Math-Net.Ru

Общероссийский математический портал

О. А. Козлитин, 2-линейный регистр сдвига над кольцом Га-
луа четной характеристики, *Матем. вопр. криптогр.*, 2012,
том 3, выпуск 2, 27–61

DOI: <https://doi.org/10.4213/mvk53>

Использование Общероссийского математического портала Math-Net.Ru подразуме-
вает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 34.229.108.108

26 апреля 2023 г., 13:13:20

УДК: 511.216+519.113.6

2-линейный регистр сдвига над кольцом Галуа четной характеристики

О. А. Козлитин

ООО «Центр сертификационных исследований», Москва

Получено 20.V.2011

Исследуются свойства выходной последовательности самоуправляемого 2-линейного регистра сдвига над кольцом Галуа четной характеристики. Показано, что для широкого класса функций самоуправления и при надлежащем выборе функции выхода почти все начальные заполнения индуцируют выходную последовательность высокой линейной сложности и максимально возможного периода. По своим частотным характеристикам эта последовательность близка к равномерной.

Ключевые слова: 2-линейные регистры сдвига, максимальный период, линейная сложность, частотные характеристики

2-linear shift register over the Galois ring of even characteristic

O. A. Kozlitin

LLC "Certification Research Center", Moscow

Abstract. Output sequence properties of self-controlled 2-linear shift register over the Galois ring of even characteristic are investigated. It is shown that almost all initial values generate the output sequence with large linear complexity and maximal possible period for a wide class of control functions and proper choice of an output function. Frequency characteristics of this sequence are close to that of a uniform one.

Key words: 2-linear shift registers, maximal period, linear complexity, frequency characteristics

Citation: *Mathematical Aspects of Cryptography*, 2012, vol. 3, no. 2, pp. 27–61 (Russian).

Работа выполнена при поддержке гранта Президента РФ НШ-8.2010.10.

§ 1. Введение

Двумерный линейный регистр сдвига (2-линейный регистр сдвига, 2-ЛРС) является естественным многомерным обобщением стандартного (одномерного) линейного регистра сдвига. Первоначально 2-ЛРС был предложен японскими математиками Nomura и Fukuda [12] в качестве кодера и декодера двумерного циклического кода. Позже отечественные специалисты указали на возможность использования полилинейного регистра для выработки псевдослучайных последовательностей (см., например, [6] и [10]). В работе [1] исследованы периодические свойства генератора псевдослучайных последовательностей (ПСП), построенного на основе 2-линейного регистра сдвига (2-ЛРС) над кольцом вычетов $\mathbb{Z}_{2^n}$ с линейной функцией самоуправления. В работе [2] показано, что выходная последовательность этого генератора обладает большим рангом и хорошими частотными характеристиками. Работа [3] обобщает результаты [1] на случай произвольного кольца Галуа четной характеристики. В настоящей работе исследуются криптографические свойства выходной последовательности самоуправляемого 2-ЛРС, функция самоуправления которого, вообще говоря, нелинейна.

Пусть $r, n \in \mathbb{N}$, $q = 2^r$, $R = GR(q^n, 2^n)$ — кольцо Галуа мощности q^n и характеристики 2^n , $F(x) \in R[x]$ — многочлен максимального периода степени $m \geq 2$. Обозначим через $e_{i,j}$ матричную единицу, т.е. матрицу размера $m \times m$, в которой на пересечении i -й строки и j -го столбца стоит 1, а на остальных позициях — 0 (счет строк и столбцов будем вести с нуля). Обозначим через $e^\downarrow$ записанный столбцом базис R -бимодуля $R_{m,m}$, состоящий из матричных единиц в следующем порядке:

$$e_{0,0}, \dots, e_{0,m-1}, e_{1,0}, \dots, e_{1,m-1}, \dots, e_{m-1,0}, \dots, e_{m-1,m-1},$$

и определим автоморфизмы φ_0 и φ_1 бимодуля $R_{m,m}$ соотношением

$$\varphi_x(w) = \vec{w} \cdot (S(F)^{1-x} \otimes S(F)^x) \cdot e^\downarrow, \quad x \in \{0, 1\}.$$

Здесь $\vec{w}$ — строка координат матрицы $w \in R_{m,m}$ в базисе $e^\downarrow$, $\otimes$ — операция *тензорного произведения* матриц, а $S(F)$ — *сопровождающая матрица* многочлена F :

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

где коэффициенты $f_0, f_1, \dots, f_{m-1} \in R$ определены равенством

$$F(x) = x^m - f_{m-1}x^{m-1} - f_{m-2}x^{m-2} - \dots - f_1x - f_0.$$

Пусть $\tau = q^m - 1$. Выберем такое значение $k \in \{1, \dots, \tau - m + 1\}$, что $(k, \tau) = 1$. Определим автоморфизм σ_k бимодуля $R_{m,m}$ равенством

$$\sigma_k = \varphi_0^{-2^{n-1}k} \cdot \varphi_1^{2^{n-1}k}, \quad (1)$$

пусть θ — корень многочлена $F(x)$ в кольце $Q = GR(q^{mn}, 2^n)$. Элементу $\alpha_k = \theta^{-2^{n-1}k}$ сопоставим его образ $\overline{\alpha}_k$ при естественном эпиморфизме $Q \rightarrow Q/2Q$, а каждому значению $s \in \{1, \dots, m-1\}$ — минимальный многочлен $\mu_{s,k}(x)$ элемента $\overline{\alpha}_k^{q^s-1}$ над полем $\overline{R} = R/2R$.

Утверждение 1. *Характеристический многочлен автоморфизма σ_k имеет следующее каноническое разложение:*

$$\chi_k(x) = G_{0,k}(x)G_{1,k}(x) \dots G_{m-1,k}(x), \quad (2)$$

где $G_{0,k}(x) = (x-1)^m$ и $\overline{G}_{s,k}(x) = \mu_{s,k}(x)$, $s = 1, 2, \dots, m-1$.

Доказательство. См. § 2.

Разложение (2) индуцирует однозначное представление всякой матрицы $w \in R_{m,m}$:

$$w = w_{0,k} + w_{1,k} + w_{2,k} + \dots + w_{m-1,k},$$

где $w_{s,k} \in \text{Ker } G_{s,k}(\sigma_k)$, $s = 0, 1, \dots, m-1$. Пусть $\text{Tr}: Q \rightarrow R$ — функция «след» из кольца Q в кольцо R . В § 2 будет доказано, что для подходящего элемента $a_0 \in Q$ слагаемое $w_{0,k}$ имеет вид

$$w_{0,k} = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \text{Tr}(a_0 \cdot \theta^{i+j}) e_{i,j}. \quad (3)$$

Если $\overline{w}_{0,k} \neq 0$, то существует ЛРП максимального периода $u \in L_R(F)$ со свойством

$$w_{0,k} = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} u(i+j) e_{i,j}. \quad (4)$$

Рассмотрим функцию $f: \overline{R}^m \rightarrow \mathbb{Z}_2$ со следующими свойствами:

- 1) $f(0, 0, \dots, 0) = 0$;

- 2) в множестве $\overline{R}^m$ существует ровно k наборов, на которых функция f принимает значение 1;
- 3) вектор $(0, 0, \dots, 0, 1) \in \mathbb{Z}_2^m$ появляется на цикле выходной последовательности *фильтрующего генератора* [9] с характеристическим многочленом $F(x)$ и фильтрующей функцией f .

Зададим функцию самоуправления $\beta: R_{m,m} \rightarrow \mathbb{Z}_2$ равенством

$$\beta(w) = f(\overline{u}(0), \overline{u}(1), \dots, \overline{u}(m-1)), \quad (5)$$

где знаки рекурренты u определяются из (4). Пусть функция $\psi: R_{m,m} \rightarrow R$ принимает значение, стоящее в первой строке и первом столбце ее аргумента. Определим функцию перехода h_β автономного автомата

$$\mathfrak{A}^\beta = (R_{m,m}, R, h_\beta, \psi) \quad (6)$$

соотношением

$$h_\beta(w) = \varphi_{\beta(w)}(w).$$

Следуя [6], будем называть автомат (6) *самоуправляемым 2-линейным регистром сдвига* (самоуправляемым 2-ЛРС).

Всюду далее фраза «свойство выполняется почти для всех состояний» означает, что доля состояний, для которых свойство не выполняется, есть $o(1)$ при $m \rightarrow \infty$. Под *нормой* $\|z\|$ матрицы $z \in R_{m,m}$ будем понимать максимальное $l \in \{0, \dots, n\}$ со свойством $z \in 2^l R_{m,m}$. Перечислим основные результаты этой работы.

1. Пусть w — начальное заполнение 2-ЛРС $\mathfrak{A}^\beta$. Если $\overline{w}_{0,k} \neq 0$, ε_s — индикатор того, что $w_{s,k} \neq 0$, и $\tau_s = \tau/(q^{(m,s)} - 1)$, $s = 1, 2, \dots, m-1$, то период $T(\gamma)$ выходной последовательности γ 2-ЛРС $\mathfrak{A}^\beta$ вычисляется по формуле

$$T(\gamma) = 2^{n-1} \tau \cdot [\tau_1^{\varepsilon_1}, \tau_2^{\varepsilon_2}, \dots, \tau_{m-1}^{\varepsilon_{m-1}}] \leq \frac{2^{n-1} \tau^2}{q-1}, \quad (7)$$

где квадратные скобки означают *наименьшее общее кратное*.

2. Неравенство (7) обращается в равенство тогда и только тогда, когда

$$(\varepsilon_1, 2\varepsilon_2, 3\varepsilon_3, \dots, (m-1)\varepsilon_{m-1}, m) = 1.$$

Почти для всех начальных заполнений w справедливо соотношение

$$T(\gamma) = O(q^{2m}), \quad m \rightarrow \infty.$$

3. Число $N(\mathfrak{A}^\beta)$ начальных состояний w , для которых неравенство (7) обращается в равенство, выражается формулой

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

где μ — функция Мебиуса. Таким образом, почти все состояния 2-ЛРС $\mathfrak{A}^\beta$ принадлежат циклам максимальной длины.

4. Если $n = 1$, то в условиях и обозначениях пункта 1 ранг выходной последовательности γ удовлетворяет двойному неравенству

$$m + m \sum_{s=1}^{m-1} \tau_s \varepsilon_s \leq \text{rang } \gamma \leq m + m\tau \sum_{s=1}^{m-1} \varepsilon_s.$$

5. Если $n = 2$ и $\overline{w} = \overline{w}_{0,k}$, то в условиях и обозначениях пункта 1 ранг старшей координаты y_1 в 2-адическом разложении выходной последовательности γ удовлетворяет двойному неравенству

$$\frac{1}{2} \cdot m(m+3) + m \sum_{s=1}^{m-1} \tau_s \varepsilon_s \leq \text{rang } y_1 \leq \frac{1}{2} \cdot m(m+3) + m\tau \sum_{s=1}^{m-1} \varepsilon_s.$$

6. Пусть выполнены условия пункта 1, $\varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_{m-1} = 1$ и $s \in \{1, \dots, m-1\}$ таково, что $\|w_{s,k}\| = t < n$. Тогда знаки последовательности y_t (t -й координаты выходной последовательности γ) имеют асимптотически равномерное распределение при $m \rightarrow \infty$. Если $(q-1) \mid \tau_s$, то относительная частота $p_z(y_t)$ появления всякого знака $z \in \overline{R}$ на цикле последовательности y_t удовлетворяет неравенству

$$\left| p_z(y_t) - \frac{q^{m-1} - 1/2}{q^m - 1} \right| \leq \frac{1}{2\tau} + \frac{q-1}{q} \cdot \left(\frac{1}{\tau_s} - \frac{1}{\tau} \right) \cdot q^{m/2}.$$

В работе обобщены основные результаты работ [1, 3] и [2].

§ 2. Эффект сокращения периода

В этом параграфе исследуется связь между периодом $T(w)$ последовательности состояний

$$w = (w(0), w(1), w(2), \dots, w(i), \dots)$$

самоуправляемого 2-ЛРС $\mathfrak{A}^\beta$ и периодом $T(\gamma)$ его выходной последовательности γ . Так как $\gamma(i) = \psi(w(i))$ при всех $i \geq 0$, то, очевидно, $T(\gamma) \mid T(w)$. Далее будет показано, при каких условиях отсутствует эффект сокращения периода, т. е. выполняется равенство

$$T(\gamma) = T(w). \quad (8)$$

Напомним, что $Q = GR(q^{mn}, 2^n)$. Имеет место следующее 2-адическое разложение всякого элемента $x \in Q$:

$$x = x_0 + 2x_1 + 2^2x_2 + \dots + 2^{n-1}x_{n-1},$$

где $x_i^{q^m} = x_i$, $i = 0, 1, \dots, n-1$. Рассмотрим автоморфизм φ кольца Q , определенный равенством

$$\varphi(x) = \sum_{i=0}^{n-1} 2^i x_i^q, \quad x \in Q.$$

Тогда группа $\text{Aut}(Q/R)$ автоморфизмов кольца Q , оставляющих элементы кольца R неподвижными, порождена автоморфизмом φ :

$$\text{Aut}(Q/R) = \langle \varphi \rangle.$$

Очевидно, что $\text{ord } \varphi = m$.

Если θ — корень многочлена $F(x)$ в кольце $Q = R[\theta]$, то

$$F(x) = (x - \theta)(x - \varphi(\theta)) \dots (x - \varphi^{m-1}(\theta)),$$

где $\varphi^i = \varphi \cdot \varphi \cdot \dots \cdot \varphi$ (i раз). При этом

$$S(F) \approx \text{diag}(\theta, \varphi(\theta), \dots, \varphi^{m-1}(\theta)),$$

где $\approx$ — отношение подобия матриц над Q (см., например, [7]). В силу (1) характеристический многочлен $\chi_k(x)$ автоморфизма σ_k равен характеристическому многочлену матрицы

$$S(F)^{-2^{n-1}k} \otimes S(F)^{2^{n-1}k}.$$

Положив $\alpha_k = \theta^{-2^{n-1}k}$, получим

$$\chi_k(x) = \prod_{i=0}^{m-1} \prod_{j=0}^{m-1} (x - \varphi^i(\alpha_k) \cdot \varphi^j(\alpha_k^{-1})), \quad (9)$$

где φ^0 есть тождественное преобразование.

Для элементов $a, b \in Q$ будем писать $a \sim b$, если они лежат на одном цикле автоморфизма φ . Имеем

$$\varphi^i(\alpha_k) \cdot \varphi^j(\alpha_k^{-1}) = \varphi^j(\varphi^{i-j}(\alpha_k)\alpha_k^{-1}) \sim \varphi^{i-j}(\alpha_k)\alpha_k^{-1}. \quad (10)$$

Для всякого $s \in \{0, \dots, m-1\}$ положим $\vartheta_{s,k} = \varphi^s(\alpha_k)\alpha_k^{-1}$. Из (9) и (10) следует равенство

$$\chi_k(x) = \prod_{s=0}^{m-1} G_{s,k}(x), \quad (11)$$

где

$$G_{s,k}(x) = (x - \vartheta_{s,k})(x - \varphi(\vartheta_{s,k})) \dots (x - \varphi^{m-1}(\vartheta_{s,k})), \quad s = 0, 1, \dots, m-1.$$

Унитарный многочлен $G(x) \in R[x]$ назовем *многочленом Галуа*, если результат $\overline{G}(x)$ его приведения по модулю радикала $2R$ кольца R является неприводимым многочленом над полем $\overline{R} = GF(q)$.

Утверждение 2. *Многочлены $G_{1,k}(x)$, $G_{2,k}(x)$, $\dots$, $G_{m-1,k}(x)$ суть попарно взаимно простые многочлены Галуа.*

Для всякого $t \in \mathbb{N}$ обозначим через $\rho_m(t)$ число со свойствами:

- 1) $1 \leq \rho_m(t) \leq q^m - 1$;
- 2) $\rho_m(t) \equiv t \pmod{q^m - 1}$.

Циклотомическим классом с представителем $x \in \{1, \dots, q^m - 1\}$ назовем множество

$$C_m(x) = \{\rho_m(x \cdot q^i) \mid i \geq 0\}.$$

Каждому числу $z \in C_m(x)$ можно сопоставить его q -ичную запись длины m :

$$l_q(z) = (z_{m-1}, z_{m-2}, \dots, z_1, z_0), \quad z_i \in \{0, \dots, q-1\}.$$

Тогда множество $\{l_q(z) \mid z \in C_m(x)\}$ совпадает с множеством всех циклических сдвигов вектора $l_q(x)$. Отсюда следует, что для чисел $s_1, s_2 \in \{1, 2, \dots, m-1\}$ верна эквивалентность

$$C_m(q^{s_1} - 1) = C_m(q^{s_2} - 1) \Leftrightarrow s_1 = s_2. \quad (12)$$

Теперь докажем утверждение 2.

Доказательство. Пусть $s \in \{1, \dots, m-1\}$. Имеет место следующее разложение многочлена $\overline{G}_{s,k}(x)$ над полем $GF(q^m)$:

$$\overline{G}_{s,k}(x) = (x - \overline{\vartheta}_{s,k})(x - \overline{\vartheta}_{s,k}^q) \dots (x - \overline{\vartheta}_{s,k}^{q^{m-1}}).$$

Чтобы доказать неприводимость $\overline{G}_{s,k}(x)$ над $GF(q)$, достаточно показать, что длина цикла автоморфизма $\overline{\varphi}(x) = x^q$, которому принадлежит $\overline{\vartheta}_{s,k}$, равна m . От противного: пусть существует такое $l \in \{1, \dots, m-1\}$, что $\overline{\vartheta}_{s,k}^{q^l} = \overline{\vartheta}_{s,k}$. Напомним (см. § 1), что $(k, \tau) = 1$. Поскольку

$$\overline{\vartheta}_{s,k} = \overline{\varphi}^s(\overline{\alpha}_k) \cdot \overline{\alpha}_k^{-1} = \left(\overline{\theta}^{-2^{n-1}k} \right)^{q^s - 1}$$

и

$$\text{ord } \overline{\theta}^{-2^{n-1}k} = (q^m - 1)/(\tau, 2^{n-1}k) = q^m - 1,$$

имеем

$$q^l(q^s - 1) \equiv q^s - 1 \pmod{q^m - 1}.$$

Следовательно, циклический сдвиг на l шагов влево оставляет вектор $l_q(q^s - 1)$ неподвижным, что, очевидно, неверно. Итак, многочлен $\overline{G}_{s,k}(x)$ неприводим над $GF(q)$.

Пусть теперь $1 \leq s_1 < s_2 \leq m-1$. Докажем, что $\overline{G}_{s_1,k}(x) \neq \overline{G}_{s_2,k}(x)$ (и, следовательно, $G_{s_1,k}(x)$ взаимно прост с $G_{s_2,k}(x)$). Достаточно показать, что $\overline{\vartheta}_{s_1,k}$ и $\overline{\vartheta}_{s_2,k}$ лежат на разных циклах автоморфизма $\overline{\varphi}$. От противного: пусть

$$\exists l \in \{0, \dots, m-1\}: \overline{\vartheta}_{s_1,k}^{q^l} = \overline{\vartheta}_{s_2,k}.$$

Тогда

$$q^l(q^{s_1} - 1) \equiv q^{s_2} - 1 \pmod{q^m - 1},$$

т. е.

$$C_m(q^{s_1} - 1) = C_m(q^{s_2} - 1).$$

Отсюда согласно (12) имеем: $s_1 = s_2$. Противоречие. ■

В обозначениях § 1 очевидны равенства

$$G_{0,k}(x) = (x - 1)^m \quad \text{и} \quad \overline{G}_{s,k}(x) = \mu_{s,k}(x), \quad s = 1, 2, \dots, m-1.$$

Ввиду (11) получаем, что справедливо утверждение 1. Равенство (2) индуцирует следующее разложение R -бимодуля $R_{m,m}$ в прямую сумму ядер эндоморфизмов:

$$R_{m,m} = \text{Ker } G_{0,k}(\sigma_k) \dot{+} \text{Ker } G_{1,k}(\sigma_k) \dot{+} \dots \dot{+} \text{Ker } G_{m-1,k}(\sigma_k). \quad (13)$$

При этом

$$\forall s \in \{0, \dots, m-1\}: |\text{Ker } G_{s,k}(\sigma_k)| = |R|^{\deg G_{s,k}(x)} = |R|^m. \quad (14)$$

Равенство (13) порождает однозначное представление всякого состояния w 2-ЛРС $\mathcal{A}^\beta$:

$$w = w_{0,k} + w_{1,k} + \dots + w_{m-1,k}, \quad (15)$$

где $w_{s,k} \in \text{Ker } G_{s,k}(\sigma_k)$, $s = 0, 1, \dots, m-1$.

Пусть $\text{Tr}: Q \rightarrow R$ — функция «след» из Q в R :

$$\text{Tr}(x) = \sum_{j=0}^{m-1} \varphi^j(x), \quad x \in Q.$$

Всякому $s \in \{0, \dots, m-1\}$ сопоставим отображение $\pi_s: Q \rightarrow R_{m,m}$, определенное равенством

$$\pi_s(x) = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \text{Tr}([\varphi^s(\theta)]^i \theta^j x) e_{i,j}, \quad x \in Q. \quad (16)$$

Утверждение 3. Для всякого $s \in \{0, \dots, m-1\}$ отображение π_s задает изоморфизм R -бимодулей Q и $\text{Ker } G_{s,k}(\sigma_k)$.

Доказательство. Выберем и зафиксируем $s \in \{0, \dots, m-1\}$. Покажем, что π_s — мономорфизм R -бимодулей Q и $R_{m,m}$. Гомоморфность отображения π_s следует из свойств функции «след». Докажем его инъективность.

Если $x, y \in Q$ и $x \neq y$, то существует такое $j \in \{0, \dots, m-1\}$, что

$$\text{Tr}(\theta^j x) \neq \text{Tr}(\theta^j y).$$

Но тогда в силу (16) элементы, стоящие в нулевой строке и j -м столбце матриц $\pi_s(x)$ и $\pi_s(y)$, различны. Следовательно, $\pi_s(x) \neq \pi_s(y)$.

Из инъективности π_s и цепочки равенств (14) имеем

$$|\pi_s(Q)| = |Q| = |R|^m = |\text{Ker } G_{s,k}(\sigma_k)|.$$

Осталось доказать включение

$$\pi_s(Q) \subseteq \text{Ker } G_{s,k}(\sigma_k). \quad (17)$$

Пусть $x \in Q$, $x_0 = x$ и

$$x_{i+1} = \varphi^s(\theta)x_i, \quad i \in \{0, \dots, m-2\}.$$

Тогда в силу (16) верно равенство

$$\pi_s(x) = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \text{Tr}(x_i \theta^j) e_{i,j}. \quad (18)$$

Элементы θ и $\varphi^s(\theta)$ являются корнями многочлена $F(x)$. Поэтому ввиду (18) имеем

$$\varphi_0(\pi_s(x)) = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \text{Tr}(x_i \varphi^s(\theta) \theta^j) e_{i,j} = \pi_s(x \varphi^s(\theta)), \quad (19)$$

$$\varphi_1(\pi_s(x)) = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \text{Tr}(x_i \theta \theta^j) e_{i,j} = \pi_s(x \theta). \quad (20)$$

Из (1), (19) и (20) следует цепочка равенств

$$\sigma_k(\pi_s(x)) = \pi_s(x \varphi^s(\theta^{-2^{n-1}k}) \theta^{2^{n-1}k}) = \pi_s(x \varphi^s(\alpha_k) \alpha_k^{-1}) = \pi_s(x \vartheta_{s,k}), \quad x \in Q.$$

Отсюда, пользуясь гомоморфностью π_s , получаем

$$G_{s,k}(\sigma_k)(\pi_s(x)) = \pi_s(x G_{s,k}(\vartheta_{s,k})) = 0 \text{ для всех } x \in Q.$$

Таким образом, включение (17) доказано. ■

Из утверждения 3 вытекают следующие факты:

- 1) $\text{Ker } G_{0,k}(\sigma_k) = \pi_0(Q)$, т. е. имеет место равенство (3);
- 2) разложение (13) можно переписать в виде

$$R_{m,m} = \pi_0(Q) \dot{+} \pi_1(Q) \dot{+} \dots \dot{+} \pi_{m-1}(Q).$$

Поскольку сумма (13) — прямая, слагаемые $w_{s,k}$ из разложения (15) не зависят от k , поэтому вместо $w_{s,k}$ всюду далее будем писать w_s . В новых обозначениях разложение (15) принимает вид

$$w = w_0 + w_1 + \dots + w_{m-1}, \quad (21)$$

где $w_s \in \pi_s(Q)$, $s = 0, 1, \dots, m-1$.

Утверждение 4. Для каждого состояния w автомата $\mathcal{A}^\beta$ найдутся такие элементы

$$a_0, a_1, \dots, a_{m-1} \in Q,$$

что

$$w = \sum_{s=0}^{m-1} \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \text{Tr}([\varphi^s(\theta)]^i \theta^j a_s) e_{i,j}. \quad (22)$$

Утверждение 4 следует из (15), (16) и утверждения 3.

Пусть управляющая последовательность δ определена равенством

$$\forall i \geq 0: \delta(i) = \beta(w(i)).$$

Утверждение 5. Если w — начальное заполнение 2-ЛРС $\mathcal{A}^\beta$ и в разложении (22) $\bar{a}_0 \neq 0$, то $T(\delta) = \tau$ и на цикле последовательности δ имеется k единиц и $\tau - k$ нулей.

Доказательство. Так как $\bar{a}_0 \neq 0$ и

$$u(i) = \text{Tr}(a_0 \cdot \theta^i) \text{ при всех } i \geq 0,$$

то $\bar{u} \neq 0$ и на цикле рекурренты $\bar{u} \in L_{\bar{R}}(\bar{F})$ появляются все ненулевые m -граммы. По свойствам 1 и 2 функции f (см. § 1) число k совпадает с количеством единиц на отрезке

$$\delta(0), \delta(1), \dots, \delta(\tau - 1).$$

Осталось доказать, что период $T(\delta)$ управляющей последовательности δ равен τ . Очевидно, что $T(\delta) \mid T(\bar{u}) = \tau$. Пусть $\tau = l \cdot T(\delta)$. Тогда $l \mid k$ и $l \mid \tau$. При $l > 1$ приходим к противоречию со взаимной простотой чисел k и τ . Следовательно, $T(\delta) = \tau$. ■

Ввиду (21) каждый член $w(i)$ последовательности состояний w однозначно представляется в виде

$$w(i) = w_0(i) + w_1(i) + \dots + w_{m-1}(i), \quad (23)$$

где $w_s(i) \in \pi_s(Q)$, $s = 0, 1, \dots, m-1$. Типом состояния $w(i)$ назовем вектор

$$\text{typ } w(i) = (\|w_0(i)\|, \|w_1(i)\|, \dots, \|w_{m-1}(i)\|) \in \mathbb{Z}^m.$$

Поскольку автоморфизмы φ_0 и φ_1 сохраняют норму матрицы-состояния, справедливо равенство

$$\text{typ } w(i) = \text{typ } w(0) \text{ при всех } i \geq 0.$$

Это означает, что тип постоянен на компонентах связности графа переходов 2-ЛРС $\mathfrak{A}^\beta$. Условия $\bar{a}_0 \neq 0$ и $\bar{w}_0 \neq 0$ эквивалентны. Поэтому в автомате $\mathfrak{A}^\beta$ существует подавтомат $\tilde{\mathfrak{A}}^\beta$ с множеством состояний

$$S = \{\omega \in R_{m,m} \mid \bar{a}_0 \neq 0\} \quad (24)$$

(см. разложение (22)). При этом граф переходов автомата $\tilde{\mathfrak{A}}^\beta$ есть объединение некоторых компонент связности графа переходов автомата $\mathfrak{A}^\beta$.

Следующая теорема — центральный результат.

Теорема 6. *Автомат $\tilde{\mathfrak{A}}^\beta$ минимален, т. е. не имеет эквивалентных состояний.*

Доказательство. Пусть ω — начальное состояние автомата $\tilde{\mathfrak{A}}^\beta$, δ — индуцируемая им управляющая последовательность, γ — соответствующая выходная последовательность. Покажем сначала, что δ однозначно восстанавливается по F, f и γ .

Согласно утверждению 5, на отрезке управляющей последовательности δ длины $2^{n-1}\tau$ имеется $2^{n-1}(\tau - k)$ нулей и $2^{n-1}k$ единиц. Поэтому для выходной последовательности γ справедлива цепочка равенств

$$\gamma(i + j \cdot 2^{n-1}\tau) = \psi[\omega(i + j \cdot 2^{n-1}\tau)] = \psi[\sigma_k^j(\omega(i))] \quad \text{для всех } i, j \geq 0.$$

Это равенство можно переписать в следующем виде:

$$[x^{2^{n-1}j\tau}\gamma](i) = \psi[\sigma_k^j(\omega(i))] \quad \text{для всех } i, j \geq 0. \quad (25)$$

С другой стороны, в силу утверждения 2 многочлены $\widehat{G}_{s,k}(x) = \chi_k(x)/G_{s,k}(x)$, $s = 0, 1, \dots, m-1$, взаимно просты в совокупности. Это означает, что существуют многочлены $U_{s,k}(x) \in R[x]$, $s = 0, 1, \dots, m-1$, со свойством

$$\sum_{s=0}^{m-1} \widehat{G}_{s,k}(x) U_{s,k}(x) = 1.$$

Если обозначить $H_{s,k}(x) = \widehat{G}_{s,k}(x) U_{s,k}(x)$, $s = 0, 1, \dots, m-1$, то

$$\sum_{s=0}^{m-1} H_{s,k}(\sigma_k) = \varepsilon,$$

где ε — тождественное преобразование бимодуля $R_{m,m}$. Применим правую и левую части последнего равенства к $w(i)$, $i \geq 0$:

$$\sum_{s=0}^{m-1} H_{s,k}(\sigma_k)[w(i)] = w(i).$$

В силу однозначности разложения (21) и включения $H_{s,k}(\sigma_k)[w(i)] \in \text{Ker } G_{s,k}(\sigma_k)$

$$H_{s,k}(\sigma_k)[w(i)] = w_s(i) \text{ для всех } i \geq 0, s \in \{0, \dots, m-1\}.$$

В частности, при всех $i \geq 0$

$$H_{0,k}(\sigma_k)[w(i)] = w_0(i). \quad (26)$$

Рассмотрим стандартную запись многочлена $H_{0,k}$:

$$H_{0,k}(x) = \sum_{j \geq 0} h_j x^j.$$

Учитывая линейность функции ψ , просуммируем равенства (25) по всем $j \geq 0$ с коэффициентами h_j , а затем применим равенство (26):

$$[H_{0,k}(x^{2^{n-1}\tau}) \cdot \gamma](i) = \psi[H_{0,k}(\sigma_k)(w(i))] = \psi(w_0(i)) = u(i), \quad i \geq 0.$$

Следовательно,

$$u = H_{0,k}(x^{2^{n-1}\tau})\gamma.$$

Отсюда и из равенства (5) получаем, что управляющая последовательность δ однозначно восстанавливается по выходной последовательности γ . Поэтому δ однозначно восстанавливается по F, f и γ .

Теперь докажем, что w однозначно восстанавливается по F, f, γ и δ . По свойству 3 функции f (см. § 1) существует такое $t \geq 0$, что

$$\delta(t, \dots, t+m-1) = (0, 0, \dots, 0, 1).$$

Пусть на отрезке $\delta(0, \dots, t-1)$ имеется t_0 нулей и t_1 единиц. Тогда

$$w(t) = \varphi_0^{t_0} \varphi_1^{t_1}(w(0)).$$

Очевидно, восстановление $w = w(0)$ сводится к восстановлению $w(t)$.

Положим $\mathfrak{F} = \{0, \dots, m-1\} \times \{0, \dots, m-1\}$. Рассмотрим такую 2-линейную рекуррентную последовательность (2-ЛРП) $\nu \in L_R(F, F)$, что $\nu[\mathfrak{F}] = w(t)$ (см., например, [6]). Из утверждения 4 следует, что существуют элементы $c_0, c_1, \dots, c_{m-1} \in Q$ со свойством

$$\nu(i, j) = \sum_{s=0}^{m-1} \text{Tr}([\varphi^s(\theta)]^i \theta^j c_s) \quad \text{при всех } i \geq 0, j \geq 0. \quad (27)$$

Для $i \in \{0, \dots, m-1\}$ положим

$$b_i = \sum_{s=0}^{m-1} [\varphi^s(\theta)]^i c_s.$$

Тогда

$$w(t) = \nu[\mathfrak{F}] = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \text{Tr}(b_i \theta^j) e_{i,j}.$$

Поэтому задача восстановления $w(t)$ эквивалентна задаче восстановления вектора $(b_0, b_1, \dots, b_{m-1})$.

Выберем и зафиксируем $l \in \{0, \dots, m-1\}$. Пусть $y_l = \gamma(t + l\tau, \dots, t + l\tau + m-1)$, и

$$e_i = (0, \dots, 0, 1, 0, \dots, 0) \in R^m, \quad i \in \{0, \dots, m-1\},$$

где 1 стоит на $(i+1)$ -м месте. Если

$$y_l = \sum_{i=0}^{m-1} y_l(i) e_i, \quad y_l(i) \in R,$$

то в силу цепочки равенств

$$\delta(t + l\tau, \dots, t + l\tau + m-1) = \delta(t, \dots, t + m-1) = (0, 0, \dots, 0, 1)$$

при всех $i \in \{0, \dots, m-1\}$ верно соотношение

$$y_l(i) = \nu(l(\tau - k) + i, lk).$$

Ввиду (27)

$$y_l = \sum_{i=0}^{m-1} \sum_{s=0}^{m-1} \text{Tr}([\varphi^s(\theta)]^{l(\tau-k)+i} \theta^{lk} c_s) e_i.$$

Положив $z_l = y_l \cdot S(F)^{-l(\tau-k)}$ и учитывая, что $F(\varphi^s(\theta)) = 0$, получаем

$$z_l = \sum_{i=0}^{m-1} \sum_{s=0}^{m-1} \text{Tr}([\varphi^s(\theta)]^i \theta^{lk} c_s) e_i = \sum_{i=0}^{m-1} \text{Tr}(b_i \vartheta_k^l) e_i, \text{ где } \vartheta_k = \theta^k. \quad (28)$$

Пусть Q_{ϑ_k} — расширение кольца R элементом ϑ_k : $R[\vartheta_k] = Q_{\vartheta_k} \leq Q$. Элемент ϑ_k является корнем некоторого многочлена Галуа $G(x) \in R[x]$. Поскольку

$$\text{ord } \bar{\vartheta}_k = \text{ord } \bar{\theta} = q^m - 1,$$

имеем

$$\bar{G}(x) = (x - \bar{\vartheta}_k)(x - \bar{\varphi}(\bar{\vartheta}_k)) \dots (x - \bar{\varphi}^{m-1}(\bar{\vartheta}_k)).$$

Поэтому $\deg \bar{G}(x) = \deg G(x) = m$, $R[\vartheta_k] = Q_{\vartheta_k} = Q$, и система

$$1, \vartheta_k, \vartheta_k^2, \dots, \vartheta_k^{m-1} \quad (29)$$

является базисом R -бимодуля Q .

Пусть $(\varepsilon_{0,k}, \varepsilon_{1,k}, \dots, \varepsilon_{m-1,k})$ — базис, двойственный к базису (29). Если

$$z_l = \sum_{i=0}^{m-1} z_l(i) e_i, \quad z_l(i) \in R, \quad l = 0, 1, \dots, m-1,$$

то, ввиду (28),

$$b_i = \sum_{l=0}^{m-1} z_l(i) \varepsilon_{l,k}, \quad i \in \{0, \dots, m-1\}.$$

Итак, вектор $(b_0, b_1, \dots, b_{m-1})$ однозначно выражается через знаки последовательности γ . Поэтому ω однозначно восстанавливается по F, f, γ и δ . ■

Результаты этого параграфа показывают, что если $\omega = \omega(0) \in S$, то эффект сокращения периода отсутствует. Легко показать, что почти все состояния 2-ЛРС $\mathcal{A}^\beta$ лежат во множестве S .

§ 3. Период выходной последовательности

В этом параграфе исследуются периодические свойства выходной последовательности γ при условии, что $\omega(0) \in S$. В силу (8) вопрос сводится к изучению периода $T(\omega)$ последовательности ω .

Ввиду (23) имеет место однозначное разложение последовательности состояний ω :

$$\omega = \omega_0 + \omega_1 + \dots + \omega_{m-1},$$

где $w_s \in \pi_s(Q)^\infty$ — последовательность над модулем $\pi_s(Q)$, $s = 0, 1, \dots, m-1$. Если положить $v = w_1 + w_2 + \dots + w_{m-1}$, то периоды последовательностей w , w_0 и v связаны соотношением

$$T(w) = [T(w_0), T(v)].$$

В силу (16) и утверждения 3 при каждом $l \geq 0$

$$w_0(l) = h_\beta^l \pi_0(a_0) = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \text{Tr}(\theta^{i+j+l} a_0) e_{i,j}.$$

Так как $w(0) \in S$, то $T(w_0) = 2^{n-1} \tau$ (см. (24)). Поэтому

$$T(w) = [2^{n-1} \tau, T(v)]. \quad (30)$$

Осталось вычислить $T(v)$. Если v — нулевая последовательность ($v = 0$), то $T(w) = 2^{n-1} \tau$. Далее считаем, что $v \neq 0$. Пусть $v = (v(0), v(1), \dots)$. Для всякого $w \in R_{m,m}$ обозначим через $T_{\sigma_k}(w)$ длину того цикла автоморфизма σ_k , которому принадлежит w . Очевидно, что

$$T_{\sigma_k}(v(0)) = [T_{\sigma_k}(w_1), \dots, T_{\sigma_k}(w_{m-1})]. \quad (31)$$

Выберем и зафиксируем $s \in \{1, \dots, m-1\}$. Если $n_s = \|w_s\| = n$, то $T_{\sigma_k}(w_s) = 1$. Пусть $n_s < n$. Тогда

$$w_s = 2^{n_s} \cdot v_s \quad \text{и} \quad \bar{v}_s \neq 0.$$

Определим автоморфизм $\bar{\sigma}_k \in \text{Aut}(\bar{R}_{m,m})$ соотношением

$$\forall w \in R_{m,m}: \bar{\sigma}_k(\bar{w}) = \overline{\sigma_k(w)}.$$

Согласно [8, лемма 1.1], имеем

$$T_{\sigma_k}(w_s) = 2^{\nu_s} \cdot T_{\bar{\sigma}_k}(\bar{v}_s), \quad 0 \leq \nu_s \leq n - n_s - 1.$$

В силу равенства $\bar{G}_{s,k}(\bar{\sigma}_k)(\bar{v}_s) = 0$ и неприводимости $\bar{G}_{s,k}(x)$ получаем, что $\bar{G}_{s,k}(x)$ есть минимальный многочлен вектора $\bar{v}_s$ относительно преобразования $\bar{\sigma}_k$. Тогда

$$T_{\bar{\sigma}_k}(\bar{v}_s) = T(\bar{G}_{s,k}) = \tau_s,$$

где $\tau_s = \text{ord } \bar{\vartheta}_{s,k} = \text{ord } \bar{\alpha}_k^{q^s-1} = \tau/(q^{(m,s)} - 1)$.

Пусть ε_s — индикатор неравенства $n_s < n$, $s = 1, 2, \dots, m-1$. Из (31) следуют соотношения

$$T_{\sigma_k}(v(i)) = 2^{d(i)} \cdot [\tau_1^{\varepsilon_1}, \tau_2^{\varepsilon_2}, \dots, \tau_{m-1}^{\varepsilon_{m-1}}], \quad i \geq 0, \quad (32)$$

где $d(i) \in \{0, \dots, n-1\}$. Из очевидного равенства

$$v(i + j \cdot 2^{n-1}\tau) = \sigma_k^j(v(i)), \quad i, j \geq 0,$$

и соотношения (32) получаем, что наименьшее общее кратное периодов всех регулярных $2^{n-1}\tau$ -выборок из последовательности v равно

$$2^d \cdot [\tau_1^{\varepsilon_1}, \tau_2^{\varepsilon_2}, \dots, \tau_{m-1}^{\varepsilon_{m-1}}],$$

где $d = \max\{d(0), d(1), \dots, d(2^{n-1}\tau - 1)\} \in \{0, \dots, n-1\}$. Отсюда

$$\frac{T(v)}{(T(v), 2^{n-1}\tau)} = 2^d \cdot [\tau_1^{\varepsilon_1}, \tau_2^{\varepsilon_2}, \dots, \tau_{m-1}^{\varepsilon_{m-1}}]. \quad (33)$$

Заметим, что при всех $x \in R_{m,m}$

$$\varphi_0^{2^{n-1}\tau}(x) = \varphi_1^{2^{n-1}\tau}(x) = x.$$

Так как $T(\delta) = \tau$, то для всякого $i \geq 0$

$$v(i + 2^{n-1}\tau^2) = \varphi_0^{2^{n-1}\tau \sum_{j=i}^{i+\tau-1} (1-\delta(j))} \varphi_1^{2^{n-1}\tau \sum_{j=i}^{i+\tau-1} \delta(j)}(v(i)) = v(i).$$

Отсюда $T(v) \mid 2^{n-1}\tau^2$. Следовательно, ввиду (33),

$$T(v) \mid 2^{n-1}\tau \cdot [\tau_1^{\varepsilon_1}, \tau_2^{\varepsilon_2}, \dots, \tau_{m-1}^{\varepsilon_{m-1}}]. \quad (34)$$

Утверждение 7. Если $v \neq 0$, то $\tau \mid T(v)$.

Доказательство. Поскольку $v \neq 0$, существует такое $s \in \{1, \dots, m-1\}$, что $w_s \neq 0$. Так как $T(w_s) \mid T(v)$, достаточно доказать, что $\tau \mid T(w_s)$.

От противного: допустим, что τ не делит $T(w_s)$. Поскольку $\tau = T(\delta)$, существует такое $l \geq 0$, что

$$\delta(l) \neq \delta(l + T(w_s)). \quad (35)$$

Положим для каждого $i \geq 0$

$$\Delta(i) = \sum_{j=i}^{i+T(w_s)-1} (1 - \delta(j));$$

тогда

$$w_s(i) = \varphi_0^{\Delta(i)} \varphi_1^{T(w_s) - \Delta(i)}(w_s(i)). \quad (36)$$

Для каждого $i \geq 0$ существуют такие $s_0(i) \geq 0$ и $s_1(i) \geq 0$, что

$$w_s(i) = \varphi_0^{s_0(i)} \varphi_1^{s_1(i)}(w_s),$$

поэтому из (36) следует равенство

$$w_s = \varphi_0^{\Delta(l)} \varphi_1^{T(w_s) - \Delta(l)}(w_s).$$

Отсюда, заменив l на $l + 1$ и учитывая (35), имеем

$$w_s = \varphi_0^{\Delta(l+1)} \varphi_1^{T(w_s) - \Delta(l+1)}(w_s) = \varphi_0^{\pm 1} \varphi_1^{\mp 1}(\varphi_0^{\Delta(l)} \varphi_1^{T(w_s) - \Delta(l)}(w_s)) = \varphi_0^{\pm 1} \varphi_1^{\mp 1}(w_s).$$

Учитывая перестановочность автоморфизмов φ_0 и φ_1 , полученное соотношение можно переписать в виде

$$\varphi_0^{-1} \varphi_1(w_s) = w_s.$$

Поэтому

$$\sigma_k(w_s) = \varphi_0^{-2^{n-1}k} \varphi_1^{2^{n-1}k}(w_s) = w_s.$$

Так как $G_{0,k}(x) = (x - 1)^m$, получаем, что $G_{0,k}(\sigma_k)(w_s) = 0$. Поскольку $s > 0$, имеем $w_s \notin \text{Ker } G_{0,k}(\sigma_k)$. Противоречие. ■

Из утверждения 7 и (33) следует, что

$$\tau \cdot [\tau_1^{\varepsilon_1}, \tau_2^{\varepsilon_2}, \dots, \tau_{m-1}^{\varepsilon_{m-1}}] \mid T(v).$$

Ввиду (34) отсюда вытекает, что при некотором $\nu \in \{0, \dots, n - 1\}$

$$T(v) = 2^\nu \tau \cdot [\tau_1^{\varepsilon_1}, \tau_2^{\varepsilon_2}, \dots, \tau_{m-1}^{\varepsilon_{m-1}}].$$

Тогда, согласно (30),

$$T(w) = 2^{n-1} \tau \cdot [\tau_1^{\varepsilon_1}, \tau_2^{\varepsilon_2}, \dots, \tau_{m-1}^{\varepsilon_{m-1}}],$$

и, ввиду (8),

$$T(\gamma) = 2^{n-1} \tau \cdot [\tau_1^{\varepsilon_1}, \tau_2^{\varepsilon_2}, \dots, \tau_{m-1}^{\varepsilon_{m-1}}].$$

Теорема 8. Пусть $w(0) \in S$ и ε_s — индикатор того, что $w_s \neq 0$, $s = 1, 2, \dots, m - 1$. Тогда период $T(\gamma)$ выходной последовательности γ вычисляется по формуле

$$T(\gamma) = 2^{n-1} \tau \cdot [\tau_1^{\varepsilon_1}, \tau_2^{\varepsilon_2}, \dots, \tau_{m-1}^{\varepsilon_{m-1}}] \leq \frac{2^{n-1} \tau^2}{q - 1}.$$

Теорема 8 следует из эквивалентности условий $n_s < n$ и $w_s \neq 0$.

Следствие 9. В условиях теоремы 8 равенство

$$T(\gamma) = \frac{2^{n-1}\tau^2}{q-1} \quad (37)$$

выполняется тогда и только тогда, когда

$$(\varepsilon_1, 2\varepsilon_2, 3\varepsilon_3, \dots, (m-1)\varepsilon_{m-1}, m) = 1. \quad (38)$$

Доказательство. Пусть в сумме $\omega_1 + \omega_2 + \dots + \omega_{m-1}$ имеется ровно s ненулевых слагаемых и

$$\{j_1, j_2, \dots, j_s\} = \{j \in \{1, \dots, m-1\} : \varepsilon_j = 1\}.$$

Тогда по теореме 8

$$T(\gamma) = 2^{n-1}\tau \cdot \left[\frac{\tau}{q^{(m,j_1)} - 1}, \frac{\tau}{q^{(m,j_2)} - 1}, \dots, \frac{\tau}{q^{(m,j_s)} - 1} \right] = \frac{2^{n-1}\tau^2}{q^{(m,j_1,j_2,\dots,j_s)} - 1}.$$

Следовательно, (37) выполняется тогда и только тогда, когда

$$(m, j_1, j_2, \dots, j_s) = 1. \quad (39)$$

Это условие, очевидно, эквивалентно равенству (38). ■

Состояния $\omega(0)$ 2-ЛРС $\mathfrak{A}^\beta$, для которых выполняется равенство (37), будем называть *основными*. Это состояния, принадлежащие циклам максимальной длины. Найдем число основных состояний.

Следствие 10. Количество $N(\mathfrak{A}^\beta)$ основных состояний регистра $\mathfrak{A}^\beta$ выражается формулой

$$N(\mathfrak{A}^\beta) = (q^m - 1) \sum_{d|m} \mu(m/d) \cdot q^{m(nd-1)}, \quad (40)$$

где μ — функция Мебиуса.

Доказательство. Пусть $s \in \{1, \dots, m-1\}$. Обозначим через $\varphi^{[s]}(m)$ количество таких наборов $(j_1, j_2, \dots, j_s)$, что $1 \leq j_1 < j_2 < \dots < j_s \leq m-1$ и выполняется (39). Согласно [1, лемма 20], верно равенство

$$\varphi^{[s]}(m) = \sum_{d|m} \mu(d) \binom{\frac{m}{d} - 1}{s}, \quad (41)$$

где μ — функция Мебиуса.

По утверждению 4, существует взаимно однозначное соответствие между состояниями w 2-ЛРС $\mathfrak{A}^\beta$ и наборами $(a_0, a_1, \dots, a_{m-1}) \in Q^m$. Пусть

$$a_1 + a_2 + \dots + a_{m-1} = a_{j_1} + a_{j_2} + \dots + a_{j_s},$$

где $1 \leq j_1 < j_2 < \dots < j_s \leq m-1$, и пусть все слагаемые в правой части ненулевые. Если $\bar{a}_0 = 0$, то, по свойству 1 функции f , верно равенство $\delta = 0$, и

$$T(\gamma) \mid T(w) \mid 2^{n-1} \tau.$$

Поэтому основные состояния соответствуют тем и только тем наборам

$$(a_0, a_1, \dots, a_{m-1}) \in Q^m,$$

для которых $\bar{a}_0 \neq 0$ и выполняется (39). При фиксированном s число таких наборов равно

$$|Q^*| \cdot (|Q| - 1)^s \varphi^{[s]}(m) = q^{m(n-1)}(q^m - 1)(q^{mn} - 1)^s \varphi^{[s]}(m).$$

Суммируя эту величину по $s \in \{1, \dots, m-1\}$ и учитывая (41), получаем

$$\begin{aligned} N(\mathfrak{A}^\beta) &= q^{m(n-1)}(q^m - 1) \sum_{s=1}^{m-1} (q^{mn} - 1)^s \varphi^{[s]}(m) = \\ &= (q^m - 1) \sum_{d|m} \mu(d) \cdot q^{m(n-1)} \sum_{s=1}^{m-1} (q^{mn} - 1)^s \binom{\frac{m}{d} - 1}{s} = \\ &= (q^m - 1) \sum_{d|m} \mu(d) \cdot q^{m(n-1)} \sum_{s=0}^{\frac{m}{d}-1} (q^{mn} - 1)^s \binom{\frac{m}{d} - 1}{s} - \\ &- (q^m - 1) \sum_{d|m} \mu(d) \cdot q^{m(n-1)} = (q^m - 1) \sum_{d|m} \mu(d) \cdot q^{m(n-1)} \cdot (q^{mn})^{\frac{m}{d}-1} = \\ &= (q^m - 1) \sum_{d|m} \mu(m/d) \cdot q^{m(n-1)} q^{mn(d-1)} = (q^m - 1) \sum_{d|m} \mu(m/d) \cdot q^{m(nd-1)}. \end{aligned}$$

Формула (40) доказана. ■

Из следствия 10 вытекает, что

$$N(\mathfrak{A}^\beta) = q^{m^2 n} (1 + o(1)) = |R|^{m^2} (1 + o(1)), \quad m \rightarrow \infty,$$

т.е. почти для всех начальных заполнений $w(0)$ 2-ЛРС $\mathfrak{A}^\beta$ имеет место цепочка равенств

$$T(\gamma) = \frac{2^{n-1}\tau^2}{q-1} = O(\tau^2) = O(q^{2m}), \quad m \rightarrow \infty.$$

Теорема 8 и следствия из нее обобщают теорему 2, следствие 1 и следствие 2 из работы [3].

§ 4. Ранг результирующей последовательности

Знаки выходной последовательности γ самоуправяемого 2-ЛРС $\mathfrak{A}^\beta$ принадлежат кольцу Галуа R . В то же время для нужд практики полезно уметь вырабатывать ПСП над полем $\bar{R} = GF(q)$. Простейший способ построить на основе γ последовательность над R — выделить фиксированную координату в 2-адическом разложении

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

где $y_i \in \bar{R}^\infty$, $i = 0, 1, \dots, n-1$. Всюду далее $t = \|\omega_1 + \omega_2 + \dots + \omega_{m-1}\|$, и в качестве итоговой (результирующей) ПСП рассматривается y_t .

Ранг (линейная сложность) результирующей последовательности y_t , т.е. длина кратчайшего одномерного ЛРС над полем $\bar{R}$, ее вырабатывающего, характеризует стойкость обсуждаемого генератора к методу линеаризации. В этом параграфе будут получены верхняя и нижняя оценки для ранга y_t .

Изучим строение ПСП γ при условии, что $w(0) \in S$ (см. (24)). Ввиду (23) и линейности ψ имеем

$$\gamma = \gamma_0 + \gamma_1 + \dots + \gamma_{m-1}, \quad (42)$$

где $\gamma_s(i) = \psi(w_s(i))$ при всех $i \geq 0$, $s \in \{0, 1, \dots, m-1\}$.

Для всякого $d \geq 0$ обозначим через γ_s^d регулярную $(d, 2^{n-1}\tau)$ -выборку из последовательности γ_s . Под нормой $\|a\|$ последовательности $a \in R^\infty$ будем понимать максимальное $l \in \{0, \dots, n\}$ со свойством $a \in 2^l R^\infty$.

Утверждение 11. Для любых $s \in \{1, 2, \dots, m-1\}$ и $d \geq 0$ верна цепочка равенств

$$\|\gamma_s^d\| = \|\gamma_s\| = \|w_s\|.$$

Доказательство. Выберем и зафиксируем $s \in \{1, 2, \dots, m-1\}$. Цепочка неравенств

$$\|\gamma_s^d\| \geq \|\gamma_s\| \geq \|w_s\|$$

очевидна. Докажем, что $\|\gamma_s\| = \|w_s\|$.

Если $w_s = 0$, то требуемое равенство очевидно. Пусть $n_s = \|w_s\| < n$. Рассмотрим факторкольцо $\tilde{R} = R/2^{n_s+1}R$. Для всякой последовательности $a \in R^\infty$ обозначим через $\tilde{a}$ ее образ при естественном эпиморфизме $R \rightarrow \tilde{R}$. Если $\|\gamma_s\| > n_s$, то $\tilde{\gamma}_s = 0$. Последовательность $\tilde{\gamma}_0 + \tilde{\gamma}_s$ можно рассматривать как выходную ПСП самоуправляемого 2-ЛРС над кольцом $\tilde{R}$ с последовательностью состояний $\tilde{w}_0 + \tilde{w}_s$. По теореме 8 имеем

$$2^{n_s}\tau = T(\tilde{\gamma}_0) = T(\tilde{\gamma}_0 + \tilde{\gamma}_s) = 2^{n_s}\tau \cdot \tau_s.$$

Отсюда $\tau_s = 1$. Противоречие.

Итак, существует такое $d_0 \geq 0$, что $\|\gamma_s^{d_0}\| = \|w_s\|$. Выберем и зафиксируем произвольное $d \geq 0$. Докажем, что $\|\gamma_s^d\| = \|\gamma_s^{d_0}\|$.

Если $w_s = 0$, то требуемое равенство очевидно. Пусть $n_s < n$. Для всякого

$$\vec{x} = (x_0, x_1, \dots, x_{m-1}) \in R^m$$

положим

$$(\vec{0}, \vec{x}, \vec{0}) = (0, 0, \dots, 0, x_0, x_1, \dots, x_{m-1}, 0, 0, \dots, 0) \in R^{m^2},$$

где длина первой серии нулей равна ms . Рассмотрим матрицу автоморфизма σ_k в базисе $e^\perp$ из матричных единиц. Она подобна распавшейся форме:

$$A \cdot [S(F)^{-2^{n-1}k} \otimes S(F)^{2^{n-1}k}] \cdot A^{-1} = \text{Diag}(E_{m \times m}, S(G_{1,k}), \dots, S(G_{m-1,k})),$$

где $A \in R_{m^2, m^2}^*$, $\otimes$ — операция *тензорного произведения* матриц. По утверждению 3 имеем

$$\pi_s(Q) = \{(\vec{0}, \vec{x}, \vec{0}) \cdot A \cdot e^\perp \mid \vec{x} \in R^m\}.$$

Пусть биекция $\lambda_s: \pi_s(Q) \rightarrow R^m$ определена равенством

$$\lambda_s[(\vec{0}, \vec{x}, \vec{0}) \cdot A \cdot e^\perp] = \vec{x},$$

$v_{s,d} \in L_R(G_{s,k})$ — ЛРП с начальным вектором $\lambda_s(w_s(d))$, $A = (a_{i,j})$, и

$$f_s(x) = a_{m(s+1),1}x^{m-1} + a_{m(s+1)-1,1}x^{m-2} + \dots + a_{ms+1,1} \in R[x].$$

Тогда имеет место соотношение

$$\gamma_s^d = f_s(x) \cdot v_{s,d}. \quad (43)$$

Оно справедливо, в частности, для $d = d_0$. Поэтому

$$\|f_s(x) \cdot v_{s,d_0}\| = \|\gamma_s^{d_0}\| = n_s = \|w_s(d_0)\| = \|\lambda_s(w_s(d_0))\| = \|v_{s,d_0}\|$$

и $\bar{f}_s(x) \neq 0$. Отсюда и из (43) вытекает цепочка равенств

$$\|\gamma_s^d\| = \|v_{s,d}\| = \|\lambda_s(w_s(d))\| = \|w_s(d)\| = \|w_s(d_0)\| = \|\gamma_s^{d_0}\|. \quad \blacksquare$$

Выберем и зафиксируем $s \in \{1, 2, \dots, m-1\}$. Рассмотрим ПСП $\xi_s \in R^\infty$, удовлетворяющую равенству

$$\gamma_s = 2^{n_s} \cdot \xi_s. \quad (44)$$

По утверждению 11 при $w_s \neq 0$ ПСП $\bar{\xi}_s$ является ненулевой и однозначно определяется начальным заполнением w . Ближайшая задача — оценить ранг $\bar{\xi}_s$.

Пусть $d \geq 0$. Поскольку для всех $j \geq 0$

$$\gamma_s^d(j) = \psi[w_s(d + j \cdot 2^{n-1}\tau)] = \psi[\sigma_k^j(w_s(d))]$$

и $w_s(d) \in \text{Ker } G_{s,k}(\sigma_k)$, верно равенство $G_{s,k}(x) \cdot \gamma_s^d = 0$. Так как d выбрано произвольно, то

$$G_{s,k}(x^{2^{n-1}\tau}) \cdot \gamma_s = 0. \quad (45)$$

Отсюда, ввиду (44),

$$\bar{G}_{s,k}(x^{2^{n-1}\tau}) \cdot \bar{\xi}_s = 0 \quad \text{и} \quad \text{rang } \bar{\xi}_s \leq 2^{n-1} \cdot m\tau.$$

Полученную оценку ранга можно усилить. Далее будет показано, что

$$\bar{G}_{s,k}(x^\tau) \cdot \bar{\xi}_s = 0 \quad \text{и} \quad \text{rang } \bar{\xi}_s \leq m\tau. \quad (46)$$

Рассмотрим автономный автомат

$$\mathfrak{A}_\beta = (\text{Ker } G_{0,k}(\sigma_k), \mathbb{Z}_2, \varphi_\beta, \beta)$$

и внешне автономный автомат

$$\mathfrak{B}_s = (\mathbb{Z}_2, \text{Ker } G_{s,k}(\sigma_k), R, \{\varphi_0, \varphi_1\}, \psi).$$

Пусть (w_0, w_s) — начальное состояние последовательного соединения

$$\mathfrak{A}_\beta \rightarrow \mathfrak{B}_s. \quad (47)$$

Выходная последовательность этого автомата совпадает с γ_s .

Аналогично автоморфизму $\bar{\sigma}_k$ можно ввести автоморфизмы $\bar{\varphi}_0$ и $\bar{\varphi}_1$ пространства $\bar{R}_{m,m}$. Рассмотрим автоматы

$$\bar{\mathcal{A}}_\beta = (\text{Ker } \bar{G}_{0,k}(\bar{\sigma}_k), \mathbb{Z}_2, \bar{\varphi}_\beta, \beta) \quad \text{и} \quad \bar{\mathcal{B}}_s = (\mathbb{Z}_2, \text{Ker } \bar{G}_{s,k}(\bar{\sigma}_k), \bar{R}, \{\bar{\varphi}_0, \bar{\varphi}_1\}, \psi).$$

Последовательное соединение

$$\bar{\mathcal{A}}_\beta \rightarrow \bar{\mathcal{B}}_s \quad (48)$$

есть автомат над полем $\bar{R} = GF(q)$, т.е. над кольцом Галуа $GR(q, 2)$. Напомним (см. § 3), что

$$\omega_s = 2^{n_s} \cdot v_s. \quad (49)$$

Пусть $(\bar{w}_0, \bar{v}_s)$ — начальное состояние автомата (48). Тогда ввиду (45) его выходная последовательность аннулируется многочленом $\bar{G}_{s,k}(x^\tau)$.

Автомат $\bar{\mathcal{A}}_\beta$ генерирует управляющую последовательность δ . Значение $\beta(w)$ полностью определяется образом $\bar{w}$ матрицы $w \in R_{m,m}$ при естественном эпиморфизме $R \rightarrow \bar{R}$. Следовательно, выходная последовательность автомата $\bar{\mathcal{A}}_\beta$ совпадает с δ . Ввиду (49) получаем, что n_s -я координата $\bar{\xi}_s$ в 2-адическом разложении выходной последовательности γ_s автомата (47) совпадает с выходной последовательностью автомата (48). Следовательно, имеют место соотношения (46).

Получим нижнюю оценку ранга последовательности $\bar{\xi}_s$.

Утверждение 12. Для всякого $s \in \{1, 2, \dots, m-1\}$ верно неравенство

$$\text{rang } \bar{\xi}_s \geq m\tau_s.$$

Доказательство. Выберем и зафиксируем $s \in \{1, 2, \dots, m-1\}$. Пусть $m(x)$ — минимальный многочлен ЛРП $\bar{\xi}_s$ над полем $\bar{R}$. Из равенства $\bar{G}_{s,k}(x^\tau) \times \bar{\xi}_s = 0$ следует соотношение

$$m(x) \mid \prod_{i=0}^{m-1} (x^\tau - \bar{\varphi}^i(\bar{v}_{s,k})),$$

где $\bar{\varphi}(x) = x^q$ для всякого $x \in \bar{Q}$. Положим

$$A_i(x) = x^\tau - \bar{\varphi}^i(\bar{v}_{s,k}) \in \bar{Q}[x], \quad i \in \{0, \dots, m-1\}.$$

Так как корни $\bar{v}_{s,k}$, $\bar{\varphi}(\bar{v}_{s,k})$, $\dots$, $\bar{\varphi}^{m-1}(\bar{v}_{s,k})$ многочлена $\bar{G}_{s,k}(x)$ попарно различны, то многочлены

$$A_0(x), A_1(x), \dots, A_{m-1}(x) \quad (50)$$

попарно взаимно просты.

Многочлен $m(x)$ можно рассматривать как многочлен над полем $\overline{Q} > \overline{R}$. Если элемент a — корень многочлена $m(x)$ в его поле разложения $P > \overline{Q}$, то существует такое значение $i \in \{0, \dots, m-1\}$, что $A_i(a) = 0$. Поэтому найдется неприводимый над $\overline{Q}$ многочлен $h_i(x)$ со свойствами $h_i(x) \mid A_i(x)$ и $h_i(a) = 0$. Многочлены $h_i(x) \in \overline{Q}[x]$ и $m(x) \in \overline{Q}[x]$ не взаимно просты над P , поэтому они не взаимно просты и над $\overline{Q}$. В силу неприводимости $h_i(x)$ над полем $\overline{Q}$ имеем $h_i(x) \mid m(x)$.

Элементы

$$a, a^q, a^{q^2}, \dots, a^{q^{m-1}} \in P$$

суть некоторые корни многочлена $m(x) \in \overline{R}[x]$, и при любом $\lambda \in \{0, \dots, m-1\}$

$$A_{i+\lambda}(a^{q^\lambda}) = 0$$

(сумма $i + \lambda$ — по модулю m). Поэтому для всякого $j = i + \lambda \in \{0, \dots, m-1\}$ найдется такой неприводимый над $\overline{Q}$ делитель $h_j(x)$ многочлена $A_j(x)$, что $h_j(x) \mid m(x)$. Так как многочлены (50) попарно взаимно просты, то

$$h_0(x)h_1(x) \dots h_{m-1}(x) \mid m(x),$$

откуда

$$\text{rang } \overline{\xi}_s \geq \sum_{i=0}^{m-1} \deg h_i(x). \quad (51)$$

Выберем и зафиксируем $i \in \{0, \dots, m-1\}$. Исследуем неприводимые делители многочлена $A_i(x) \in \overline{Q}[x]$. Пусть b — корень многочлена $A_i(x)$ в его поле разложения A и автоморфизм $\rho \in \text{Aut}(A/\overline{Q})$ определен равенством

$$\rho(x) = x^{q^m}, \quad x \in A.$$

Поскольку $b = b^{q^m} \overline{\varphi}^i(\overline{\vartheta}_{s,k}^{-1})$ и $\overline{\vartheta}_{s,k} \in \overline{Q}$, при любом $j \geq 0$

$$b = b^{q^{mj}} \overline{\varphi}^i(\overline{\vartheta}_{s,k}^{-j}).$$

Очевидно, $\text{ord } \overline{\vartheta}_{s,k} = \tau_s$. Положив $j = \tau_s$, получим

$$b \in GF(q^{m\tau_s}) \quad \text{и} \quad b \notin GF(q^{ml}) \quad \text{при} \quad l < \tau_s.$$

Пусть l — длина цикла автоморфизма ρ , которому принадлежит элемент b . Тогда $b = b^{q^{ml}}$ и $l = \tau_s$. Если $h_i(x)$ — минимальный многочлен элемента b над полем $\overline{Q}$, то

$$h_i(x) = (x - b)(x - \rho(b)) \dots (x - \rho^{\tau_s-1}(b))$$

и $\deg h_i(x) = \tau_s$. Так как $i \in \{0, \dots, m-1\}$ было фиксировано произвольно, то

$$\forall i \in \{0, \dots, m-1\}: \deg h_i(x) = \tau_s.$$

Рассматривая это соотношение совместно с (51), получаем требуемое неравенство. ■

Напомним, что $t = \|w_1 + w_2 + \dots + w_{m-1}\|$. Начальному состоянию $w(0) \in S$ сопоставим множество

$$J_t = \{s \in \{1, \dots, m-1\} : \|w_s\| = t\}. \quad (52)$$

Через $L_R(F)^*$ обозначим множество всех ЛРП максимального периода над R с характеристическим многочленом $F(x)$. Справедлива

Теорема 13. Пусть $w(0) \in S$. Во введенных обозначениях ранг t -й координаты y_t в 2-адическом разложении выходной последовательности γ удовлетворяет двойному неравенству

$$m \cdot \sum_{s \in J_t} \tau_s \leq \text{rang } y_t - \text{rang } \gamma_{0,t} \leq m \cdot |J_t| \cdot \tau, \quad (53)$$

где $\gamma_{0,t}$ — t -я координата в 2-адическом разложении ЛРП $\gamma_0 \in L_R(F)^*$.

Доказательство. Ввиду разложения (42), равенства (44) и определения (52) множества J_t имеем

$$y_t = \gamma_{0,t} + \sum_{s \in J_t} \bar{\xi}_s,$$

где суммирование осуществляется в поле $\bar{R} = GF(q)$. Поскольку характеристические многочлены $\bar{G}_{s,k}(x^\tau)$, $s \in J_t$, попарно взаимно просты,

$$\text{rang } y_t = \text{rang } \gamma_{0,t} + \sum_{s \in J_t} \text{rang } \bar{\xi}_s.$$

Теперь двойное неравенство (53) следует из (46) и утверждения 12.

Кроме того, при всех $i \geq 0$

$$\gamma_0(i) = \psi(w_0(i)) = u(i),$$

где $u \in L_R(F)^*$. ■

Очевидно, что $\text{rang } \bar{\gamma}_0 = m$. Известно (см. [4]), что $\text{rang } \gamma_{0,1} = \frac{1}{2} \times m(m+3)$. Поэтому справедливы следующие утверждения.

Следствие 14. Если выполнены условия теоремы 13, $n = 1$ и ε_s — индикатор того, что $\omega_s \neq 0$, $s = 1, 2, \dots, m-1$, то

$$m + m \sum_{s=1}^{m-1} \tau_s \varepsilon_s \leq \text{rang } \gamma \leq m + m\tau \sum_{s=1}^{m-1} \varepsilon_s.$$

В частности, если $\varepsilon_s = 1$ для всякого $s \in \mathbb{Z}_m^*$, то

$$\text{rang } \gamma \geq m + m\varphi(m) \cdot \frac{q^m - 1}{q - 1},$$

где φ — функция Эйлера.

Следствие 15. Если выполнены условия теоремы 13, $n = 2$, $t \geq 1$ и ε_s — индикатор того, что $\omega_s \neq 0$, $s = 1, 2, \dots, m-1$, то

$$\frac{1}{2} \cdot m(m+3) + m \sum_{s=1}^{m-1} \tau_s \varepsilon_s \leq \text{rang } y_1 \leq \frac{1}{2} \cdot m(m+3) + m\tau \sum_{s=1}^{m-1} \varepsilon_s.$$

В частности, если $\varepsilon_s = 1$ для всякого $s \in \mathbb{Z}_m^*$, то

$$\text{rang } y_1 \geq \frac{1}{2} \cdot m(m+3) + m\varphi(m) \cdot \frac{q^m - 1}{q - 1},$$

где φ — функция Эйлера.

Теорема 13 и следствия из нее обобщают на кольцо Галуа теорему 5 из работы [2].

§ 5. Частотные характеристики результирующей последовательности

Как и в предыдущем параграфе, $t = \|\omega_1 + \omega_2 + \dots + \omega_{m-1}\|$. Изучим частотные характеристики ПСП y_t в ситуации, когда $\omega(0) \in S$ и $\varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_{m-1} = 1$.

Рассмотрим сначала случай $n = 1$. Пусть $\varepsilon_s = 1$ и $\varepsilon_i = 0$ для всякого $i \neq s$. Тогда

$$\gamma = \gamma_0 + \gamma_s, \quad (54)$$

причем $\gamma_0 \in L_R(F)^*$ и $\gamma_s \in L_R(G_{s,k}(x^T))$. Поскольку $\omega_s \neq 0$, утверждение 11 гарантирует, что всякая регулярная (d, τ) -выборка γ_s^d из ЛРП γ_s , $d \geq 0$, является ненулевой. Следовательно, минимальный многочлен ЛРП γ_s^d равен $G_{s,k}(x)$.

Пусть $d_s = (q - 1, \tau_s)$. Параметры q, m, s определяют вещественные величины

$$A = \frac{d_s}{q-1} - \frac{1}{q^{(m,s)}-1} \quad \text{и} \quad B = \sqrt{q} \left(1 - \frac{d_s}{q-1}\right). \quad (55)$$

Если $q > 2$, то определена также вещественная величина

$$C = \left(\frac{q-1}{q-2} \sqrt{q} + \frac{q-1}{q^{(m,s)}-1} \right) \cdot \left(1 + \frac{\sqrt{q}}{q-2} \right)^{-1}.$$

Легко видеть, что

$$0 \leq A < 1, \quad 0 \leq B < \sqrt{q}, \quad 1 < C < q-1. \quad (56)$$

Положим

$$\Delta(q, m, s) = \begin{cases} \frac{q-1}{q} \cdot A \cdot q^{m/2}, & \text{если } q = 2 \text{ или } q > 2, \quad d_s \geq C, \\ \frac{1}{q} \cdot (A + B) \cdot q^{m/2}, & \text{если } q > 2 \text{ и } d_s < C. \end{cases} \quad (57)$$

Для всякого $z \in R$ обозначим через $N_z(\gamma_s)$ количество знаков z на цикле ЛРП γ_s .

Утверждение 16. Пусть $n = 1$, $w(0) \in S$, $\varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_{m-1} = 1$ и $\varepsilon_s = 1$ для некоторого $s \in \{1, \dots, m-1\}$. Тогда при любых $z \in R$ и $d \geq 0$

$$\left| N_z(\gamma_s^d) - \frac{q^{m-1} - \delta_{z,0}}{q^{(m,s)} - 1} \right| \leq \Delta(q, m, s),$$

где $\delta_{z,0}$ — символ Кронекера.

Доказательство. Выберем $z \in R$ и $d \geq 0$. Минимальный многочлен ЛРП γ_s^d есть $G_{s,k}(x)$. Этот многочлен неприводим и имеет период τ_s . Положим

$$h = [\tau_s, q-1] = \frac{\tau_s \cdot (q-1)}{d_s}.$$

Согласно [11], частоты появления знаков на цикле γ_s^d удовлетворяют неравенствам

$$\begin{aligned} \left| N_0(\gamma_s^d) - \frac{(q^{m-1} - 1) \cdot \tau_s}{q^m - 1} \right| &\leq \frac{q-1}{q} \cdot \left(\frac{\tau_s}{h} - \frac{\tau_s}{q^m - 1} \right) \cdot q^{m/2}, \\ \left| N_a(\gamma_s^d) - \frac{q^{m-1} \cdot \tau_s}{q^m - 1} \right| &\leq \frac{1}{q} \left(\frac{\tau_s}{h} - \frac{\tau_s}{q^m - 1} + \frac{h - \tau_s}{h} \sqrt{q} \right) \cdot q^{m/2}, \quad a \neq 0. \end{aligned}$$

Учитывая обозначения (55), эти соотношения можно переписать в виде

$$\begin{aligned} \left| N_0(\gamma_s^d) - \frac{q^{m-1} - 1}{q^{(m,s)} - 1} \right| &\leq \frac{q-1}{q} \cdot A \cdot q^{m/2}, \\ \left| N_a(\gamma_s^d) - \frac{q^{m-1}}{q^{(m,s)} - 1} \right| &\leq \frac{1}{q} \cdot (A+B) \cdot q^{m/2}, \quad a \neq 0. \end{aligned}$$

Отсюда следует, что при любом $z \in R$

$$\left| N_z(\gamma_s^d) - \frac{q^{m-1} - \delta_{z,0}}{q^{(m,s)} - 1} \right| \leq \frac{1}{q} \cdot \max\{(q-1) \cdot A, A+B\} \cdot q^{m/2}.$$

Если $q = 2$, то $B = 0$, $\max\{(q-1) \cdot A, A+B\} = A$, и утверждение доказано. Непосредственно проверяется, что в случае $q > 2$ условия $(q-1)A \geq A+B$ и $d_s \geq C$ эквивалентны. ■

Пусть $p_z(\gamma) = N_z(\gamma)/T(\gamma)$ — относительная частота появления $z \in R$ на цикле последовательности γ .

Теорема 17. Пусть $n = 1$, $w(0) \in S$, $\varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_{m-1} = 1$ и $\varepsilon_s = 1$ для некоторого $s \in \{1, \dots, m-1\}$. Тогда при любом $z \in R$

$$\left| p_z(\gamma) - \frac{\tau^2 - (1-q)^{\delta_{z,0}}}{q \cdot \tau^2} \right| \leq \Delta(q, m, s) \cdot \tau_s^{-1},$$

где $\delta_{z,0}$ — символ Кронекера.

Доказательство. Последовательность γ_0 есть ЛРП максимального периода τ . Последовательность γ_s^d есть регулярная (d, τ) -выборка из γ_s . Поэтому, ввиду (54),

$$N_z(\gamma) = \sum_{d=0}^{\tau-1} N_{z-\gamma_0(d)}(\gamma_s^d) = \sum_{d: \gamma_0(d)=0} N_z(\gamma_s^d) + \sum_{a \neq 0} \sum_{d: \gamma_0(d)=a} N_{z-a}(\gamma_s^d).$$

С учетом того, что $GF(q) = GF(2^r)$ — поле характеристики 2, получаем

$$N_0(\gamma) = \sum_{d: \gamma_0(d)=0} N_0(\gamma_s^d) + \sum_{a \neq 0} \sum_{d: \gamma_0(d)=a} N_a(\gamma_s^d), \quad (58)$$

$$N_z(\gamma) = \sum_{d: \gamma_0(d)=z} N_0(\gamma_s^d) + \sum_{d: \gamma_0(d)=0} N_z(\gamma_s^d) + \sum_{a \notin \{0, z\}} \sum_{d: \gamma_0(d)=a} N_{z-a}(\gamma_s^d), \quad z \neq 0. \quad (59)$$

Согласно утверждению 16, величины $N_0(\gamma_s^d)$ и $N_z(\gamma_s^d)$, $z \neq 0$ представляются в виде

$$N_0(\gamma_s^d) = \frac{q^{m-1} - 1}{q^{(m,s)} - 1} + D_0(\gamma_s^d), \quad N_a(\gamma_s^d) = \frac{q^{m-1}}{q^{(m,s)} - 1} + D_a(\gamma_s^d), \quad (60)$$

где $|D_z(\gamma_s^d)| \leq \Delta(q, m, s)$ для всякого $z \in R$.

На цикле ЛРП γ_0 присутствуют $q^{m-1} - 1$ нулей, а каждый ненулевой элемент появляется q^{m-1} раз. Следовательно, в правой части равенства (58) первая сумма содержит $(q^{m-1} - 1)$ слагаемых, а вторая — $(q^m - q^{m-1})$ слагаемых. Подставив (60) в (58) и проведя очевидные преобразования, получим

$$N_0(\gamma) = \frac{\tau^2 + (q - 1)}{q(q^{(m,s)} - 1)} + \left[\sum_{d: \gamma_0(d)=0} D_0(\gamma_s^d) + \sum_{a \neq 0} \sum_{d: \gamma_0(d)=a} D_a(\gamma_s^d) \right].$$

Поскольку

$$\begin{aligned} & \left| \sum_{d: \gamma_0(d)=0} D_0(\gamma_s^d) + \sum_{a \neq 0} \sum_{d: \gamma_0(d)=a} D_a(\gamma_s^d) \right| \leq \\ & \leq \sum_{d: \gamma_0(d)=0} |D_0(\gamma_s^d)| + \sum_{a \neq 0} \sum_{d: \gamma_0(d)=a} |D_a(\gamma_s^d)| \leq \Delta(q, m, s) \cdot \tau, \end{aligned}$$

имеем

$$\left| N_0(\gamma) - \frac{\tau^2 + (q - 1)}{q(q^{(m,s)} - 1)} \right| \leq \Delta(q, m, s) \cdot \tau. \quad (61)$$

Аналогично, подставив (60) в (59), получим

$$\left| N_z(\gamma) - \frac{\tau^2 - 1}{q(q^{(m,s)} - 1)} \right| \leq \Delta(q, m, s) \cdot \tau \quad \text{для всех } z \neq 0. \quad (62)$$

Символ Кронекера позволяет записать (61) и (62) в виде одного неравенства

$$\left| N_z(\gamma) - \frac{\tau^2 - (1 - q)^{\delta_{z,0}}}{q(q^{(m,s)} - 1)} \right| \leq \Delta(q, m, s) \cdot \tau \quad \text{для всех } z \in R.$$

Разделив обе части на $T(\gamma) = \tau \cdot \tau_s$, получим утверждение теоремы. ■

Заметим, что начальное заполнение $\omega(0)$ является основным тогда и только тогда, когда $(m, j) = 1$. Из доказанной теоремы и неравенств (56) вытекает

Следствие 18. Пусть выполнены условия теоремы 17, $q > 2$ и $\omega(0)$ — основное состояние. Тогда:

а) если $d_s < C$, то для всякого $z \in R$

$$\left| p_z(\gamma) - \frac{\tau^2 - (1-q)^{\delta_{z,0}}}{q \cdot \tau^2} \right| < \frac{(\sqrt{q} + 1)(q-1)}{q^m - 1} \cdot q^{m/2-1} = O(q^{-m/2}), \quad m \rightarrow \infty;$$

б) если $d_s \geq C$, то для всякого $z \in R$

$$\left| p_z(\gamma) - \frac{\tau^2 - (1-q)^{\delta_{z,0}}}{q \cdot \tau^2} \right| < \frac{(q-1)^2}{q^m - 1} \cdot q^{m/2-1} = O(q^{-m/2}), \quad m \rightarrow \infty.$$

В ситуации, когда $d_s = q - 1$, формулировка теоремы 17 существенно упрощается.

Следствие 19. Пусть выполнены условия теоремы 17, $(q-1) \mid \tau_s$. Тогда для всякого $z \in R$ справедливо неравенство

$$\left| p_z(\gamma) - \frac{\tau^2 - (1-q)^{\delta_{z,0}}}{q \cdot \tau^2} \right| \leq \frac{q-1}{q} \cdot \left(\frac{1}{\tau_s} - \frac{1}{\tau} \right) \cdot q^{m/2}.$$

Доказательство. Если $(q-1) \mid \tau_s$, то, согласно (56), $d_s = q - 1 > C$. По теореме 17 для всякого $z \in R$ имеем

$$\begin{aligned} & \left| p_z(\gamma) - \frac{\tau^2 - (1-q)^{\delta_{z,0}}}{q \cdot \tau^2} \right| \leq \frac{q-1}{q} \cdot A \cdot q^{m/2} \cdot \frac{q^{(m,s)} - 1}{q^m - 1} = \\ & = \frac{q-1}{q} \cdot \left(1 - \frac{1}{q^{(m,s)} - 1} \right) \cdot q^{m/2} \cdot \frac{q^{(m,s)} - 1}{q^m - 1} = \frac{q-1}{q} \cdot \left(\frac{1}{\tau_s} - \frac{1}{\tau} \right) \cdot q^{m/2}. \quad \blacksquare \end{aligned}$$

Теперь рассмотрим общий случай $n \geq 1$. ПСП $\bar{\xi}_s$ является выходной последовательностью автомата (48) и аннулируется многочленом $\bar{G}_{s,k}(x^\tau)$. По утверждению 11, всякая регулярная τ -выборка из $\bar{\xi}_s$ является ненулевой и, следовательно, имеет минимальный многочлен $\bar{G}_{s,k}(x)$. Для всякого $d \geq 0$ обозначим через $\bar{\xi}_s^{(d)}$ регулярную $(d, 2^i \cdot \tau)$ -выборку из $\bar{\xi}_s$. Поскольку $\bar{\vartheta}_{s,k}$ — корень многочлена $\bar{G}_{s,k}(x)$ в поле $\bar{Q}$, имеем

$$\forall d \geq 0 \quad \exists a_{s,d} \in \bar{Q} \quad \forall i \geq 0: \bar{\xi}_s^{(d)}(i) = \text{tr}_{\bar{Q}}(a_{s,d} \cdot \bar{\vartheta}_{s,k}^{2^i}), \quad (63)$$

где tr — функция «след».

Будем использовать следующий теоретико-числовой результат (см., например, [5, т.1, с.102]).

Утверждение 20. Если $m \geq 2$, $q \geq 2$ и каждый простой делитель числа $q^m - 1$ делит число $q^l - 1$ при некотором $l \in \{1, 2, \dots, m-1\}$, то либо $m = 2$ и $q + 1 = 2^i$ для некоторого $i \geq 1$, либо $m = 6$ и $q = 2$.

Пусть $g_{s,k}(x) \in \bar{R}[x]$ — минимальный многочлен элемента $\bar{\vartheta}_{s,k}^{2^t} \in \bar{Q}$ над полем $\bar{R}$. Справедливо

Утверждение 21. Для всякого $d \geq 0$ многочлен $g_{s,k}(x)$ является минимальным многочленом ЛРП $\bar{\xi}_s^{(d)}$, причем $\deg g_{s,k}(x) = m$.

Доказательство. Пусть $\tilde{R} = R/2^{t+1}R$ и $\tilde{\gamma}_s$ — образ γ_s под действием естественного эпиморфизма $R \rightarrow \tilde{R}$. Тогда, по утверждению 11, $\tilde{\gamma}_s \neq 0$ и всякая регулярная $(d, 2^t \cdot \tau)$ -выборка из $\tilde{\gamma}_s$ является ненулевой. Следовательно, $\bar{\xi}_s^{(d)} \neq 0$, и ввиду (63) многочлен $g_{s,k}(x)$ является минимальным для ЛРП $\bar{\xi}_s^{(d)}$.

Степень многочлена $g_{s,k}(x)$ равна минимальному $l \geq 1$ со свойством $\bar{\vartheta}_{s,k}^{2^t} \in GF(q^l)$, т. е. минимальному $l \geq 1$ со свойством

$$\text{ord } \bar{\vartheta}_{s,k}^{2^t} = \frac{q^m - 1}{q^{(m,s)} - 1} \mid q^l - 1. \quad (64)$$

Из утверждения 20 следует, что минимальное $l \geq 1$ со свойством (64) равно m . ■

Применив к ЛРП $\bar{\xi}_s^{(d)}$ и ее минимальному многочлену $g_{s,k}(x)$ результаты работы [11], получим

$$\left| N_z(\bar{\xi}_s^{(d)}) - \frac{q^{m-1} - \delta_{z,0}}{q^{(m,s)} - 1} \right| \leq \Delta(q, m, s) \quad \text{для всех } z \in \bar{R}. \quad (65)$$

Воспользовавшись очевидным равенством $\delta_{z,0} = 1/2 - (-1)^{\delta_{z,0}} \cdot 1/2$, получим

$$\frac{q^{m-1} - \delta_{z,0}}{q^{(m,s)} - 1} = \frac{q^{m-1} - 1/2}{q^{(m,s)} - 1} + \frac{(-1)^{\delta_{z,0}}}{2(q^{(m,s)} - 1)}.$$

Отсюда

$$\begin{aligned} \left| N_z(\bar{\xi}_s^{(d)}) - \frac{q^{m-1} - \delta_{z,0}}{q^{(m,s)} - 1} \right| &= \left| N_z(\bar{\xi}_s^{(d)}) - \frac{q^{m-1} - 1/2}{q^{(m,s)} - 1} - \frac{(-1)^{\delta_{z,0}}}{2(q^{(m,s)} - 1)} \right| \geq \\ &\geq \left| N_z(\bar{\xi}_s^{(d)}) - \frac{q^{m-1} - 1/2}{q^{(m,s)} - 1} \right| - \frac{1}{2(q^{(m,s)} - 1)}. \end{aligned}$$

С учетом (65) имеем для всех $z \in \bar{R}$, $d \geq 0$

$$\left| N_z(\bar{\xi}_s^{(d)}) - \frac{q^{m-1} - 1/2}{q^{(m,s)} - 1} \right| \leq \frac{1}{2(q^{(m,s)} - 1)} + \Delta(q, m, s). \quad (66)$$

Поскольку $T(\gamma_{0,t}) = 2^t \cdot \tau$, а $\bar{\xi}_s^{(d)}$ есть регулярная $(d, 2^t \cdot \tau)$ -выборка из последовательности $\bar{\xi}_s$, справедливо равенство

$$N_z(y_t) = \sum_{d=0}^{2^t \tau - 1} N_{z-\gamma_{0,t}(d)}(\bar{\xi}_s^{(d)}). \quad (67)$$

В силу (66) для всякого $a \in \bar{R}$ величина $N_a(\bar{\xi}_s^{(d)})$ представляется в виде

$$N_a(\bar{\xi}_s^{(d)}) = \frac{q^{m-1} - 1/2}{q^{(m,s)} - 1} + \Delta_a(\bar{\xi}_s^{(d)}), \quad (68)$$

где

$$|\Delta_a(\bar{\xi}_s^{(d)})| \leq \frac{1}{2(q^{(m,s)} - 1)} + \Delta(q, m, s). \quad (69)$$

Подставив (68) в (67), получим

$$N_z(y_t) = 2^t \tau_s \cdot (q^{m-1} - 1/2) + \sum_{d=0}^{2^t \tau - 1} \Delta_{z-\gamma_{0,t}(d)}(\bar{\xi}_s^{(d)}).$$

Отсюда ввиду (69) имеем

$$|N_z(y_t) - 2^t \tau_s \cdot (q^{m-1} - 1/2)| \leq 2^{t-1} \tau_s + \Delta(q, m, s) \cdot 2^t \tau.$$

Разделив обе части на $T(y_t) = 2^t \tau \tau_s$, придем к следующему утверждению.

Теорема 22. Пусть $\omega(0) \in S$, $\varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_{m-1} = 1$ и $t = \|\omega_s\| < n$ для некоторого $s \in \{1, \dots, m-1\}$. Тогда

$$\forall z \in \bar{R}: \left| p_z(y_t) - \frac{q^{m-1} - 1/2}{q^m - 1} \right| \leq \frac{1}{2\tau} + \Delta(q, m, s) \cdot \tau_s^{-1},$$

где $\delta_{z,0}$ — символ Кронекера.

Аналогично следствиям 18 и 19 доказываются следующие утверждения.

Следствие 23. Пусть выполнены условия теоремы 22, $q > 2$ и $w(0)$ — основное состояние. Тогда:

а) если $d_s < C$, то для всякого $z \in \bar{R}$

$$\left| p_z(y_t) - \frac{q^{m-1} - 1/2}{q^m - 1} \right| < \frac{1}{2(q^m - 1)} + \frac{(\sqrt{q} + 1)(q - 1)}{q^m - 1} \cdot q^{m/2-1} = O(q^{-m/2});$$

б) если $d_s \geq C$, то для всякого $z \in \bar{R}$

$$\left| p_z(y_t) - \frac{q^{m-1} - 1/2}{q^m - 1} \right| < \frac{1}{2(q^m - 1)} + \frac{(q - 1)^2}{q^m - 1} \cdot q^{m/2-1} = O(q^{-m/2}).$$

Следствие 24. Пусть выполнены условия теоремы 22, $(q - 1) \mid \tau_s$. Тогда для всякого $z \in \bar{R}$ справедливо неравенство

$$\left| p_z(y_t) - \frac{q^{m-1} - 1/2}{q^m - 1} \right| \leq \frac{1}{2\tau} + \frac{q - 1}{q} \cdot \left(\frac{1}{\tau_s} - \frac{1}{\tau} \right) \cdot q^{m/2}.$$

Теоремы 17, 22 и следствия из них свидетельствуют об асимптотической равномерности при $m \rightarrow \infty$ распределения знаков на цикле результирующей последовательности y_t .

§ 6. Заключение

В работе рассмотрен самоуправляемый 2-линейный регистр сдвига $\mathcal{A}^\beta$ над кольцом Галуа $R = GR(q^n, 2^n)$ с равными элементарными характеристическими многочленами максимального периода $2^{n-1}(q^m - 1)$ и функцией самоуправления β вида (5), вообще говоря, нелинейной. Установлено следующее:

1. Автомат $\mathcal{A}^\beta$ регулярен. Его цикловая структура полностью описана (теорема 8). Почти все состояния лежат на циклах максимальной длины $O(q^{2m})$, $m \rightarrow \infty$.
2. Имеется широкий класс начальных заполнений регистра $\mathcal{A}^\beta$, при которых ранг одной из координат y_t в 2-адическом разложении выходной последовательности γ есть $O(m^2 q^m)$, $m \rightarrow \infty$ (теорема 13).
3. Для одного семейства начальных заполнений показано, что отклонение частоты появления знаков на цикле последовательности y_t от среднего значения есть $O(q^{-m/2})$, $m \rightarrow \infty$ (теорема 22).

§ 7. Благодарности

Автор выражает глубокую признательность А. А. Нечаеву за постановку задачи и постоянное внимание к этой работе, а также О. В. Камловскому за обсуждение результатов и ценные замечания.

Список литературы

1. *Козлитин О. А.* Периодические свойства простейшего 2-линейного регистра сдвига // Дискретная математика. — 2007. — Т. 19. Вып. 3. — С. 51–78.
2. *Козлитин О. А.* Свойства выходной последовательности простейшего самоуправляемого 2-линейного регистра сдвига // Дискретная математика. — 2007. — Т. 19. Вып. 4. — С. 70–96.
3. *Козлитин О. А.* Периодические свойства 2-линейного регистра сдвига над кольцом Галуа // Обзорение прикладной и промышленной математики. — 2011. — Т. 18. Вып. 4. — С. 513–526.
4. *Кузьмин А. С., Нечаев А. А.* Линейные рекуррентные последовательности над кольцами Галуа // Алгебра и логика. — 1995. — Т. 34. Вып. 2. — С. 169–189.
5. *Лидл Р., Нидеррайтер Г.* Конечные поля. — М.: Мир, 1988. — 818 с.
6. *Нечаев А. А.* Многомерные регистры сдвига и сложность мультипоследовательностей // В сб.: Труды по дискретной математике. Т. 6. — М.: ФИЗМАТЛИТ, 2002. — С. 150–164.
7. *Нечаев А. А.* О подобии матриц над коммутативным локальным артиновым кольцом // Труды семинара имени И. Г. Петровского. — 1983. — Вып. 9. — С. 81–101.
8. *Нечаев А. А.* Цикловые типы линейных подстановок над конечными коммутативными кольцами // Математический сборник. — 1993. — Т. 184. Вып. 3. — С. 21–56.
9. *Фомичев В. М.* Дискретная математика и криптология. — М.: Диалог-МИФИ, 2003. — 397 с.
10. *Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A.* Linear recurring sequences over rings and modules // J. Math. Sciences. — 1995. — V. 76. № 6. — P. 2793–2915.
11. *McEliece R. J.* Irreducible cyclic codes and Gauss sums // In: Combinatorics (M. Hall, Jr. and J. H. van Lint, eds.). — 1975. — P. 185–202.
12. *Nomura T., Fukuda A.* Linear recurring planes and two-dimensional cyclic codes // Electronic Commun. Japan. — 1971. — V. 54. No 3. — P. 23–30.