочка равенств

$$\forall i \geq 0: \quad \nu(i) = \varepsilon^{(d, \tau)}(k + 2i) = \text{tr}_2^{2^m}(\alpha_1 \theta^{2i}),$$

поэтому согласно теореме 10 на с. 314 в т. 2 в [1] минимальный многочлен $\mu_{\theta^2}(x)$ элемента θ^2 над полем $\mathbf{Z}_2$ есть минимальный многочлен последовательности ν . Для дальнейшего изложения потребуется следующее утверждение.

Лемма 10. *Во введенных обозначениях*

$$\deg \mu_{\theta^2}(x) = m.$$

Доказательство. Согласно описанию корней неприводимого многочлена над конечным полем (см., например, [1]), степень многочлена $\mu_{\theta^2}(x)$ равна минимальному $k \in \mathbf{N}$ такому, что

$$\theta^{2 \cdot 2^k} = \theta^2. \quad (65)$$

Поскольку $\text{ord } \theta = T(\varepsilon^{(d, \tau)}) = (\tau / (2^{(m, l)} - 1))$, равенство (65) равносильно сравнению

$$2^{k+1} \equiv 2 \pmod{\frac{\tau}{2^{(m, l)} - 1}},$$

что, в свою очередь, эквивалентно сравнению

$$2^k \equiv 1 \pmod{\tau / (2^{(m, l)} - 1)}. \quad (66)$$

Согласно следствию 4.4 из [2], минимальное $k \in \mathbf{N}$ со свойством (66) равно m . Лемма доказана.

Рассмотрим частотные характеристики последовательности $y_1^{(d, \tau)}$.

Лемма 11. *В ситуации (а)*

$$\begin{aligned} \left| N_0(y_1^{(d, \tau)}) - \frac{2^{m-1} - 1}{2^{(m, l)} - 1} \right| &\leq \frac{1}{2} \left(1 - \frac{1}{2^{(m, l)} - 1} \right) 2^{m/2}, \\ \left| N_1(y_1^{(d, \tau)}) - \frac{2^{m-1}}{2^{(m, l)} - 1} \right| &\leq \frac{1}{2} \left(1 - \frac{1}{2^{(m, l)} - 1} \right) 2^{m/2}. \end{aligned}$$

В ситуации (б)

$$\begin{aligned} \left| N_0(y_1^{(d, \tau)}) - \frac{2^{m-1}}{2^{(m, l)} - 1} \right| &\leq \frac{1}{2} \left(1 - \frac{1}{2^{(m, l)} - 1} \right) 2^{m/2}, \\ \left| N_1(y_1^{(d, \tau)}) - \frac{2^{m-1} - 1}{2^{(m, l)} - 1} \right| &\leq \frac{1}{2} \left(1 - \frac{1}{2^{(m, l)} - 1} \right) 2^{m/2}. \end{aligned}$$

В ситуациях (в) и (г) для каждого $z \in \{0, 1\}$

$$\left| N_z(y_1^{(d, \tau)}) - \frac{2^m - 1}{2^{(m, l)} - 1} \right| \leq \left(1 - \frac{1}{2^{(m, l)} - 1} \right) 2^{m/2}. \quad (67)$$

Доказательство. Ввиду (63) и леммы 9, доказывать надо лишь неравенство (67). Как показано выше, всякая регулярная 2-выборка v из последовательности $\varepsilon^{(d,\tau)}$ есть ЛРП ранга m с минимальным многочленом $\mu_{\theta^2}(x)$. В обозначениях теоремы 6

$$q = 2, \quad h = T, \quad T = T(v) = \text{ord } \theta^2 = \frac{\tau}{2^{(m,l)} - 1}, \quad \Delta = 2^{(m,l)} - 1.$$

Подставив эти значения в формулы теоремы 6, получим, что

$$\begin{aligned} \left| N_0(v) - \frac{2^{m-1} - 1}{2^{(m,l)} - 1} \right| &\leq \frac{1}{2} \left(1 - \frac{1}{2^{(m,l)} - 1} \right) 2^{m/2}, \\ \left| N_1(v) - \frac{2^{m-1}}{2^{(m,l)} - 1} \right| &\leq \frac{1}{2} \left(1 - \frac{1}{2^{(m,l)} - 1} \right) 2^{m/2}. \end{aligned} \quad (68)$$

Поскольку величина $T(\varepsilon^{(d,\tau)})$ нечетна, из равенства $T(u_1^{(d,\tau)}) = 2$ и соотношения (63) следует, что

$$T(y_1^{(d,\tau)}) = 2T(\varepsilon^{(d,\tau)}) = \frac{2\tau}{2^{(m,l)} - 1} = 2T(v). \quad (69)$$

Пусть v_0 и v_1 суть соответственно регулярная $(0, 2)$ -выборка и регулярная $(1, 2)$ -выборка из $\varepsilon^{(d,\tau)}$. Цепочка равенств (69) верна для любой 2-выборки v из последовательности $\varepsilon^{(d,\tau)}$. В частности, она верна для v_0 и v_1 . Поэтому для всех $z \in \{0, 1\}$

$$T(y_1^{(d,\tau)}) = 2T(v_z). \quad (70)$$

Выберем и зафиксируем $z \in \{0, 1\}$. Пусть $e = u_1^{(d,\tau)}(0) \in \{0, 1\}$. Так как $T(u_1^{(d,\tau)}) = 2$, в силу (63), (70),

$$N_z(y_1^{(d,\tau)}) = N_{z \oplus e}(v_0) + N_{z \oplus e \oplus 1}(v_1), \quad (71)$$

где $\oplus$ — символ сложения по модулю 2. Неравенства (68) справедливы для любой 2-выборки v из последовательности $\varepsilon^{(d,\tau)}$. В частности,

$$\begin{aligned} \left| N_{z \oplus e}(v_0) - \frac{2^{m-1} - 1}{2^{(m,l)} - 1} \right| &\leq \frac{1}{2} \left(1 - \frac{1}{2^{(m,l)} - 1} \right) 2^{m/2}, \\ \left| N_{z \oplus e \oplus 1}(v_1) - \frac{2^{m-1}}{2^{(m,l)} - 1} \right| &\leq \frac{1}{2} \left(1 - \frac{1}{2^{(m,l)} - 1} \right) 2^{m/2}. \end{aligned}$$

Отсюда и из (71) следует неравенство (67). Лемма доказана.

Для $z \in \{0, 1\}$ обозначим через p_z величину $N_z(y_1)/T(y_1)$. Величина p_z есть относительная частота появления знака z на цикле последовательности y_1 . Сформулируем и докажем центральный результат этого раздела.

Теорема 7. Во введенных обозначениях для каждого $z \in \{0, 1\}$ справедливо неравенство

$$\left| p_z - \frac{1}{2} \right| \leq \frac{1}{2\tau} (2^{m/2+(m,l)} - 2^{m/2+1} + 1). \quad (72)$$

Доказательство. Для $r \geq 1$, $v \in \mathbf{Z}_2^\infty$, $z \in \{0, 1\}$ обозначим через $N_z^r(v)$ число знаков z на отрезке $v(0), v(1), \dots, v(r-1)$.

Пусть

$$t = \frac{2\tau}{2^{(m,l)} - 1}.$$

В ситуациях (а) и (б) выполняется равенство $t = 2T(y_1^{(d,\tau)})$. Поэтому из леммы 11 в этом случае следуют неравенства

$$\begin{aligned} \frac{2^m - 2}{2^{(m,l)} - 1} - \left(1 - \frac{1}{2^{(m,l)} - 1}\right) 2^{m/2} &\leq N_z^t(y_1^{(d,\tau)}) \\ &\leq \frac{2^m}{2^{(m,l)} - 1} + \left(1 - \frac{1}{2^{(m,l)} - 1}\right) 2^{m/2}, \end{aligned} \quad (73)$$

выполняющиеся для всех $z \in \{0, 1\}$.

В ситуациях (в) и (г) верно равенство

$$t = T(y_1^{(d,\tau)}),$$

поэтому согласно лемме 11 для каждого $z \in \{0, 1\}$ выполняются неравенства

$$\begin{aligned} \frac{2^m - 1}{2^{(m,l)} - 1} - \left(1 - \frac{1}{2^{(m,l)} - 1}\right) 2^{m/2} &\leq N_z^t(y_1^{(d,\tau)}) \\ &\leq \frac{2^m - 1}{2^{(m,l)} - 1} + \left(1 - \frac{1}{2^{(m,l)} - 1}\right) 2^{m/2}. \end{aligned} \quad (74)$$

Интервал (73), очевидно, шире интервала (74). Поэтому неравенства (73) выполняются независимо от вида последовательности $u_1^{(d,\tau)}$.

В силу (61) выполняется равенство $T(W) = \tau t$, а последовательность $y_1^{(d,\tau)}$ есть регулярная (d, τ) -выборка из y_1 , $d = 0, 1, \dots, \tau - 1$. Следовательно, неравенства (73) влекут неравенства

$$\begin{aligned} \frac{2^m - 2}{2^{(m,l)} - 1} \tau - \left(1 - \frac{1}{2^{(m,l)} - 1}\right) 2^{m/2} \tau &\leq N_z^{T(W)}(y_1) \\ &\leq \frac{2^m}{2^{(m,l)} - 1} \tau + \left(1 - \frac{1}{2^{(m,l)} - 1}\right) 2^{m/2} \tau. \end{aligned}$$

Разделив все части этого соотношения на $T(W)$, получим, что

$$\begin{aligned} &\left(\frac{2^m - 2}{2^{(m,l)} - 1} \tau - \left(1 - \frac{1}{2^{(m,l)} - 1}\right) 2^{m/2} \tau\right) \frac{1}{T(W)} \\ &= \left(\frac{2^m - 2}{2^{(m,l)} - 1} \tau - \left(1 - \frac{1}{2^{(m,l)} - 1}\right) 2^{m/2} \tau\right) \frac{2^{(m,l)} - 1}{2\tau^2} \\ &= \frac{1}{2} - \frac{1}{2\tau} (2^{m/2+(m,l)} - 2^{m/2+1} + 1), \\ &\left(\frac{2^m}{2^{(m,l)} - 1} \tau + \left(1 - \frac{1}{2^{(m,l)} - 1}\right) 2^{m/2} \tau\right) \frac{1}{T(W)} \\ &= \left(\frac{2^m}{2^{(m,l)} - 1} \tau + \left(1 - \frac{1}{2^{(m,l)} - 1}\right) 2^{m/2} \tau\right) \frac{2^{(m,l)} - 1}{2\tau^2} \\ &= \frac{1}{2} + \frac{1}{2\tau} (2^{m/2+(m,l)} - 2^{m/2+1} + 1), \end{aligned}$$

$$N_z^{T(W)}(y_1) \frac{1}{T(W)} = \frac{T(W)}{T(y_1)} N_z(y_1) \frac{1}{T(W)} = p_z.$$

В результате получаем неравенства

$$\frac{1}{2} - \frac{1}{2\tau} \left(2^{m/2+(m,l)} - 2^{m/2+1} + 1 \right) \leq p_z \leq \frac{1}{2} + \frac{1}{2\tau} \left(2^{m/2+(m,l)} - 2^{m/2+1} + 1 \right),$$

эквивалентные неравенству (72). Теорема доказана.

При всех значениях $m \geq 2$, $l \in \{1, \dots, m-1\}$ оценка (72) нетривиальна. Если состояние $W(0)$ основное, то в силу (37) числа m и l взаимно просты. Оценка (72) приобретает в этом случае вид

$$\forall z \in \{0, 1\}: |p_z - 1/2| \leq \frac{1}{2\tau}. \quad (75)$$

Неравенство (75), в частности, свидетельствует, что усложненная путем выделения первого разряда выходная последовательность асимптотически равновероятна при $m \rightarrow \infty$.

6. Сравнение свойств одномерного и двумерного регистров сдвига

Результаты данной работы и результаты работы [2] позволяют сравнить одномерный и двумерный линейные регистры сдвига по следующим параметрам.

1. Максимальная длина цикла в графе переходов состояний и максимальный период выходной последовательности при полном переборе всех начальных заполнений.
2. Число вершин, лежащих на циклах максимальной длины в графе переходов состояний.
3. Максимальный ранг выходной последовательности при полном переборе начальных заполнений, лежащих на циклах максимальной длины.

Пусть $R = \mathbf{Z}_4$, число $2^m - 1$ простое, $G(x) \in R[x]$ — многочлен максимального периода степени m^2 , $F(x) \in R[x]$ — многочлен максимального периода степени m . Будем сравнивать 1-ЛРС с характеристическим многочленом $G(x)$ и функцией выхода ψ_1 , определенной равенством

$$\psi_1(x_1, x_2, \dots, x_{m^2}) = x_1,$$

и простейший самоуправляемый 2-ЛРС $\mathcal{A}^\beta$, частичные функции перехода которого определены соотношениями (3), а функция выхода ψ_2 задана равенством

$$\forall X \in M: \psi_2(X) = x_{1,1}.$$

Выходную последовательность y в обоих случаях будем усложнять путем выделения первого разряда y_1 в двоичном разложении y . Используя результаты работ [2], [3], а также доказанные в разделах 3 и 4 оценки ранга выходной последовательности, получаем следующую таблицу:

Параметр	1-ЛРС	2-ЛРС
Объем накопителя	m^2	m^2
Макс. длина цикла в графе переходов состояний	$2(2^{m^2} - 1)$	$2(2^m - 1)^2$
Число вершин, лежащих на циклах макс. длины	$4^{m^2} - 2^{m^2}$	$(2^m - 1)(2^{m^2} - 2^m)$
Макс. ранг выходной последовательности y	m^2	$m(m-1)(2^m - 1) + m$
Макс. ранг усложненной выходной последовательности y_1	$\frac{m^2(m^2+3)}{2}$	$m(m-1)(2^m - 1) + \frac{m(m+3)}{2}$

Из таблицы следует, что 2-ЛРС по сравнению с 1-ЛРС имеет меньше состояний, принадлежащих циклам максимальной длины, и меньшую максимальную длину цикла, однако его выходная последовательность имеет значительно больший ранг.

Второй способ сравнить 1-ЛРС и 2-ЛРС с точки зрения ранга вырабатываемой последовательности состоит в следующем. Пусть $y_1^{(1)}$ — первая координатная последовательность выхода $y^{(1)}$ одномерного ЛРС над $\mathbf{Z}_4$ с характеристическим многочленом $G(x)$, а $y_1^{(2)}$ — первая координатная последовательность выхода $y^{(2)}$ двумерного ЛРС $\mathfrak{A}^\beta$ над $\mathbf{Z}_4$. Согласно [3], если начальное заполнение 1-ЛРС является ненулевым по модулю радикала, то

$$\text{rank}(y_1^{(1)}) = \frac{m^2(m^2 + 3)}{2}.$$

Из результатов раздела 4 (теорема 5) вытекает, что если $W(0)$ — основное состояние, число $2^m - 1$ простое, и в разложении (18) матрицы $W(0)$ параметр s равен $m - 1$, то

$$\text{rank}(y_1^{(2)}) = m(m-1)(2^m - 1) + \frac{m(m+3)}{2}.$$

Обозначим $\text{rank}(y_1^{(1)})$ через μ . Будем усложнять последовательность $y_1^{(1)}$ над полем $\mathbf{Z}_2$ с помощью полинома $\Phi(x_1, x_2, \dots, x_k) \in \mathbf{Z}_2[x_1, x_2, \dots, x_k]$, то есть рассмотрим последовательность $v^{(1)}$ над полем $\mathbf{Z}_2$, определенную равенствами

$$\forall i \geq 0: \quad v^{(1)}(i) = \Phi(y_1^{(1)}(i), y_1^{(1)}(i+1), \dots, y_1^{(1)}(i+k-1)).$$

В силу [3], минимальный многочлен последовательности $y_1^{(1)}$ имеет вид $\bar{G}(x)^2 g_{1,1}(x)$, где $G(x)g_{1,1}(x) \mid x^{2^{m^2}-1} - 1$. Отсюда и из теоремы 2 в [4] получаем неравенство

$$\text{rank}(v^{(1)}) \leq \sum_{j=0}^r \binom{\mu + j - 1}{j} (j + 1), \quad (76)$$

где $r = \deg \Phi$. Обозначим r_0 минимальное число $r \in \mathbf{N}$, для которого существуют полином Φ степени r и начальное заполнение 1-ЛРС такие, что

$$\text{rank}(v^{(1)}) \geq m(m-1)(2^m - 1) + \frac{m(m+3)}{2}.$$

Если такого r_0 нет, будем считать, что $r_0 = \infty$. Величина r_0 показывает, насколько выходная последовательность самоуправляемого 2-ЛРС сложнее выходной последовательности 1-ЛРС.

Оценим величину r_0 для значений $m \in \{2, 3, 5, 7, 13, 17, 19, 31, 127\}$. Согласно [1] для всех таких m число $2^m - 1$ является простым. Из приведенной выше таблицы видно, что если $m \in \{2, 3\}$, то

$$\text{rank}(y_1^{(1)}) \geq m(m-1)(2^m - 1) + \frac{m(m+3)}{2},$$

и следовательно, $r_0 = 1$. В случае $m = 5$ для любого начального заполнения одномерного ЛРС

$$\text{rank}(y_1^{(1)}) < m(m-1)(2^m-1) + \frac{m(m+3)}{2}.$$

Поэтому $r_0 \geq 2$. Согласно (76) для $m > 5$ в качестве нижней оценки r_0 можно взять минимальное натуральное r , удовлетворяющее неравенству

$$m(m-1)(2^m-1) + \frac{m(m+3)}{2} \leq \sum_{j=0}^r \binom{(m^2(m^2+3)/2 + j - 1)}{j} (j+1).$$

Отсюда получаем нижние оценки для r_0 , приведенные в следующей таблице:

m	2	3	5	7	13	17	19	31	127
$r_0 \geq$	1	1	2	2	2	2	2	3	6

К примеру, в случае $m = 127$ для того, чтобы 1-ЛРС давал выходную последовательность не менее сложную, чем выходная последовательность 2-ЛРС, одномерный регистр должен быть усложнен полиномом Φ , степень которого не меньше 6.

Наконец, третий способ сравнить 1-ЛРС и самоуправляемый 2-ЛРС заключается в том, чтобы сопоставить ранги последовательности y_1 , первого разряда выходной последовательности y регистра $\mathfrak{A}^\beta$ над кольцом $\mathbf{Z}_4$, и последовательности γ , полученной путем усложнения с помощью полинома Φ текущего заполнения одномерного линейного регистра сдвига над $\mathbf{Z}_2$, имеющего накопитель длины $2m^2$ и характеристический многочлен максимального периода $4m^2 - 1$ ($2m^2$ есть число битов в начальном заполнении регистра $\mathfrak{A}^\beta$ над кольцом $\mathbf{Z}_4$). Согласно [9], если $\deg \Phi = r$, то максимальный возможный ранг последовательности γ выражается формулой

$$\text{rank}(\gamma) = \sum_{j=1}^r \binom{2m^2}{j}.$$

Как уже отмечалось, если $W(0)$ — основное состояние, число $2^m - 1$ простое, и в разложении (18) матрицы $W(0)$ параметр s равен $m - 1$, то

$$\text{rank}(y_1^{(2)}) = m(m-1)(2^m-1) + \frac{m(m+3)}{2}.$$

Обозначим через r_1 минимальное число r , для которого выполняется неравенство

$$\sum_{j=1}^r \binom{2m^2}{j} \geq m(m-1)(2^m-1) + \frac{m(m+3)}{2}.$$

Величина r_1 показывает, насколько выходная последовательность y_1 самоуправляемого регистра $\mathfrak{A}^\beta$ сложнее выходной последовательности фильтрующего генератора с длиной накопителя $2m^2$. В следующей таблице приведены значения r_1 для каждого $m \in \{2, 3, 5, 7, 13, 17, 19, 31, 127\}$:

m	2	3	5	7	13	17	19	31	127
r_1	2	2	2	3	3	4	4	5	12

Таким образом, все три способа сравнения регистров показывают, что выходная последовательность самоуправляемого 2-ЛРС значительно сложнее выходной последовательности 1-ЛРС с тем же объемом накопителя. Результаты раздела 5 свидетельствуют о том, что выходная последовательность простейшего самоуправляемого 2-ЛРС над кольцом $\mathbf{Z}_4$, усложненная путем выделения первого разряда, статистически близка к равновероятной.

Автор выражает глубокую признательность А. А. Нечаеву за постановку задачи, обсуждение полученных результатов и существенную помощь при подготовке этой статьи, О. В. Камловскому за методические указания, а также Б. А. Погорелову за ценные замечания по тексту.

Список литературы

1. Глухов М. М., Елизаров В. П., Нечаев А. А., *Алгебра*. Гелиос-АРВ, Москва, 2003.
2. Козлитин О. А., Периодические свойства простейшего 2-линейного регистра сдвига. *Дискретная математика* (2007) **19**, №3, 51–78.
3. Кузьмин А. С., Нечаев А. А., Линейные рекуррентные последовательности над кольцами Галуа. *Алгебра и логика* (1995) **34**, №2, 169–189.
4. Куракин В. Л., Полиномиальные преобразования линейных рекуррентных последовательностей над конечными коммутативными кольцами. *Дискретная математика* (2000) **12**, №3, 3–36.
5. Лидл Р., Нидеррайтер Г., *Конечные поля*. Мир, Москва, 1988.
6. Нечаев А. А., О подобии матриц над коммутативным локальным артиновым кольцом. *Труды семинара им. И. Г. Петровского* (1983) **9**, 81–101.
7. Нечаев А. А., Цикловые типы линейных подстановок над конечными коммутативными кольцами. *Матем. сб.* (1993) **184**, №3, 21–56.
8. Фомичев В. М., *Дискретная математика и криптология*. Диалог–МИФИ, Москва, 2003.
9. Key E. L., An analysis of the structure and complexity of nonlinear binary sequence generators. *IEEE Trans. Inform. Theory* (1976) **22**, №6, 732–736.
10. Niederreiter H., Weights of cyclic codes. *Inform. Control* (1977) **34**, №2, 130–140.
11. Zsigmondy K., Zur Theorie der Potenzreste. *Monatsh. f. Math.* (1892) **3**, 265–284.

Статья поступила 15.11.2006.