Math-Net.Ru

Общероссийский математический портал

О. А. Козлитин, Периодические свойства простейшего 2-линейного регистра сдвига, *Дискрет. матем.*, 2007, том 19, выпуск 3, 51–78

DOI: <https://doi.org/10.4213/dm965>

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: 44.207.124.84

26 апреля 2023 г., 12:25:05

Периодические свойства простейшего 2-линейного регистра сдвига

© 2007 г. О. А. Козлитин

Изучается граф переходов состояний простейшего самоуправляемого 2-линейного регистра сдвига над кольцом Галуа $R = GR(2^r, 2^n)$. Найдена верхняя оценка длины цикла в этом графе. В случае $R = \mathbb{Z}_{2^n}$ описаны состояния, принадлежащие циклам максимальной длины. Определено количество таких состояний.

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

1. Введение

Пусть $r, n \in \mathbb{N}$, $q = 2^r$, $R = GR(q^n, 2^n)$ – кольцо Галуа [3] порядка q^n и характеристики 2^n . 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 [2], 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

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

Унитарный периодический многочлен $F(x) \in R[x]$ такой, что $D(F) = 0$, назовем реверсивным. Согласно [2] унитарный многочлен $F(x) \in R[x]$ реверсивен, если и только если его свободный коэффициент обратим, то есть $F(0) \in R^*$.

Пусть $F_0(x_0)$ и $F_1(x_1)$ — реверсивные многочлены над кольцом R степеней m_0 и m_1 соответственно. Множество прямоугольных матриц $M = R_{m_0 \times m_1}$ является левым модулем над кольцом R . Зададим автоморфизмы φ_0 и φ_1 модуля ${}_R M$ равенствами

$$\forall X \in M: \quad \varphi_0(X) = S(F_0)^T X, \quad \varphi_1(X) = XS(F_1),$$

где символ T означает операцию транспонирования. Используя эти автоморфизмы как частичные функции перехода, построим автономный автомат $\mathfrak{A}^\beta = \langle M, R, h, \psi \rangle$, где M — множество состояний, R — выходной алфавит, $\psi: M \rightarrow R$ — 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 [8], построенный автомат $\mathfrak{A}^\beta$ будем называть простейшим самоуправляемым 2-линейным регистром сдвига (2-ЛРС) или просто регистром. Реверсивные многочлены $F_0(x_0)$ и $F_1(x_1)$ называются элементарными характеристическими многочленами регистра $\mathfrak{A}^\beta$.

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

$$R \rightarrow \bar{R} = R/2R = GF(q) = GF(2^r).$$

Для каждого элемента $a \in R$ (матрицы $X \in M$, многочлена $F(x) \in R[x]$) будем обозначать через $\bar{a}$ (соответственно, через $\bar{X}$, $\bar{F}$) 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

$$\forall X \in M: \quad \beta(X) = \text{tr}(\bar{x}_{1,1}), \quad (2)$$

где через tr обозначена функция след из поля $\bar{R} = GF(2^r)$ в поле $GF(2)$:

$$\forall a \in \bar{R}: \quad \text{tr}(a) = a + a^2 + a^{2^2} + \dots + a^{2^{r-1}}.$$

Автомату $\mathfrak{A}^\beta$ естественным образом ставится в соответствие граф переходов состояний $\mathcal{G}(\mathfrak{A}^\beta) = (M, V)$, в котором пара $(X, Y) \in M^2$ принадлежит множеству дуг V в точности если $Y = h(X) = \varphi_{\beta(X)}(X)$.

Основные результаты данной работы, связанные с исследованием графа $\mathcal{G}(\mathfrak{A}^\beta)$, могут быть охарактеризованы следующим образом. Пусть

$$W = (W(0), W(1), \dots, W(i), \dots), \quad W(i+1) = h(W(i)) = \varphi_{\beta(W(i))}(W(i)), \quad (3)$$

есть последовательность состояний автомата $\mathfrak{A}^\beta$ с начальным состоянием $W(0)$. Тогда это периодическая последовательность с длиной подхода (дефектом) $D(W)$ и периодом $T(W)$. Напомним, что унитарный многочлен $F(x) \in R[x]$ степени m называется многочленом Галуа, если $\bar{F}(x)$ — неприводимый многочлен над полем $\bar{R}$, и многочленом максимального периода, если $T(F) = 2^{n-1}(q^m - 1)$.

1. Если $F_0(x_0)$ и $F_1(x_1)$ — многочлены Галуа, то справедливо неравенство

$$D(W) + T(W) \leq 2^{n-1} \frac{T(\bar{F}_0)T(\bar{F}_1)}{(T(\bar{F}_0), T(\bar{F}_1), q-1)}, \quad (4)$$

где в знаменателе стоит наибольший общий делитель чисел $T(\bar{F}_0)$, $T(\bar{F}_1)$ и $q-1$ (теорема 1). В частности, если $\bar{F}_0$ и $\bar{F}_1$ суть многочлены максимального периода, то длина любого цикла в графе $\mathcal{G}(\mathfrak{A}^\beta)$ не превосходит величины

$$2^{n-1} \frac{(q^{m_0} - 1)(q^{m_1} - 1)}{q - 1}.$$

2. Пусть $R = \mathbf{Z}_{2^n}$. Тогда для любых реверсивных многочленов $F_0(x_0)$ и $F_1(x_1)$ справедливо неравенства

$$D(W) + T(W) \leq 2^{n-1} T(\bar{F}_0)T(\bar{F}_1) \leq 2^{n-1} (2^{m_0} - 1)(2^{m_1} - 1). \quad (5)$$

Найдены условия, необходимые для того, чтобы выполнялось соотношение

$$T(W) = 2^{n-1} (2^{m_0} - 1)(2^{m_1} - 1) \quad (6)$$

(следствие 1). В частности, если $n \geq 2$, $F_0(x) = F_1(x) = F(x)$ — многочлен максимального периода степени $m \geq 2$, то равенство (6) влечет совокупность условий

$$\bar{W}(0) \neq 0, \quad S(\bar{F})^T \bar{W}(0) = \bar{W}(0)S(\bar{F}), \quad S(F)^T W(0) \neq W(0)S(F). \quad (7)$$

3. Пусть $R = \mathbf{Z}_{2^n}$, $n \geq 2$, $F_0(x) = F_1(x) = F(x)$ — многочлен максимального периода степени $m \geq 2$. Назовем состояние $W(0)$ регистра $\mathfrak{A}^\beta$ основным, если для последовательности W выполняется равенство (6), то есть $T(W) = 2^{n-1} (2^m - 1)^2$. Найден простой критерий свойства быть основным состоянием (следствие 4). Показано, что число $N(\mathfrak{A}^\beta)$ основных состояний регистра $\mathfrak{A}^\beta$ удовлетворяет соотношению

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

где μ — функция Мебиуса (теорема 7).

2. Верхняя граница длины цикла в графе переходов состояний

В этом параграфе будет получена верхняя оценка величины $D(W) + T(W)$. При этом понадобятся некоторые понятия и результаты из работ [4] и [12].

Напомним понятие ЛПП-семейства [12]. Всякую функцию $\mu: \mathbf{N}_0^2 \rightarrow R$ назовем 2-последовательностью над кольцом R . Обозначим через $R^{(2)}$ семейство всех 2-последовательностей над R . Множество $R^{(2)}$ является абелевой группой с операцией сложения

$$\forall \mu, \nu \in R^{(2)}, \mathbf{z} = (z_0, z_1) \in \mathbf{N}_0^2: \quad (\mu + \nu)(\mathbf{z}) = \mu(\mathbf{z}) + \nu(\mathbf{z}).$$

Всякий многочлен из $R[x_0, x_1]$ может быть записан в виде

$$H(x_0, x_1) = H(\mathbf{x}) = \sum_{\mathbf{s}=(s_0, s_1) \in \mathbf{N}_0^2} h_{\mathbf{s}} \mathbf{x}^{\mathbf{s}},$$

где $\mathbf{x}^s = x_0^{s_0} x_1^{s_1}$.

Произведением многочлена $H(\mathbf{x})$ и 2-последовательности μ назовем 2-последовательность ν , определяемую равенством

$$\forall \mathbf{z} = (z_0, z_1) \in \mathbb{N}_0^2: \quad \nu(\mathbf{z}) = \sum_{\mathbf{s} \in \mathbb{N}_0^2} h_{\mathbf{s}} \mu(\mathbf{z} + \mathbf{s}).$$

Эта операция превращает группу $R^{(2)}$ в левый модуль над кольцом $R[x_0, x_1]$.

Идеал I кольца $R[x_0, x_1]$ называется унитарным, если существуют унитарные многочлены $F_0(x), F_1(x) \in R[x]$ такие, что $F_0(x_0), F_1(x_1) \in I$.

Для всякого унитарного идеала $I \triangleleft R[x_0, x_1]$ назовем ЛРП-семейством с характеристическим идеалом I множество 2-последовательностей

$$L_R(I) = \{\mu \in R^{(2)} : \forall H(\mathbf{x}) \in I \quad H(\mathbf{x})\mu = 0\}.$$

Всякую 2-последовательность $\mu \in L_R(I)$ назовем 2-линейной рекуррентной последовательностью (2-ЛРП) с характеристическим идеалом I , а унитарные многочлены $F_0(x_0), F_1(x_1) \in I$ — элементарными характеристическими многочленами 2-ЛРП μ . Если идеал I порожден унитарными многочленами $F_0(x_0)$ и $F_1(x_1)$, то используем запись $L_R(I) = L_R(F_0, F_1)$.

Напомним понятие периода унитарного идеала $I \triangleleft R[x_0, x_1]$ из [4] и [12]. Поскольку кольцо $R = GR(q^n, 2^n)$ конечно, факторкольцо $S = R[x_0, x_1]/I$ также конечно. В таком кольце мультипликативная полугруппа

$$\mathbb{O}(I) = [e, \theta_0, \theta_1] < (S, \cdot),$$

порожденная единицей e кольца S и элементами $\theta_i = x_i + I$, также конечна и называется орбитальной полугруппой идеала I . Если $\varepsilon(I)$ есть произведение всех идемпотентов орбитальной полугруппы $\mathbb{O}(I)$, то $\mathcal{T}(I) = \varepsilon(I)\mathbb{O}(I)$ есть подгруппа полугруппы $\mathbb{O}(I)$ с единицей $\varepsilon(I)$. Величину $T(I) = |\mathcal{T}(I)|$ называют периодом идеала I .

Согласно [4] строка $\mathbf{t} \in \mathbb{N}_0^2$ называется вектор-периодом идеала I , если существует такой вектор $\mathbf{l} \in \mathbb{N}_0^2$, что $\mathbf{x}^{\mathbf{l}}(\mathbf{x}^{\mathbf{t}} - 1) \in I$. Обозначим через $\mathfrak{P}(I)$ подгруппу группы $(\mathbb{Z}^2, +)$, порожденную всеми вектор-периодами идеала I . Всюду далее

$$\begin{aligned} f_i(x_i) &= \bar{F}_i(x_i) \in \bar{R}[x_0, x_1], & i &= 0, 1, \\ I &= (F_0(x_0), F_1(x_1)) \triangleleft R[x_0, x_1], & \bar{I} &= (f_0(x_0), f_1(x_1)) \triangleleft \bar{R}[x_0, x_1]. \end{aligned}$$

Во введенных обозначениях период $T(I)$ равен индексу $[\mathbb{Z}^2 : \mathfrak{P}(I)]$ подгруппы $\mathfrak{P}(I)$ в группе $\mathbb{Z}^2$. Отсюда, очевидно, вытекает соотношение

$$T(\bar{I}) = [\mathbb{Z}^2 : \mathfrak{P}(\bar{I})]. \quad (8)$$

Если $A = (a_{i,j})_{n_1 \times n_2}$ и $B = (b_{i,j})_{n_3 \times n_4}$ суть матрицы над кольцом R , то тензорным произведением матриц A и B называется $n_1 n_3 \times n_2 n_4$ матрица

$$A \otimes B = \begin{pmatrix} a_{1,1}B & \dots & a_{1,n_2}B \\ \dots & \dots & \dots \\ a_{n_1,1}B & \dots & a_{n_1,n_2}B \end{pmatrix}.$$

Пусть E — единичная матрица над R размера $m_0 m_1 \times m_0 m_1$. Центральному результату данного параграфа предположим две леммы.

Лемма 1. Пусть $F_0(x_0)$, $F_1(x_1)$ — реверсивные многочлены над кольцом R .

(1) Включение $(t_0, t_1) \in \mathfrak{P}(I)$ выполнено тогда и только тогда, когда

$$S(F_0)^{t_0} \otimes S(F_1)^{t_1} = E.$$

(2) Включение $(t_0, t_1) \in \mathfrak{P}(\bar{I})$ выполнено тогда и только тогда, когда

$$S(f_0)^{t_0} \otimes S(f_1)^{t_1} = \bar{E}.$$

Доказательство. Докажем первое утверждение. Поскольку многочлены $F_0(x_0)$ и $F_1(x_1)$ реверсивны, $F_0(x_0) \mid x_0^{T(F_0)} - 1$, $F_1(x_1) \mid x_1^{T(F_1)} - 1$, откуда $x_0^{T(F_0)} - 1, x_1^{T(F_1)} - 1 \in I$. Поэтому $\theta_0 \theta_0^{T(F_0)-1} = e$, $\theta_1 \theta_1^{T(F_1)-1} = e$, где e — единица кольца S . Следовательно, элементы θ_0 и θ_1 обратимы. Заметим, что элементы θ_0 и θ_1 можно интерпретировать как операторы, действующие на семействе $L_R(I)$ по правилу $\theta_i \mu = x_i \mu$. Тогда согласно определению вектор-периода, по определению операторов θ_i , $i = 0, 1$, и в силу обратимости этих операторов для каждого вектора $(t_0, t_1) \in \mathbb{N}_0^2$ следующие утверждения эквивалентны:

- (а) $(t_0, t_1) \in \mathfrak{P}(I)$,
- (б) существуют числа $l_0 \geq 0$ и $l_1 \geq 0$ такие, что $x_0^{t_0+l_0} x_1^{t_1+l_1} \equiv x_0^{l_0} x_1^{l_1} \pmod{I}$,
- (в) существуют числа $l_0 \geq 0$ и $l_1 \geq 0$ такие, что $\theta_0^{t_0+l_0} \theta_1^{t_1+l_1} = \theta_0^{l_0} \theta_1^{l_1}$,
- (г) $\theta_0^{t_0} \theta_1^{t_1} = e$,
- (д) $\theta_0^{t_0} \theta_1^{t_1}$ есть тождественное преобразование семейства $L_R(I)$.

Пусть $\Pi = \{0, 1, \dots, m_0 - 1\} \times \{0, 1, \dots, m_1 - 1\}$. Для всякой 2-последовательности $\mu \in L_R(I)$ обозначим через $\mu[\Pi]$ матрицу начального состояния ЛРП μ :

$$\mu[\Pi] = \begin{pmatrix} \mu(0, 0) & \mu(0, 1) & \dots & \mu(0, m_1 - 1) \\ \mu(1, 0) & \mu(1, 1) & \dots & \mu(1, m_1 - 1) \\ \dots & \dots & \dots & \dots \\ \mu(m_0 - 1, 0) & \mu(m_0 - 1, 1) & \dots & \mu(m_0 - 1, m_1 - 1) \end{pmatrix}.$$

Поскольку $I = (F_0(x_0), F_1(x_1))$,

$$\{\mu[\Pi]: \mu \in L_R(I)\} = R_{m_0 \times m_1} = M. \quad (9)$$

Для каждой пары $(i, j) \in \{1, \dots, m_0\} \times \{1, \dots, m_1\}$ обозначим через $E^{(i,j)}$ матрицу, у которой в строке i и столбце j стоит 1, а на остальных позициях 0. Рассмотрим базис $E^{(1,1)}, \dots, E^{(1,m_1)}, E^{(2,1)}, \dots, E^{(2,m_1)}, \dots, E^{(m_0,1)}, \dots, E^{(m_0,m_1)}$ свободного модуля ${}_R M$. Будем записывать этот базис в виде столбца

$$e^\downarrow = (E^{(1,1)}, \dots, E^{(1,m_1)}, E^{(2,1)}, \dots, E^{(2,m_1)}, \dots, E^{(m_0,1)}, \dots, E^{(m_0,m_1)})^T. \quad (10)$$

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

$$X = \vec{X} e^\downarrow, \quad \vec{X} = (x_{1,1}, \dots, x_{1,m_1}, x_{2,1}, \dots, x_{m_0,m_1}).$$

Тогда если $\nu = \theta_0^{t_0} \theta_1^{t_1} \mu$, то, как нетрудно видеть, справедливо равенство

$$\vec{\nu}[\Pi] = \vec{\mu}[\Pi](S(F_0)^{t_0} \otimes S(F_1)^{t_1}).$$

Пусть $\theta_0^{t_0} \theta_1^{t_1}$ есть тождественное преобразование семейства $L_R(I)$. Тогда для любой 2-последовательности $\mu \in L_R(I)$

$$\vec{\mu}[\Pi] = \vec{\mu}[\Pi](S(F_0)^{t_0} \otimes S(F_1)^{t_1}).$$

В силу (9) для любой матрицы $X \in M$ выполняется равенство

$$\vec{X} = \vec{X}(S(F_0)^{t_0} \otimes S(F_1)^{t_1}),$$

откуда

$$S(F_0)^{t_0} \otimes S(F_1)^{t_1} = E.$$

Обратно, пусть $S(F_0)^{t_0} \otimes S(F_1)^{t_1} = E$. Для произвольной 2-последовательности $\mu \in L_R(I)$, если $\nu = \theta_0^{t_0} \theta_1^{t_1} \mu$, то $\vec{\nu}[\Pi] = \vec{\mu}[\Pi]$, откуда $\nu = \mu$. Значит, $\theta_0^{t_0} \theta_1^{t_1}$ есть тождественное преобразование семейства $L_R(I)$. Первое утверждение леммы доказано.

Второе утверждение следует из первого.

Лемма доказана.

Введем обозначение

$$\forall X \in M: \quad \alpha(X) = 1 - \beta(X) = 1 - \text{tr}(\bar{x}_{1,1}), \quad (11)$$

где значения функции след 0 и 1 рассматриваются как целые числа. Тогда для функции перехода h автономного автомата $\mathcal{A}^\beta$ справедливо соотношение

$$\forall X \in M: \quad h(X) = \vec{X}(S(F_0)^{\alpha(X)} \otimes S(F_1)^{\beta(X)} e^\downarrow, \quad (12)$$

где $e^\downarrow$ — базис модуля ${}_R M$, определенный равенством (10). Для изучаемой последовательности W вида (3) зададим последовательность $\mathbf{s}$ управляющих векторов равенствами

$$\forall j \geq 0: \quad \mathbf{s}(j) = (s_0(j), s_1(j)) = \left(\sum_{i=0}^{j-1} \alpha(W(i)), \sum_{i=0}^{j-1} \beta(W(i)) \right) \in \mathbb{N}_0^2. \quad (13)$$

При этом будем считать, что $\mathbf{s}(0) = (0, 0)$.

Рассмотрим отрезок из $T(\bar{I}) + 1$ таких векторов

$$\mathbf{s}(0), \mathbf{s}(1), \dots, \mathbf{s}(T(\bar{I})). \quad (14)$$

В силу равенства (8) в последовательности (14) для некоторых $d \geq 0, t > 0$ пара векторов $\mathbf{s}(d)$ и $\mathbf{s}(d+t)$ принадлежит одному смежному классу по подгруппе $\mathfrak{P}(\bar{I})$, то есть

$$\mathbf{s}(d+t) - \mathbf{s}(d) = \mathbf{t} \in \mathfrak{P}(\bar{I}). \quad (15)$$

Справедливо следующее утверждение.

Лемма 2. Во введенных обозначениях при условии (15) для всех $i \geq d$ справедливо равенство

$$\mathbf{s}(i+t) - \mathbf{s}(i) = \mathbf{t}.$$

Доказательство. Докажем лемму индукцией по параметру $i \geq d$. Для $i = d$ доказываемое утверждение следует из (15). Пусть оно верно для $i \geq d$, докажем его для $i + 1$.

Согласно пункту 2 леммы 1, поскольку $\mathbf{t} = (t_0, t_1)$ принадлежит группе вектор-периодов $\mathfrak{P}(\bar{I})$, справедливо равенство

$$S(f_0)^{t_0} \otimes S(f_1)^{t_1} = \bar{E}.$$

Напомним, что через $s_0(j)$ и $s_1(j)$ обозначены соответственно первая и вторая компонента вектора $\mathbf{s}(j)$. Тогда, учитывая цепочку соотношений

$$(t_0, t_1) = \mathbf{t} = \mathbf{s}(i + t) - \mathbf{s}(i) = (s_0(i + t) - s_0(i), s_1(i + t) - s_1(i)),$$

получаем, что

$$\begin{aligned} \bar{W}(i) &= \bar{W}(0)(S(f_0)^{s_0(i)} \otimes S(f_1)^{s_1(i)})\bar{e}^\downarrow = \bar{W}(0)(S(f_0)^{t_0+s_0(i)} \otimes S(f_1)^{t_1+s_1(i)})\bar{e}^\downarrow \\ &= \bar{W}(0)(S(f_0)^{s_0(i+t)} \otimes S(f_1)^{s_1(i+t)})\bar{e}^\downarrow = \bar{W}(i + t), \end{aligned}$$

где $\bar{e}^\downarrow$ — образ базиса $e^\downarrow$ под действием эпиморфизма $R \rightarrow \bar{R}$. Поскольку значения $\alpha(X)$ и $\beta(X)$ полностью определяются образом $\bar{X}$ матрицы $X \in M$ под действием эпиморфизма $R \rightarrow \bar{R}$, из последней цепочки равенств следуют соотношения

$$\alpha(W(i)) = \alpha(W(i + t)), \quad \beta(W(i)) = \beta(W(i + t)). \quad (16)$$

Из равенств (16) получаем, что

$$\begin{aligned} \mathbf{s}(i + t + 1) - \mathbf{s}(i + 1) &= \left(\sum_{j=i+1}^{i+t} \alpha(W(j)), \sum_{j=i+1}^{i+t} \beta(W(j)) \right) \\ &= \mathbf{s}(i + t) - \mathbf{s}(i) + (\alpha(W(i + t)) - \alpha(W(i)), \beta(W(i + t)) - \beta(W(i))) \\ &= \mathbf{s}(i + t) - \mathbf{s}(i) = \mathbf{t}. \end{aligned}$$

Лемма доказана.

Основным результатом этого параграфа является следующая теорема.

Теорема 1. Пусть $R = GR(2^n, 2^n)$, $F_0(x_0)$ и $F_1(x_1)$ суть реверсивные многочлены над кольцом R , $I = (F_0(x_0), F_1(x_1))$, $\beta(X) = \text{tr}(\bar{x}_{1,1})$ для всех матриц $X \in M$. Тогда для всякого начального состояния $W(0)$ автомата $\mathfrak{A}^\beta$, определенного в разделе 1, справедливо неравенство

$$D(W) + T(W) \leq 2^{n-1}T(\bar{I}). \quad (17)$$

Доказательство. Согласно лемме 2 для всех $i \geq d$, $j \geq 0$

$$\mathbf{s}(i + jt) = \mathbf{s}(i) + j(\mathbf{s}(i + t) - \mathbf{s}(i)) = \mathbf{s}(i) + j\mathbf{t}. \quad (18)$$

Так как $\mathbf{t} \in \mathfrak{P}(\bar{I})$, справедливо соотношение

$$\mathbf{x}^{\mathbf{t}} = x_0^{t_0} x_1^{t_1} \equiv 1 \pmod{\bar{I}},$$

то есть существуют $H(x_0, x_1) \in R[x_0, x_1]$ и $J(x_0, x_1) \in I$ такие, что

$$\mathbf{x}^t - 1 = J(\mathbf{x}) + 2H(\mathbf{x}).$$

Отсюда

$$\mathbf{x}^t \equiv 1 + 2H(\mathbf{x}) \pmod{I}.$$

Методом математической индукции легко показать, что для $i \in \{0, 1, \dots, n-1\}$ существует многочлен $H_i(\mathbf{x}) \in R[x_0, x_1]$ такой, что

$$\mathbf{x}^{2^i t} \equiv 1 + 2^{i+1} H_i(\mathbf{x}) \pmod{I}.$$

В частности, $\mathbf{x}^{2^{n-1} t} \equiv 1 \pmod{I}$. Следовательно,

$$2^{n-1} t = (2^{n-1} t_0, 2^{n-1} t_1) \in \mathfrak{P}(I).$$

Отсюда согласно пункту 1 леммы 1 следует равенство

$$S(F_0)^{2^{n-1} t_0} \otimes S(F_1)^{2^{n-1} t_1} = E. \quad (19)$$

Из соотношений (18) и (19) получаем цепочку равенств, выполняющуюся для всех $i \geq d$,

$$\begin{aligned} W(i + 2^{n-1} t) &= \vec{W}(0)(S(F_0)^{s_0(i+2^{n-1} t)} \otimes S(F_1)^{s_1(i+2^{n-1} t)})e^\downarrow \\ &= \vec{W}(0)(S(F_0)^{s_0(i)+2^{n-1} t_0} \otimes S(F_1)^{s_1(i)+2^{n-1} t_1})e^\downarrow \\ &= \vec{W}(0)(S(F_0)^{s_0(i)} \otimes S(F_1)^{s_1(i)})(S(F_0)^{2^{n-1} t_0} \otimes S(F_1)^{2^{n-1} t_1})e^\downarrow \\ &= \vec{W}(i)(S(F_0)^{2^{n-1} t_0} \otimes S(F_1)^{2^{n-1} t_1})e^\downarrow = \vec{W}(i)e^\downarrow = W(i). \end{aligned}$$

Отсюда, пользуясь неравенством $d + t \leq T(\bar{I})$, справедливым по определению величин d и t , получаем, что

$$D(W) + T(W) \leq d + 2^{n-1} t \leq 2^{n-1}(d + t) \leq 2^{n-1} T(\bar{I}). \quad (20)$$

Теорема доказана.

В следующем параграфе будет использовано следующее утверждение.

Предложение 1. Если в условиях теоремы 1 $n \geq 2$ и

$$T(W) = 2^{n-1} T(\bar{I}), \quad (21)$$

то векторы $\mathbf{s}(0), \mathbf{s}(1), \dots, \mathbf{s}(T(\bar{I}) - 1)$ попарно несравнимы по модулю $\mathfrak{P}(\bar{I})$ и

$$\mathbf{s}(0) \equiv \mathbf{s}(T(\bar{I})) \pmod{\mathfrak{P}(\bar{I})}. \quad (22)$$

Доказательство. Поскольку $n \geq 2$, из (21) и совокупности неравенств (20) следует, что $d = 0$ и $t = T(\bar{I})$. Тогда (15) влечет (22). Если же для некоторых $d' \geq 0$ и $t' > 0$ таких, что $d' + t' \leq T(\bar{I}) - 1$, векторы $\mathbf{s}(d')$ и $\mathbf{s}(d' + t')$ сравнимы по модулю $\mathfrak{P}(\bar{I})$, то, заменяя в (20) d на d' и t на t' , получаем, что

$$T(W) \leq 2^{n-1}(d' + t') \leq 2^{n-1}(T(\bar{I}) - 1) < 2^{n-1} T(\bar{I}),$$

что противоречит (21).

Предложение 1 доказано.

В [7] показано, что если $F_0(x_0)$ и $F_1(x_1)$ — многочлены Галуа, то

$$T(\bar{I}) = \frac{T(f_0)T(f_1)}{(T(f_0), T(f_1), q-1)}.$$

Отсюда и из теоремы 1 следует, что

$$D(W) + T(W) \leq 2^{n-1} \frac{T(f_0)T(f_1)}{(T(f_0), T(f_1), q-1)},$$

то есть справедлива оценка (4). В случае $q = 2$, то есть $R = \mathbf{Z}_{2^n}$, для произвольных реверсивных многочленов $F_0(x_0)$ и $F_1(x_1)$ справедливо равенство

$$T(\bar{I}) = T(f_0)T(f_1), \quad (23)$$

откуда

$$D(W) + T(W) \leq 2^{n-1} T(f_0)T(f_1) \leq 2^{n-1} (2^{m_0} - 1)(2^{m_1} - 1),$$

то есть верны неравенства (5).

3. Необходимые условия максимальности длины цикла в графе переходов состояний

Всюду далее будем рассматривать только случай $q = 2$, то есть $R = \mathbf{Z}_{2^n}$. Если не оговорено иное, то $n \geq 2$, $\deg f_0 = m_0 \geq 2$, $\deg f_1 = m_1 \geq 2$. В этом параграфе будут найдены условия, необходимые для того, чтобы выполнялось равенство (6).

Для чисел $a \in \mathbf{Z}$, $b \in \mathbf{N}$ обозначим через $\text{res}_b(a)$ остаток от деления a на b . Рассмотрим эпиморфизм абелевых групп $\xi: \mathbf{Z} \oplus \mathbf{Z} \rightarrow \mathbf{Z}_{T(f_0)} \oplus \mathbf{Z}_{T(f_1)}$, действующий по правилу

$$\xi(z_0, z_1) = (\text{res}_{T(f_0)}(z_0), \text{res}_{T(f_1)}(z_1)).$$

Для всех $i \geq 0$ обозначим через $\tilde{s}(i)$ упорядоченную пару $\xi(s(i))$, где вектор $s(i)$ определен соотношением (13). Назовем $\tilde{s}$ редуцированной последовательностью управляющих векторов.

Пусть $\text{Ker } \xi$ — ядро эпиморфизма ξ . Напомним, что $I = (F_0(x_0), F_1(x_1))$. Докажем ряд лемм о свойствах последовательности $\tilde{s}$.

Лемма 3. *Справедливо равенство $\text{Ker } \xi = \mathfrak{P}(\bar{I})$. Для любых $i, j \in \mathbf{N}_0$ следующие утверждения эквивалентны:*

$$(a) \quad \tilde{s}(i) = \tilde{s}(j);$$

$$(б) \quad s(i) - s(j) \in \mathfrak{P}(\bar{I}).$$

Доказательство. Достаточно обосновать равенство $\text{Ker } \xi = \mathfrak{P}(\bar{I})$. Ядро $\text{Ker } \xi$ эпиморфизма ξ порождено векторами $(T(f_0), 0)$ и $(0, T(f_1))$. Поэтому по лемме 1 справедливо включение $\text{Ker } \xi \subset \mathfrak{P}(\bar{I})$. Но тогда в силу (8) и (23)

$$[\mathbf{Z}^2 : \text{Ker } \xi] = T(f_0)T(f_1) = [\mathbf{Z}^2 : \mathfrak{P}(\bar{I})], \quad \text{Ker } \xi = \mathfrak{P}(\bar{I}).$$

Лемма доказана.

Лемма 4. Если для некоторых $d \geq 0$ и $t > 0$ последовательность (13) удовлетворяет условию $\tilde{s}(d+t) = \tilde{s}(d)$, то для всех $i \geq d$ верно равенство $\tilde{s}(i+t) = \tilde{s}(i)$. Другими словами,

$$D(\tilde{s}) + T(\tilde{s}) = \min\{l \in N : \tilde{s}(l) \in \{\tilde{s}(0), \dots, \tilde{s}(l-1)\}\},$$

где $D(\tilde{s})$ и $T(\tilde{s})$ — соответственно период и дефект последовательности $\tilde{s}$.

Доказательство. Индукцией по i так же, как при обосновании леммы 2, можно показать, что если $\tilde{s}(d+t) = \tilde{s}(d) \in \mathfrak{P}(\tilde{I})$, то для всех $i \geq d$ справедливо соотношение

$$\tilde{s}(i+t) - \tilde{s}(i) = \tilde{s}(d+t) - \tilde{s}(d) \in \mathfrak{P}(\tilde{I})$$

(отличие от леммы 2 состоит в том, что неравенство $d+t \leq T(\tilde{I})$ здесь может не выполняться). Для завершения доказательства осталось применить лемму 3.

Лемма доказана.

Лемма 5. Если последовательность состояний W автомата $\mathfrak{A}^\beta$ удовлетворяет условию (21), то редуцированная последовательность управляющих векторов $\tilde{s}$ реверсивна и $T(\tilde{s}) = T(f_0)T(f_1)$.

Доказательство. Согласно предложению 1 и лемме 3 $T(\tilde{s}) \geq T(\tilde{I})$ и $\tilde{s}(0) = \tilde{s}(T(\tilde{I}))$. Поэтому ввиду леммы 4 и равенства (23) справедливы соотношения

$$T(\tilde{s}) = T(\tilde{I}) = T(f_0)T(f_1), \quad D(\tilde{s}) = 0.$$

Лемма доказана.

Далее будут доказаны леммы, позволяющие получить основной результат этого параграфа, необходимые условия максимальности длины цикла в графе $\mathcal{G}(\mathfrak{A}^\beta)$.

Лемма 6. Если последовательность состояний W автомата $\mathfrak{A}^\beta$ удовлетворяет условию (21), то существует $j \in \{0, 1\}$ такое, что $T(F_j) = 2^{n-1}T(f_j)$.

Доказательство. Пусть вектор $\mathbf{t}$ определен соотношением (15). В силу леммы 3, $\mathbf{t} \in \mathfrak{P}(\tilde{I}) = \text{Ker } \xi$, откуда $\mathbf{t} = (a_0T(f_0), a_1T(f_1))$ для некоторых $a_0, a_1 \in \mathbf{Z}$. Согласно предложению 1 и равенству (23) число t из соотношения (15) равно $T(f_0)T(f_1)$. Пусть для всех $j \in \{0, 1\}$ число c_j определено равенством $T(F_j) = 2^{c_j}T(f_j)$ и $c = \max\{c_0, c_1\}$. Согласно (18) для всех $i \geq 0$

$$\mathbf{s}(i + 2^c T(f_0)T(f_1)) = \mathbf{s}(i + 2^c t) = \mathbf{s}(i) + 2^c \mathbf{t} = (s_0(i) + 2^c a_0 T(f_0), s_1(i) + 2^c a_1 T(f_1)).$$

Поэтому для всех $i \geq 0$ справедливы равенства

$$\begin{aligned} W(i + 2^c T(f_0)T(f_1)) &= \vec{W}(0)(S(F_0)^{s_0(i)+2^c a_0 T(f_0)} \otimes S(F_1)^{s_1(i)+2^c a_1 T(f_1)})e^\downarrow \\ &= \vec{W}(0)(S(F_0)^{s_0(i)} \otimes S(F_1)^{s_1(i)})e^\downarrow = \vec{W}(i)e^\downarrow = W(i). \end{aligned}$$

В силу равенства (23) отсюда следует, что

$$2^{n-1}T(f_0)T(f_1) = T(W) \mid 2^c T(f_0)T(f_1).$$

Следовательно, $c = n - 1$.

Лемма доказана.

При доказательстве леммы 6 показано, что соотношение (21) влечет равенство $t = T(f_0)T(f_1)$. Во всех последующих утверждениях этого параграфа равенство (21) предполагается выполненным, поэтому далее в этом параграфе вместо $T(f_0)T(f_1)$ будем писать t .

Введем обозначения

$$S(F_0)^T = U, \quad S(F_1) = V, \quad S(f_0)^T = \bar{U}, \quad S(f_1) = \bar{V}. \quad (24)$$

Тогда для каждого $i \geq 0$ справедливы равенства

$$W(i) = U^{s_0(i)} W(0) V^{s_1(i)}, \quad \bar{W}(i) = \bar{U}^{\tilde{s}_0(i)} \bar{W}(0) \bar{V}^{\tilde{s}_1(i)}, \quad (25)$$

где $\tilde{s}_0(i)$ и $\tilde{s}_1(i)$ суть соответственно первая и вторая компонента вектора $\tilde{s}(i)$.

Лемма 7. Если последовательность состояний W автомата $\mathfrak{A}^\beta$ удовлетворяет условию (21), то для индексующей функции β , определенной равенством (2), справедливы соотношения

$$\forall i \geq 0: \quad \beta(UW(i)) = \beta(W(i)V) = \beta(W(i+1)).$$

Доказательство. Поскольку $m_0 \geq 2$ и $m_1 \geq 2$, справедливы неравенства

$$T(f_0) \geq 2, \quad T(f_1) \geq 2. \quad (26)$$

Выберем и зафиксируем число $i \in \mathbf{N}_0$. Рассмотрим вектор $\tilde{s}(i)$. По лемме 5 последовательность $\tilde{s}$ реверсивна и справедливо равенство $T(\tilde{s}) = t = T(f_0)T(f_1)$. Согласно лемме 4, на цикле последовательности $\tilde{s}$ все элементы попарно различны. Поскольку $\tilde{s}$ есть последовательность над кольцом $S = \mathbf{Z}_{T(f_0)} \oplus \mathbf{Z}_{T(f_1)}$, на ее цикле встречается всякий вектор $(a, b) \in S$. Следовательно, существуют числа $i_1, i_2, i_3 \in \{0, 1, \dots, t-1\}$ такие, что

$$\tilde{s}(i_1) = \tilde{s}(i) + (1, 0), \quad \tilde{s}(i_2) = \tilde{s}(i) + (0, 1), \quad \tilde{s}(i_3) = \tilde{s}(i) + (1, 1), \quad (27)$$

где векторы складываются как элементы кольца S . Пусть $j = \text{res}_t(i_3 - 1)$. Тогда $i_3 \equiv j + 1 \pmod{t}$, и по лемме 5 справедлива цепочка равенств

$$\tilde{s}(i_3) = \tilde{s}(j+1) = \tilde{s}(j) + \xi(\alpha(W(j)), \beta(W(j))).$$

В силу (27)

$$\tilde{s}(j) = \tilde{s}(i) + (1, 1) - \xi(\alpha(W(j)), \beta(W(j))).$$

Поскольку $\xi(\alpha(W(j)), \beta(W(j))) \in \{(0, 1), (1, 0)\}$, выполняется одно из двух соотношений

$$\tilde{s}(j) = \tilde{s}(i) + (1, 0) = \tilde{s}(i_1), \quad \tilde{s}(j) = \tilde{s}(i) + (0, 1) = \tilde{s}(i_2).$$

По лемме 5 имеет место включение $\tilde{s}(i_3 - 1 + t) \in \{\tilde{s}(i_1), \tilde{s}(i_2)\}$. Тогда согласно леммам 4 и 5

$$\tilde{s}(i_3) \in \{\tilde{s}(i_1 + 1), \tilde{s}(i_2 + 1)\}. \quad (28)$$

Докажем, что

$$\beta(W(i_1)) = \beta(W(i_2)). \quad (29)$$

В противном случае возможны два варианта.

1. $\beta(W(i_1)) = 0$ и $\beta(W(i_2)) = 1$. Тогда в силу (26) и (27) справедливы соотношения

$$\begin{aligned}\tilde{s}(i_1 + 1) &= \tilde{s}(i_1) + \xi(\alpha(W(i_1)), \beta(W(i_1))) \\ &= \tilde{s}(i) + (1, 0) + (1, 0) \neq \tilde{s}(i) + (1, 1) = \tilde{s}(i_3),\end{aligned}$$

и при этом

$$\begin{aligned}\tilde{s}(i_2 + 1) &= \tilde{s}(i_2) + \xi(\alpha(W(i_2)), \beta(W(i_2))) \\ &= \tilde{s}(i) + (0, 1) + (0, 1) \neq \tilde{s}(i) + (1, 1) = \tilde{s}(i_3).\end{aligned}$$

Пришли к противоречию с (28).

2. $\beta(W(i_1)) = 1$ и $\beta(W(i_2)) = 0$. Тогда

$$\begin{aligned}\tilde{s}(i_1 + 1) &= \tilde{s}(i_1) + \xi(\alpha(W(i_1)), \beta(W(i_1))) = \tilde{s}(i) + (1, 1) = \tilde{s}(i_3), \\ \tilde{s}(i_2 + 1) &= \tilde{s}(i_2) + \xi(\alpha(W(i_2)), \beta(W(i_2))) = \tilde{s}(i) + (1, 1) = \tilde{s}(i_3).\end{aligned}$$

Отсюда $\tilde{s}(i_1 + 1) = \tilde{s}(i_2 + 1)$. В силу леммы 4 и леммы 5 справедлива цепочка соотношений

$$\tilde{s}(i_1) = \tilde{s}((i_1 + 1) + (t - 1)) = \tilde{s}((i_2 + 1) + (t - 1)) = \tilde{s}(i_2).$$

Поэтому в соответствии с теми же леммами для всех $z \geq 0$ выполняются равенства

$$\begin{aligned}\tilde{s}(z + \max\{i_1, i_2\} - \min\{i_1, i_2\}) &= \tilde{s}(\max\{i_1, i_2\} + t + z - \min\{i_1, i_2\}) \\ &= \tilde{s}(\min\{i_1, i_2\} + t + z - \min\{i_1, i_2\}) = \tilde{s}(z).\end{aligned}$$

В силу (26) $i_1 \neq i_2$. Поэтому величина $\Delta = \max\{i_1, i_2\} - \min\{i_1, i_2\}$ кратна t и удовлетворяет неравенствам $1 \leq \Delta \leq t - 1$. Пришли к противоречию.

Равенство (29) доказано. В силу (25) и (27)

$$\begin{aligned}\bar{W}(i_1) &= \bar{U}^{\tilde{s}_0(i)+1} \bar{W}(0) \bar{V}^{\tilde{s}_1(i)} = \bar{U} \bar{W}(i), \\ \bar{W}(i_2) &= \bar{U}^{\tilde{s}_0(i)} \bar{W}(0) \bar{V}^{\tilde{s}_1(i)+1} = \bar{W}(i) \bar{V}.\end{aligned}$$

Тогда согласно (29) справедлива цепочка равенств

$$\beta(U \cdot W(i)) = \beta(W(i_1)) = \beta(W(i_2)) = \beta(W(i)V).$$

Для завершения доказательства осталось заметить, что $W(i + 1) \in \{UW(i), W(i)V\}$. Лемма доказана.

Лемма 8. Если последовательность состояний W автомата $\mathcal{A}^B$ удовлетворяет условию (21), то

$$\forall i_0 \geq 0, i_1 \geq 0: \quad \beta(W(i_0 + i_1)) = \beta(U^{i_0}W(0) \cdot V^{i_1}).$$

Доказательство. Индукцией по $i_0 \geq 0$ докажем равенство

$$\beta(U^{i_0}W(0)V^{i_1}) = \beta(W(0)V^{i_0+i_1}). \quad (30)$$

В случае $i_0 = 0$ равенство очевидно. Пусть $j \geq 0$, и равенство верно для всех $i_0 \leq j$. Докажем его для $i_0 = j + 1$. Как уже отмечалось при доказательстве леммы 7, из соотношения (21) следует, что на цикле последовательности $\tilde{s}$ встречаются все элементы кольца $S = \mathbf{Z}_{T(f_0)} \oplus \mathbf{Z}_{T(f_1)}$. В частности, существует $i \in \{0, 1, \dots, t - 1\}$ такое, что

$$\tilde{s}(i) = (\text{res}_{T(f_0)}(i_0 - 1), \text{res}_{T(f_1)}(i_1)).$$

Согласно (25) выполняется равенство

$$\bar{W}(i) = \bar{U}^{i_0-1} \bar{W}(0) \bar{V}^{i_1}.$$

В силу леммы 7 и предположения индукции отсюда следует, что

$$\begin{aligned} \beta(U^{i_0} W(0) V^{i_1}) &= \beta(U W(i)) = \beta(W(i) V) = \beta(U^j W(0) V^{i_1+1}) \\ &= \beta(W(0) V^{i_1+1+j}) = \beta(W(0) V^{i_0+i_1}). \end{aligned}$$

Таким образом, равенство (30) доказано.

Пусть $i_0 \geq 0, i_1 \geq 0, j_0 = s_0(i_0 + i_1), j_1 = s_1(i_0 + i_1)$. Тогда по определению функций α, β и последовательности $\mathbf{s}$, а также в силу (25)

$$i_0 + i_1 = j_0 + j_1, \quad W(i_0 + i_1) = U^{j_0} W(0) V^{j_1}. \quad (31)$$

Применив доказанное равенство (30) с заменой i_0 на j_0, i_1 на j_1 и учитывая (31), получим, что

$$\beta(W(0) V^{i_0+i_1}) = \beta(W(0) V^{j_0+j_1}) = \beta(U^{j_0} W(0) V^{j_1}) = \beta(W(i_0 + i_1)).$$

Отсюда и из равенства (30) следует доказываемое утверждение.

Лемма доказана.

Обозначим через δ последовательность над $\mathbf{Z}_2$ со знаками

$$\delta(i) = \beta(W(i)) = \bar{w}_{1,1}(i), \quad i \in \mathbf{N}_0, \quad (32)$$

где $w_{1,1}(i)$ есть элемент, стоящий в первой строке и первом столбце матрицы $W(i)$. Назовем последовательность δ управляющей. Справедливо следующее утверждение.

Лемма 9. Если последовательность состояний W автомата $\mathcal{A}^\beta$ удовлетворяет условию (21), то $\bar{U} \bar{W}(0) = \bar{W}(0) \bar{V}$, а управляющая последовательность δ есть ненулевая последовательность из семейства линейных рекуррент $L_{\mathbf{Z}_2}(d(x))$, где $d(x) = (f_0(x), f_1(x))$.

Доказательство. Рассмотрим 2-ЛРП $\mu \in L_{\mathbf{Z}_2}(f_0(x_0), f_1(x_1))$, определенную равенством

$$\forall \mathbf{z} = (z_0, z_1) \in \mathbf{N}_0^2: \quad \mu(\mathbf{z}) = \beta(U^{z_0} W(0) V^{z_1}). \quad (33)$$

То, что $f_0(x_0)$ и $f_1(x_1)$ суть элементарные характеристические многочлены μ , следует из определения отображения β и равенств (24).

Пусть $\Pi = \{0, 1, m_0 - 1\} \times \{0, 1, m_1 - 1\}$. Тогда

$$\mu[\Pi] = \bar{W}(0), \quad x_0 \mu[\Pi] = \bar{U} \bar{W}(0), \quad x_1 \mu[\Pi] = \bar{W}(0) \bar{V}. \quad (34)$$

Согласно лемме 8 для всех $\mathbf{z} \in \mathbf{N}_0^2$ имеет место цепочка соотношений

$$\begin{aligned} x_0 \mu(\mathbf{z}) &= \beta(U^{z_0+1} W(0) V^{z_1}) = \beta(W(z_0 + z_1 + 1)) \\ &= \beta(U^{z_0} W(0) V^{z_1+1}) = x_1 \mu(\mathbf{z}). \end{aligned}$$

Отсюда и из равенств (34) вытекает соотношение $\bar{U} \bar{W}(0) = \bar{W}(0) \bar{V}$.

Если последовательность δ нулевая, то, принимая во внимание (26), получаем, что

$$T(W) \mid T(F_0) \mid 2^{n-1} T(f_0) < 2^{n-1} T(f_0) T(f_1) = 2^{n-1} T(\bar{I}).$$

Следовательно, управляющая последовательность δ ненулевая.

В силу леммы 8

$$\forall \mathbf{z} = (z_0, z_1) \in \mathbf{N}_0^2: \quad \mu(\mathbf{z}) = \beta(U^{z_0}W(0)V^{z_1}) = \beta(W(z_0 + z_1)) = \delta(z_0 + z_1).$$

Следовательно, в 2-ЛРП μ первая строка $(\mu(0, 0), \mu(0, 1), \mu(0, 2), \dots)$ и первый столбец $(\mu(0, 0), \mu(1, 0), \mu(2, 0), \dots)^T$ совпадают с последовательностью δ . Поэтому

$$\delta \in L_{\mathbf{Z}_2}(f_0(x)) \cap L_{\mathbf{Z}_2}(f_1(x)) = L_{\mathbf{Z}_2}(d(x)).$$

Лемма доказана.

Унитарный многочлен $F(x) \in R[x]$ будем называть многочленом полного периода (см. [5]), если $T(F) = 2^{n-1}T(\bar{F})$. Необходимые условия максимальности длины цикла в графе переходов состояний простейшего самоуправляемого 2-ЛРС дает следующая теорема.

Теорема 2. Пусть $T(W) = 2^{n-1}T(\bar{I})$. Тогда справедливы следующие утверждения.

- (1) Хотя бы один из многочленов $F_0(x_0)$ и $F_1(x_1)$ есть многочлен полного периода.
- (2) Многочлены $\bar{F}_0(x)$ и $\bar{F}_1(x)$ не взаимно просты.
- (3) $\bar{W}(0) \neq 0$, и верно равенство $S(\bar{F}_0)^T \bar{W}(0) = \bar{W}(0)S(\bar{F}_1)$.
- (4) $S(F_0)^T W(0) \neq W(0)S(F_1)$.

Доказательство. Пункт 1 вытекает из леммы 6.

По лемме 9 в множестве $L_{\mathbf{Z}_2}(d(x))$ лежит ненулевая последовательность, поэтому $d(x) = (f_0(x), f_1(x)) \neq 1$, и справедлив пункт 2.

Пусть 2-ЛРП $\mu \in L_{\mathbf{Z}_2}(f_0, f_1)$ определена равенством (33). Поскольку

$$\forall (z_0, z_1) \in \mathbf{N}_0^2: \quad \mu(z_0, z_1) = \delta(z_0 + z_1),$$

и $\text{rank}(\delta) \leq \deg d(x) \leq \min\{m_0, m_1\}$, соотношение $\bar{W}(0) = 0$ влечет равенства $\mu[\Pi] = 0$ и $\delta = 0$. Согласно лемме 9 последовательность δ ненулевая. Поэтому $\bar{W}(0) \neq 0$. Равенство $S(f_0)^T \bar{W}(0) = \bar{W}(0)S(f_1)$ следует из леммы 9. Пункт 3 доказан.

Равенство $S(F_0)^T W(0) = W(0)S(F_1)$ влечет соотношение

$$\forall i \geq 0: \quad W(i) = W(0) \cdot S(F_1)^i,$$

откуда с учетом (26) получаем, что

$$T(W) \mid 2^{n-1}T(f_1) < 2^{n-1}T(f_0)T(f_1) = 2^{n-1}T(\bar{I}).$$

Пришли к противоречию с условием, поэтому справедлив пункт 4.

Теорема доказана.

Следствие 1. Если выполняется равенство (6): $T(W) = 2^{n-1}(2^{m_0} - 1)(2^{m_1} - 1)$, то справедливы следующие утверждения.

- (1) Хотя бы один из многочленов $F_0(x_0)$ и $F_1(x_1)$ есть многочлен максимального периода.
- (2) $\bar{F}_0(x) = \bar{F}_1(x)$.
- (3) $\bar{W}(0) \neq 0$, и верно равенство $S(\bar{F}_0)^T \bar{W}(0) = \bar{W}(0)S(\bar{F}_1)$.
- (4) $S(F_0)^T W(0) \neq W(0)S(F_1)$.

4. Критерий максимальности длины цикла и основные состояния

Всюду далее будем рассматривать регистр $\mathfrak{A}^\beta$, у которого $F_0(x) = F_1(x) = F(x)$ — многочлен максимального периода степени $m \geq 2$. В этой ситуации равенство (6) влечет соотношения (7).

В этом параграфе будут изучаться условия на матрицу $W(0)$ со свойствами (7), достаточные для выполнения равенства (6). Рассмотрим свойства управляющей последовательности δ , определенной соотношением (32).

Лемма 10. Пусть для матрицы $W(0)$ выполняются условия (7). Тогда управляющая последовательность δ есть ЛРП максимального периода ранга m над полем $\mathbf{Z}_2$ с характеристическим многочленом $f(x) = \bar{F}(x)$.

Доказательство. Пусть μ есть 2-ЛРП, определенная равенством (33). По условию

$$\bar{U} \bar{W}(0) = \bar{W}(0) \bar{V}. \quad (35)$$

Поэтому для любых пар $\mathbf{z} = (z_0, z_1)$, $\mathbf{z}' = (z'_0, z'_1) \in \mathbf{N}_0^2$ таких, что $z_0 + z_1 = z'_0 + z'_1$, справедлива цепочка равенств

$$\begin{aligned} \mu(\mathbf{z}) &= \beta(U^{z_0} W(0) V^{z_1}) = \beta(W(0) V^{z_0+z_1}) \\ &= \beta(W(0) V^{z'_0+z'_1}) = \beta(U^{z'_0} W(0) V^{z'_1}) = \mu(\mathbf{z}'). \end{aligned} \quad (36)$$

Отсюда, пользуясь определением (13) последовательностей s_0 и s_1 , получаем, в частности, что

$$\begin{aligned} \forall \mathbf{z} = (z_0, z_1) \in \mathbf{N}_0^2: \quad \mu(z_0, z_1) &= \mu(s_0(z_0 + z_1), s_1(z_0 + z_1)) \\ &= \beta(U^{s_0(z_0+z_1)} W(0) V^{s_1(z_0+z_1)}) \\ &= \beta(W(z_0 + z_1)) = \delta(z_0 + z_1). \end{aligned}$$

Если последовательность δ нулевая, и $\Pi = \{0, 1, \dots, m-1\} \times \{0, 1, \dots, m-1\}$, то $\bar{W}(0) = \mu[\Pi] = 0$, что противоречит условию леммы. Первая строка $(\mu(0, 0), \mu(0, 1), \mu(0, 2), \dots)$ 2-ЛРП μ , с одной стороны, совпадает с последовательностью δ , а с другой стороны, есть ЛРП с характеристическим многочленом $f(x)$. Поскольку $f(x)$ — многочлен максимального периода степени m и $\delta \neq 0$, последовательность δ есть ЛРП максимального периода ранга m над полем $\mathbf{Z}_2$.

Лемма доказана.

Пусть φ — произвольное биективное преобразование некоторого конечного множества, a — элемент этого множества. Обозначим через $T_\varphi(a)$ длину того цикла преобразования φ , на котором лежит элемент a . Для всех $i \geq 1$ через φ^i будем обозначать i -кратную композицию $\varphi \circ \varphi \circ \dots \circ \varphi$. По определению φ^0 есть тождественное преобразование.

Рассмотрим автоморфизм σ модуля ${}_R M$, определенный равенством

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

где $\tau = T(f) = 2^m - 1$.

Лемма 11. Пусть для матрицы $W(0)$ выполняются условия (7). Тогда последовательность W реверсивна и справедливо равенство $T(W) = T_\sigma(W(0))\tau$.

Доказательство. Согласно лемме 10 управляющая последовательность δ есть ЛРП максимального периода $\tau = 2^m - 1$. Будем рассматривать знаки 0 и 1 последовательности δ как целые числа. Тогда, поскольку $U^{2^{n-1}\tau} = V^{2^{n-1}\tau} = E$, для каждого $i \geq 0$ имеет место цепочка равенств

$$\begin{aligned} W(i + 2^{n-1}\tau^2) &= U^{\sum_{k=i}^{i+2^{n-1}\tau^2-1} (1-\delta(k))} W(i) V^{\sum_{k=i}^{i+2^{n-1}\tau^2-1} \delta(k)} \\ &= U^{2^{n-1}\tau \sum_{k=i}^{i+\tau-1} (1-\delta(k))} W(i) V^{2^{n-1}\tau \sum_{k=i}^{i+\tau-1} \delta(k)} = W(i). \end{aligned}$$

Таким образом, последовательность W реверсивна, и ее период $t = T(W)$ делит величину $2^{n-1}\tau^2$.

Для всех $i \geq 0$ выполняется соотношение $W(i+t) = W(i)$ и, следовательно, справедливо равенство

$$U^{s_0(i+t)} W(0) V^{s_1(i+t)} = U^{s_0(i)} W(0) \cdot V^{s_1(i)}.$$

Умножая обе части этого соотношения слева на матрицу $U^{-s_0(i)}$ и справа на матрицу $V^{-s_1(i)}$, получаем, что

$$U^{s_0(i+t)-s_0(i)} W(0) V^{s_1(i+t)-s_1(i)} = W(0).$$

Положим

$$\Delta(i) = s_0(i+t) - s_0(i) = \sum_{k=i}^{i+t-1} (1 - \delta(k)).$$

Тогда для всех $i \geq 0$ выполняется соотношение

$$U^{\Delta(i)} W(0) V^{-\Delta(i)} V^t = W(0). \quad (37)$$

Переписав равенство (37) с заменой i на $i+1$, получим, что

$$U^{\Delta(i+1)} W(0) V^{-\Delta(i+1)} V^t = W(0). \quad (38)$$

Покажем, что $\tau \mid t$. Проведем доказательство от противного, предположим, что $\tau \nmid t$. Тогда многочлен $x^t \oplus 1$ взаимно прост с минимальным многочленом ЛРП δ , и следовательно, $(x^t \oplus 1)\delta$ есть ЛРП максимального периода τ над $\mathbf{Z}_2$. Поскольку $(x^t \oplus 1)\delta \neq \delta$, существует i такое, что $\delta(i) = 0$, а $((x^t \oplus 1)\delta)(i) = 1$, то есть $\delta(i+t) = 1$. Тогда справедлива цепочка соотношений

$$\Delta(i+1) = \Delta(i) - (1 - \delta(i)) + (1 - \delta(i+t)) = \Delta(i) - \delta(i+t) + \delta(i) = \Delta(i) - 1.$$

Из равенства (38) следует, что

$$U^{-1}(U^{\Delta(i)} W(0) V^{-\Delta(i)} V^t) V = W(0),$$

то есть, с учетом (37), $U^{-1}W(0)V = W(0)$. Это противоречит условиям (7).

Таким образом, $t = l\tau$, где l является наименьшим положительным решением системы

$$W(i + l\tau) = W(i), \quad i \in \{0, 1, \dots, 1, 2^{n-1}\tau^2 - 1\}. \quad (39)$$

На цикле ЛРП δ лежит $(\tau - 1)/2$ нулей и $(\tau + 1)/2$ единиц. По определению последовательности W система (39) равносильна системе

$$U^{(\tau-1)/l/2} W(i) V^{(\tau+1)l/2} = W(i), \quad i \in \{0, 1, \dots, 2^{n-1}\tau^2 - 1\},$$

а она, в свою очередь, равносильна уравнению

$$U^{(\tau-1)/l/2} W(0) V^{(\tau+1)/l/2} = W(0).$$

Поэтому наименьшее положительное решение системы (39) равно $T_\sigma(W(0))$. Следовательно, $T(W) = t = T_\sigma(W(0))\tau$.

Лемма доказана.

Чтобы описать основные состояния регистра $\mathcal{A}^\beta$, осталось выяснить, для каких матриц $W(0) \in M$ выполняется равенство

$$T_\sigma(W(0)) = 2^{n-1} \cdot \tau.$$

С этой целью исследуем характеристический многочлен $\chi_\sigma(x)$ автоморфизма σ . Поскольку (в обозначениях раздела 2)

$$\forall X \in M: \quad \sigma(X) = \vec{X}(S(F)^{(\tau-1)/2} \otimes S(F)^{(\tau+1)/2})e^\downarrow,$$

многочлен $\chi_\sigma(x)$ совпадает с характеристическим многочленом матрицы

$$A = S(F)^{(\tau-1)/2} \otimes S(F)^{(\tau+1)/2}. \quad (40)$$

Пусть ϑ — некоторый корень многочлена $f(x)$ в поле $GF(2^m)$, $w = \vartheta^{(\tau-1)/2}$. Для каждого $l \in \{1, \dots, m-1\}$ обозначим через $\mu_{w^{2^l-1}}(x)$ минимальный многочлен элемента w^{2^l-1} над полем $\mathbf{Z}_2$. Докажем, что все многочлены $\mu_{w^{2^l-1}}(x)$ имеют степень m . Для этого используем следующий факт, известный в теории чисел как теорема Гжегорчика (см. теорему 1 на с. 102 в [6]).

Теорема 3. 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 см., например, в [14].

Следствие 2. Если $m \geq 2$, $d \mid m$, $d < m$, то минимальное натуральное s , удовлетворяющее соотношению

$$\frac{2^m - 1}{2^d - 1} \mid 2^s - 1,$$

равно m .

Доказательство. В случае $m = 6$ в справедливости сформулированного утверждения можно убедиться непосредственной проверкой. При $m \neq 6$ по теореме 3 существует простое p такое, что $p \mid 2^m - 1$, и $p \nmid 2^k - 1$ для всех $k \in \{1, \dots, m-1\}$. Тогда $p \nmid 2^d - 1$, и имеет место цепочка соотношений

$$p \mid \frac{2^m - 1}{2^d - 1} \mid 2^s - 1.$$

Отсюда $s \geq m$.

Следствие доказано.

Следствие 3. Для каждого $l \in \{1, \dots, m-1\}$ справедливо равенство

$$\deg \mu_{w^{2^l-1}}(x) = m.$$

Доказательство. Обозначим через $\text{ord } w$ порядок элемента $w \in GF(2^m)^*$. Ясно, что

$$\text{ord } w = \text{ord } \vartheta^{(\tau-1)/2} = \frac{\tau}{((\tau-1)/2, \tau)} = \tau = 2^m - 1.$$

Поскольку $w^{2^l-1} \in GF(2^m)$, справедливо неравенство $\deg \mu_{w^{2^l-1}}(x) \leq m$. Если $\deg \mu_{w^{2^l-1}}(x) = s$, то $w^{2^l-1} \in GF(2^s)^*$, и справедлива цепочка соотношений

$$\frac{2^m - 1}{2^{(m,l)} - 1} = \text{ord } w^{2^l-1} \mid |GF(2^s)^*| = 2^s - 1.$$

Поэтому согласно следствию 2 справедливо неравенство $s \geq m$.

Следствие доказано.

Напомним, что многочлен над конечным полем называется сепарабельным, если он не имеет кратных корней в своем поле разложения. Строение образа $\bar{\chi}_\sigma$ характеристического многочлена $\chi_\sigma(x)$ под действием естественного эпиморфизма $R \rightarrow \bar{R}$ описывает следующая лемма.

Лемма 12. *Во введенных обозначениях*

(1) *многочлен $\bar{\chi}_\sigma$ представляется в виде*

$$\bar{\chi}_\sigma(x) = (x-1)^m g(x),$$

(2) *многочлен $g(x)$ сепарабелен, он представляется в виде*

$$g(x) = \prod_{l=1}^{m-1} \mu_{w^{2^l-1}}(x).$$

Доказательство. Докажем утверждение 1. Согласно [2], все корни многочлена $f(x)$ в поле $GF(2^m)$ суть $\vartheta, \vartheta^2, \vartheta^{2^2}, \dots, \vartheta^{2^{m-1}}$. Положим $\alpha_i = \vartheta^{2^i}$, $i \in \{0, 1, \dots, m-1\}$. Тогда, обозначая знаком $\approx$ отношение подобия матриц, получаем, что

$$\bar{A} \approx \text{diag}(1, 1, \dots, 1, \dots, \alpha_i^{(\tau-1)/2} \alpha_j^{(\tau+1)/2}, \dots). \quad (41)$$

На диагонали матрицы, стоящей в правой части соотношения (41), находятся m единиц, они соответствуют произведениям $\alpha_i^{(\tau-1)/2} \alpha_j^{(\tau+1)/2} = \alpha_i^\tau = \vartheta^{2^i \tau}$, а пара (i, j) пробегает все значения из множества $\Pi = \{0, 1, \dots, m-1\} \times \{0, 1, \dots, m-1\}$ такие, что $i \neq j$. Поэтому

$$\bar{\chi}_\sigma(x) = (x-1)^m g(x),$$

где

$$g(x) = \prod_{(i,j): i \neq j} (x - \alpha_i^{(\tau-1)/2} \alpha_j^{(\tau+1)/2}). \quad (42)$$

Докажем утверждение 2. Сначала докажем, что если $1 \leq i < j \leq m-1$, то

$$\mu_{w^{2^i-1}}(x) \neq \mu_{w^{2^j-1}}(x). \quad (43)$$

Действительно, в противном случае существует $k \in \{0, 1, \dots, m-1\}$ такое, что $w^{2^i-2^0} = w^{2^k(2^j-1)}$. Пусть $l = \text{res}_m(k+j)$. Тогда

$$w^{2^i-2^0} = w^{2^l-2^k}, \quad 2^i - 2^0 = 2^l - 2^k, \quad 2^i + 2^k = 2^l + 2^0,$$

и, поскольку $i \neq 0, l \neq k$, справедливо равенство $(i, k) = (l, 0)$. Отсюда $k = 0, i = j$. Пришли к противоречию. Соотношение (43) доказано.

Рассмотрим многочлен $g(x)$, определенный равенством (42). Если пара $(i, j) \in \Pi$ такова, что $i \neq j$, то $\alpha_i^{(\tau-1)/2} \alpha_j^{(\tau+1)/2} = \vartheta^{(\tau-1)(2^i-2^j)/2} = w^{2^i-2^j}$. В частности, для любых $j \in \{0, 1, \dots, m-1\}, l \in \{1, \dots, m-1\}$ элемент $w^{2^j(2^l-1)}$ является корнем многочлена $g(x)$. Учитывая следствие 3, получаем, что

$$\forall l \in \{1, \dots, m-1\}: \quad \mu_{w^{2^l-1}}(x) = \prod_{j=0}^{m-1} (x - w^{2^j(2^l-1)}) \mid g(x).$$

Согласно (43) многочлены $\mu_{w^{2^l-1}}(x), 1 \leq l \leq m-1$, попарно взаимно просты. Поэтому

$$\prod_{l=1}^{m-1} \mu_{w^{2^l-1}}(x) \mid g(x). \quad (44)$$

По следствию 3 степень левой части соотношения (44) равна $m(m-1)$. В силу (42) степень многочлена $g(x)$ также равна $m(m-1)$. Поэтому ввиду унитарности $g(x)$ из соотношения (44) следует, что

$$g(x) = \prod_{l=1}^{m-1} \mu_{w^{2^l-1}}(x).$$

Отсюда и из (43) получаем, что многочлен $g(x)$ сепарабелен.

Лемма доказана.

Для дальнейшего исследования многочлена $\chi_\sigma(x)$ потребуется следующий факт (лемма Гензеля, [3])

Теорема 4. Пусть R — кольцо Галуа, многочлен $A(x) \in R[x]$ унитарный и существуют унитарные многочлены $b(x), c(x) \in \bar{R}[x]$ такие, что

$$\bar{A}(x) = b(x)c(x), \quad (b(x), c(x)) = 1.$$

Тогда существует единственная пара унитарных многочленов $B(x), C(x) \in R[x]$ таких, что

$$A(x) = B(x)C(x), \quad \bar{B}(x) = b(x), \quad \bar{C}(x) = c(x).$$

Напомним [2], что многочлены $B(x)$ и $C(x)$ над кольцом $R = \mathbf{Z}_{2^n}$ называются взаимно простыми, если $(B(x), C(x)) = (1)$, что эквивалентно взаимной простоте многочленов $b(x) = \bar{B}(x)$ и $c(x) = \bar{C}(x)$ (см., например, [13]).

Лемма 13. Существуют попарно взаимно простые унитарные многочлены степени m $G_0(x), G_1(x), G_2(x), \dots, G_{m-1}(x) \in \mathbf{Z}_{2^n}[x]$ такие, что $\bar{G}_0(x) = (x-1)^m$, для каждого $l \in \{1, \dots, m-1\}$ выполняется равенство

$$\bar{G}_l(x) = \mu_{w^{2^l-1}}(x),$$

и справедливо соотношение

$$\chi_\sigma(x) = \prod_{l=0}^{m-1} G_l(x). \quad (45)$$

Доказательство. Поскольку $m \geq 2$, согласно следствию 3 и пункту 2 леммы 12 многочлен $g(x)$, определенный в пункте 1 леммы 12, не имеет корней в поле $\mathbf{Z}_2$. В частности, многочлены $g(x)$ и $(x-1)^m$ взаимно просты. Попарная взаимная простота многочленов

$$\mu_w(x), \mu_{w^{2^2-1}}(x), \dots, \mu_{w^{2^m-1-1}}(x) \quad (46)$$

следует из пункта 2 леммы 12. Учитывая лемму 12, применим к многочлену $\chi_\sigma(x)$, многочлену $(x-1)^m$ и семейству многочленов (46) теорему 4. В результате получим равенство (45).

Лемма доказана.

Напомним (см. (24)), что $U = S(F)^T$, $V = S(F)$. Опишем матрицы $X \in M$ такие, что

$$UX = XV \quad (47)$$

и найдем их число.

Лемма 14. Пусть $R = \mathbf{Z}_{2^n}$, $n \geq 1$. Тогда справедливы следующие утверждения.

- (1) Если 2-ЛРП $\mu \in L_R(F(x_0), F(x_1))$ такова, что матрица $X = \mu[\Pi]$ обладает свойством (47), то существует единственная рекуррента $u \in L_R(F)$, для которой выполняется равенство

$$\forall \mathbf{z} = (z_0, z_1) \in \mathbf{N}_0^2: \quad \mu(\mathbf{z}) = u(z_0 + z_1). \quad (48)$$

Обратно, если $u \in L_R(F)$ и 2-ЛРП μ определена соотношением (48), то матрица $X = \mu[\Pi]$ обладает свойством (47). Таким образом, существует взаимно однозначное соответствие между рекуррентами $u \in L_R(F)$ и матрицами $X \in M$, обладающими свойством (47). Это соответствие имеет вид

$$u \mapsto \begin{pmatrix} u(0) & u(1) & \dots & u(m-1) \\ u(1) & u(2) & \dots & u(m) \\ \dots & \dots & \dots & \dots \\ u(m-1) & u(m) & \dots & u(2m-2) \end{pmatrix}. \quad (49)$$

- (2) Число матриц $X \in M$, обладающих свойством (47) равно 2^{nm} .

Доказательство. Рассмотрим 2-ЛРП $\mu \in L_R(F(x_0), F(x_1))$ такую, что матрица $X = \mu[\Pi]$ обладает свойством (47). Тогда

$$\forall \mathbf{z} = (z_0, z_1) \in \mathbf{N}_0^2: \quad \mu(\mathbf{z}) = \vec{E}_1 U^{z_0} X V^{z_1} E_1^\downarrow = \vec{E}_1 X V^{z_0+z_1} E_1^\downarrow,$$

где $\vec{E}_1$ — вектор-строка длины m вида $(1, 0, \dots, 0)$, а $E_1^\downarrow$ — вектор-столбец длины m вида $(1, 0, \dots, 0)^T$. Следовательно, для ЛРП $u \in L_R(F)$, начальный вектор которой совпадает с первой строкой матрицы X , выполняется равенство (48). Очевидно, что построенная

рекуррента u — единственная ЛРП из семейства $L_R(F)$, для которой выполняется равенство (48). Разным матрицам X , обладающим свойством (47), соответствуют разные $\mu \in L_R(F(x_0), F(x_1))$, а значит, разные рекурренты $u \in L_R(F)$. Следовательно, построено инъективное отображение из множества матриц X , обладающих свойством (47), в $L_R(F)$.

Обратно, пусть $u \in L_R(F)$, 2-ЛРП μ определена равенством (48), и $X = \mu[\Pi]$. Тогда очевидно включение $\mu \in L_R(F(x_0), F(x_1))$, и для любых $z_0 \geq 0$, $z_1 \geq 0$ справедлива цепочка равенств

$$x_0\mu(z_0, z_1) = \mu(z_0 + 1, z_1) = u(z_0 + z_1 + 1) = \mu(z_0, z_1 + 1) = x_1\mu(z_0, z_1).$$

Отсюда следует, что $UX = x_0\mu[\Pi] = x_1\mu[\Pi] = XV$, то есть матрица X обладает свойством (47). Таким образом, построено взаимно однозначное соответствие между матрицами, обладающими свойством (47), и рекуррентами из семейства $L_R(F)$. Это соответствие имеет вид (49). Пункт 1 доказан.

Пункт 2 следует из пункта 1.

Лемма доказана.

Далее будет сформулирован и доказан ряд лемм, позволяющих описать те циклы в графе линейного преобразования σ , на которых лежат начальные состояния $W(0)$, обладающие свойствами (7).

Лемма 15. В обозначениях леммы 13 матрица A , определенная равенством (40), подобна квазидиагональной (распавшейся) матрице

$$A \approx \text{diag}(A_0, S(G_1), S(G_2), \dots, S(G_{m-1})),$$

где матрица $A_0 \in R_{m \times m}^*$ имеет характеристический многочлен $G_0(x)$.

Доказательство. Из леммы 13 и теоремы 2 раздела 1 в [9] вытекает, что матрица A подобна квазидиагональной матрице $A \approx \text{diag}(A_0, A_1, A_2, \dots, A_{m-1})$, где для всякого $l \in \{0, 1, \dots, m-1\}$ матрица $A_l \in R_{m \times m}^*$ имеет характеристический многочлен $G_l(x)$. По лемме 13, многочлены $G_1(x), G_2(x), \dots, G_{m-1}(x)$ суть многочлены Галуа. Согласно [9], многочлен Галуа является сильным инвариантом подобия, то есть если две матрицы $P, Q \in R_{m \times m}$ аннулируются одним и тем же унитарным многочленом $G(x)$ и $G(x)$ есть многочлен Галуа, то условие $P \approx Q$ эквивалентно условию $\bar{P} \approx \bar{Q}$. Поэтому $A_l \approx S(G_l)$ для любого $l \in \{1, \dots, m-1\}$.

Лемма доказана.

Для дальнейшего изложения 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 вектор-строк длины k над R , если определить умножение $G(x) \in R[x]$ на $\gamma \in R^k$ по правилу

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

Следуя [1], будем называть $M(X)$ модулем, ассоциированным с матрицей X . Кроме того, зададим автоморфизм $\bar{\sigma} \in \text{Aut}(\bar{R}_{m \times m})$, полагая

$$\forall X \in M: \quad \bar{\sigma}(\bar{X}) = \overline{\sigma(X)}.$$

В основе всех дальнейших результатов о периодических свойствах регистра $\mathfrak{U}^\beta$ лежит разложение модуля M квадратных матриц над R , о котором идет речь в следующей лемме.

Лемма 16. Пусть $R = \mathbf{Z}_{2^n}$, $n \geq 1$. Справедливы следующие утверждения.

(1) Модуль ${}_R M$ раскладывается в прямую сумму ядер эндоморфизмов:

$${}_R M = \text{Ker } G_0(\sigma) \dot{+} \text{Ker } G_1(\sigma) \dot{+} \dots \dot{+} \text{Ker } G_{m-1}(\sigma), \quad (50)$$

причем $|\text{Ker } G_l(\sigma)| = 2^{nm}$ для всех $l \in \{0, 1, \dots, m-1\}$.

(2) Для любого $l \in \{0, 1, \dots, m-1\}$ верно равенство $\text{Ker } \bar{G}_l(\bar{\sigma}) = \overline{\text{Ker } G_l(\sigma)}$.

Доказательство. Докажем первое утверждение. Справедливость разложения (50) следует из леммы 13. Согласно лемме 15 и теореме 1 раздела 1 в [9] существует изоморфизм ζ левых $R[x]$ -модулей

$$\zeta: M(A) \rightarrow M' = M(A_0) \oplus M(S(G_1)) \oplus \dots \oplus M(S(G_{m-1})). \quad (51)$$

Введем обозначения

$$M_0 = M(A_0) \oplus \{0\} \oplus \dots \oplus \{0\} < M',$$

$$\forall l \in \{1, \dots, m-1\}: M_l = \{0\} \oplus \dots \oplus \{0\} \oplus M(S(G_l)) \oplus \{0\} \oplus \dots \oplus \{0\} < M',$$

где модуль $M(S(G_l))$ стоит на $(l+1)$ -м месте. Тогда

$$M' = M_0 \dot{+} M_1 \dot{+} \dots \dot{+} M_{m-1}.$$

Выберем и зафиксируем $l \in \{0, 1, \dots, m-1\}$. Пусть $\gamma = (\gamma_0, \gamma_1, \dots, \gamma_{m-1}) \in M'$. Справедливо равенство

$$G_l(x) \circ \gamma = (\gamma_0 G_l(A_0), \gamma_1 G_l(S(G_1)), \dots, \gamma_{m-1} G_l(S(G_{m-1}))).$$

Если характеристический многочлен матрицы X взаимно прост с $G_l(x)$, то матрица $G_l(X)$ обратима. Если характеристический многочлен матрицы X равен $G_l(x)$, то матрица $G_l(X)$ нулевая. Поэтому многочлен $G_l(x)$ аннулирует те и только те векторы $\gamma \in M'$, которые принадлежат подмодулю M_l . Учитывая (51), получаем, что $G_l(x)$ аннулирует те и только те векторы из $M(A)$, которые принадлежат подмодулю $\zeta^{-1}(M_l)$. Следовательно, справедлива цепочка равенств

$$\forall l \in \{0, 1, \dots, m-1\}: |M_l| = |\zeta^{-1}(M_l)| = |\text{Ker } G_l(\sigma)|. \quad (52)$$

Согласно лемме 13 и определению модуля, ассоциированного с матрицей, получаем, что для каждого $l \in \{1, \dots, m-1\}$ верны соотношения

$$|M_l| = |M(S(G_l))| = |R|^{\deg G_l} = 2^{nm}.$$

Поэтому

$$|M_0| = |R|^{m^2} \left(\prod_{l=1}^{m-1} |M_l| \right)^{-1} = 2^{nm}.$$

Отсюда и из равенства (52) следует, что

$$\forall l \in \{0, 1, \dots, m-1\}: |\text{Ker } G_l(\sigma)| = |M_l| = 2^{nm}.$$

Докажем второе утверждение. Включения

$$\forall l \in \{0, 1, \dots, m-1\}: \quad \overline{\text{Ker } G_l(\sigma)} \subseteq \text{Ker } \bar{G}_l(\bar{\sigma}) \quad (53)$$

очевидны. Приводя разложение (50) по модулю радикала, получим, что

$$\bar{R} \bar{R}_{m \times m} = \overline{\text{Ker } G_0(\sigma)} \dot{+} \overline{\text{Ker } G_1(\sigma)} \dot{+} \dots \dot{+} \overline{\text{Ker } G_{m-1}(\sigma)}. \quad (54)$$

С другой стороны, $\chi_{\bar{\sigma}}(x) = \bar{G}_0(x) \bar{G}_1(x) \dots \bar{G}_{m-1}(x)$, и поэтому

$$\bar{R} \bar{R}_{m \times m} = \text{Ker } \bar{G}_0(\bar{\sigma}) \dot{+} \text{Ker } \bar{G}_1(\bar{\sigma}) \dot{+} \dots \dot{+} \text{Ker } \bar{G}_{m-1}(\bar{\sigma}). \quad (55)$$

Комбинируя (53), (54) и (55), получаем требуемый результат.

Лемма доказана.

В дальнейшем будем использовать следующие обозначения:

$$\forall l \in \{0, 1, \dots, m-1\}: \quad N_l = \text{Ker } G_l(\sigma), \quad \bar{N}_l = \{\bar{X} \mid X \in N_l\}. \quad (56)$$

Согласно пункту (1) леммы 16 всякая матрица $X \in M$ однозначно представляется в виде

$$X = P + Q_1 + Q_2 + \dots + Q_{m-1}, \quad (57)$$

где $P \in N_0$ и $Q_l \in N_l$ для всех $l \in \{1, \dots, m-1\}$. В силу инвариантности подмодулей ${}_R N_l$ относительно автоморфизма σ

$$T_\sigma(X) = [T_\sigma(P), T_\sigma(Q_1), \dots, T_\sigma(Q_{m-1})]. \quad (58)$$

Лемма 17. Пусть $R = \mathbb{Z}_{2^n}$, $n \geq 1$. Справедливы следующие утверждения.

(1) Для любого $l \in \{1, \dots, m-1\}$ и любой матрицы $X \in N_l \setminus \{0\}$ верно равенство

$$T_\sigma(X) = 2^c \frac{\tau}{2^{(m,l)} - 1}, \quad (59)$$

где $0 \leq c \leq n-1$, $\tau = 2^m - 1$.

(2) Матрица $X \in M$ принадлежит N_0 , если и только если $UX = XV$.

Доказательство. Докажем первое утверждение. Поскольку $X \neq 0$, $G_l(\sigma)(X) = 0$ и $G_l(x)$ — многочлен Галуа, согласно лемме 1.1 в [10] и лемме 13

$$T_\sigma(X) = 2^c T(\bar{G}_l(x)) = 2^c T(\mu_{w^{2^l-1}}(x)) = 2^c \text{ord } w^{2^l-1} = 2^c \frac{\tau}{2^{(m,l)} - 1}$$

для некоторого $c \in \{0, 1, \dots, n-1\}$.

Докажем второе утверждение. Если $UX = XV$, то $\sigma^i(X) = XV^{\tau i}$ для всех $i \geq 0$. Отсюда следует, что $T_\sigma(X) \mid 2^{n-1}$. Рассмотрим разложение (57) матрицы X . Согласно (59) для всякого $l \in \{1, \dots, m-1\}$ такого, что $Q_l \neq 0$, выполнено соотношение $T_\sigma(Q_l) \nmid 2^{n-1}$. Поэтому в силу равенства (58) $X = P \in N_0$. Таким образом, все матрицы X , удовлетворяющие условию (47), принадлежат N_0 , и согласно пункту (2) леммы 14 их число равно 2^{nm} . По пункту (1) леммы 16 и в силу (56) справедливо равенство $2^{nm} = |N_0|$. Следовательно, множество матриц X , обладающих свойством (47), совпадает с модулем N_0 .

Лемма доказана.

Теперь сформулируем и докажем основные результаты этого параграфа. Всюду далее $n \geq 2$.

Теорема 5. Матрица $W(0) \in M$ обладает свойствами (7) тогда и только тогда, когда ее разложение (57) имеет вид

$$W(0) = P + Q_{l_1} + Q_{l_2} + \dots + Q_{l_s}, \quad (60)$$

где

$$\begin{aligned} \bar{P} &\neq 0, \quad s \geq 1, \quad 1 \leq l_1 < l_2 < \dots < l_s \leq m-1, \\ \forall l \in \{l_1, l_2, \dots, l_s\}: \quad \bar{Q}_l &= 0, \quad Q_l \neq 0. \end{aligned} \quad (61)$$

Доказательство. Пусть матрица $W(0) \in M$ обладает свойствами (7). Рассмотрим разложение (57) матрицы $W(0)$. Удалив из него нулевые матрицы Q_l , получим разложение (60), в котором $1 \leq l_1 < l_2 < \dots < l_s \leq m-1$, и для каждого значения $l \in \{l_1, l_2, \dots, l_s\}$ выполняется включение $Q_l \in N_l \setminus \{0\}$. В силу пункта 2 леммы 17 справедливо равенство $UP = PV$. Поскольку $UW(0) \neq W(0)V$, используя пункт (2) леммы 17, получаем, что $s \geq 1$. Согласно пункту (2) леммы 16 и пункту (2) леммы 17, примененному в случае $n = 1$,

$$\bar{U}\bar{W}(0) = \bar{W}(0)\bar{V} \iff \bar{W}(0) \in \text{Ker } \bar{G}_0(\bar{\sigma}) \iff \bar{W}(0) \in \overline{\text{Ker } G_0(\sigma)} \iff \bar{W}(0) = \bar{P}.$$

Отсюда $\bar{P} = \bar{W}(0) \neq 0$ и для всякого $l \in \{l_1, l_2, \dots, l_s\}$ верно равенство $\bar{Q}_l = 0$.

Обратно, пусть разложение (57) матрицы $W(0)$ имеет вид (60) и обладает свойствами (61). Тогда

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

Условие $s \geq 1$ означает, что $W(0) \notin N_0$, то есть, согласно пункту (2) леммы 17, выполняется неравенство $UW(0) \neq W(0)V$.

Теорема доказана.

Далее понадобится следующий очевидный факт.

Лемма 18. Пусть $d_1, d_2, \dots, d_s$ — делители числа τ . Тогда

$$\left[\frac{\tau}{d_1}, \frac{\tau}{d_2}, \dots, \frac{\tau}{d_s} \right] = \frac{\tau}{(d_1, d_2, \dots, d_s)}.$$

Центральным результатом о периодических свойствах регистра $\mathfrak{U}^\beta$ является следующее утверждение.

Теорема 6. Пусть матрица $W(0) \in M$ обладает свойствами (7). Тогда в обозначениях теоремы 5 справедливо равенство

$$T(W) = 2^{n-1} \frac{\tau^2}{2^{(m, l_1, l_2, \dots, l_s)} - 1}, \quad (62)$$

где $\tau = 2^m - 1$.

Доказательство. Если матрица $W(0) \in M$ обладает свойствами (7), то, согласно теореме 5, выполняются соотношения $\bar{P} \neq 0$ и $UP = PV$. Тогда $\sigma^i(P) = PV^{\tau i}$ для любого $i \geq 0$ и $T_\sigma(P) = 2^{n-1}$. Теперь равенство (62) следует из равенства (58), леммы 11, леммы 17 и леммы 18.

Теорема доказана.

Напомним (см. раздел 1), что состояние $W(0)$ автомата $\mathfrak{A}^\beta$ называется основным, если $T(W) = 2^{n-1}(2^m - 1)^2$. Теорема 6 позволяет сформулировать и доказать простой критерий свойства быть основным состоянием.

Следствие 4. Матрица $W(0) \in M$ является основным состоянием регистра $\mathfrak{A}^\beta$, если и только если она обладает свойствами (7) и для набора $(l_1, l_2, \dots, l_s)$ из разложения (60) матрицы $W(0)$ справедливо равенство $(m, l_1, l_2, \dots, l_s) = 1$.

Доказательство. Сформулированное утверждение непосредственно вытекает из следствия 1 и теоремы 6.

5. Число основных состояний

Здесь, как и в предыдущем разделе, $R = \mathbf{Z}_{2^n}$, $n \geq 2$, $F_0(x) = F_1(x) = F(x)$ — многочлен максимального периода степени $m \geq 2$. Рассмотрим естественный эпиморфизм $R \rightarrow \hat{R} = R/2^{n-1}R$. Обозначим через $\hat{X}$ образ матрицы $X \in M$ при этом эпиморфизме. Введем обозначение: пусть для всякого подмодуля ${}_R N$ модуля ${}_R M$

$$\hat{N} = \{\hat{X} \mid X \in N\}.$$

Определим автоморфизм $\hat{\sigma}$ модуля $\hat{R}\hat{M}$ равенством

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

Индекс нильпотентности кольца $\hat{R}$ равен $n - 1 \geq 1$. Согласно пункту (1) леммы 16 справедливо соотношение

$$\forall l \in \{1, \dots, m-1\}: \quad |\text{Ker } \hat{G}_l(\hat{\sigma})| = 2^{m(n-1)}. \quad (63)$$

Кроме того, для любой матрицы $X \in M$

$$\forall l \in \{1, \dots, m-1\}: \quad 2X \in \text{Ker } G_l(\sigma) \iff \hat{X} \in \text{Ker } \hat{G}_l(\hat{\sigma}). \quad (64)$$

Для каждого $s \in \{1, \dots, m-1\}$ рассмотрим функцию $\varphi^{[s]}: \mathbf{N} \rightarrow \mathbf{N}_0$, определенную равенством

$$\varphi^{[s]}(m) = |\{(l_1, l_2, \dots, l_s): 1 \leq l_1 < l_2 < \dots < l_s \leq m-1, \quad (m, l_1, l_2, \dots, l_s) = 1\}|.$$

Очевидно, $\varphi^{[1]}$ есть функция Эйлера (см. [2]). Значение функции $\varphi^{[s]}$ раскрывает следующее утверждение.

Лемма 19. Во введенных обозначениях число $N(\mathfrak{A}^\beta)$ основных состояний регистра $\mathfrak{A}^\beta$ может быть вычислено по формуле

$$N(\mathfrak{A}^\beta) = 2^{m(n-1)}(2^m - 1) \sum_{s=1}^{m-1} (2^{m(n-1)} - 1)^s \varphi^{[s]}(m). \quad (65)$$

Доказательство. Согласно пункту (2) леммы 17, теореме 5 и следствию 4 основные состояния суть матрицы вида

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

где

$$\bar{P} \neq 0, \quad UP = PV, \quad s \geq 1, \quad 1 \leq l_1 < l_2 < \dots < l_s \leq m-1, \\ \forall l \in \{l_1, l_2, \dots, l_s\}: \quad \bar{Q}_l = 0, \quad Q_l \in N_l \setminus \{0\},$$

и выполняется равенство $(m, l_1, l_2, \dots, l_s) = 1$. Из пункта (1) леммы 14 следует, что число матриц P , обладающих свойствами $\bar{P} \neq 0$ и $UP = PV$, совпадает с числом ненулевых по модулю радикала рекуррент $u \in L_R(F)$ и, следовательно, равно $2^{m(n-1)}(2^m - 1)$. При фиксированном $s \in \{1, \dots, m-1\}$ число наборов $(l_1, l_2, \dots, l_s)$, обладающих свойствами

$$1 \leq l_1 < l_2 < \dots < l_s \leq m-1, \quad (m, l_1, l_2, \dots, l_s) = 1 \quad (66)$$

равно $\varphi^{[s]}(m)$. Согласно (63) и (64), число ненулевых матриц $Q_l \in N_l = \text{Ker } G_l(\sigma)$ таких, что $\bar{Q}_l = 0$, равно

$$|\text{Ker } \hat{G}_l(\hat{\sigma})| - 1 = 2^{m(n-1)} - 1.$$

Таким образом, число основных состояний выражается формулой (65).

Лемма доказана.

Для того чтобы получить явную формулу числа основных состояний, необходимо выразить функцию $\varphi^{[s]}$ через известные комбинаторные функции. Обозначим через μ функцию Мебиуса [2].

Лемма 20. Во введенных обозначениях справедливо равенство

$$\forall s \in \{1, \dots, m-1\}: \quad \varphi^{[s]}(m) = \sum_{d|m} \mu(d) \binom{m/d-1}{s}. \quad (67)$$

Доказательство. Докажем (67) методом включения–исключения. Будем подсчитывать наборы $(l_1, l_2, \dots, l_s)$, для которых выполняются соотношения (66). Пусть в качестве элементов выступают наборы $(l_1, l_2, \dots, l_s)$ такие, что $1 \leq l_1 < l_2 < \dots < l_s \leq m-1$. Рассмотрим каноническое разложение числа $m \geq 2$

$$m = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t},$$

где $k_i \geq 1$ для всех $i \in \{1, \dots, t\}$. Пусть свойство $P_i, i \in \{1, \dots, t\}$, элемента $(l_1, l_2, \dots, l_s)$ состоит в том, что $p_i \mid l_j$ для всех $j \in \{1, \dots, s\}$. Для всякого набора чисел $(i_1, i_2, \dots, i_k), 1 \leq i_1 < i_2 < \dots < i_k \leq t$, обозначим через $N(P_{i_1}, P_{i_2}, \dots, P_{i_k})$ число элементов, одновременно обладающих свойствами $P_{i_1}, P_{i_2}, \dots, P_{i_k}$. Согласно формуле включения–исключения (см., например, [11]) число N_0 элементов, не обладающих ни одним из свойств P_i , вычисляется по формуле

$$N_0 = \sum_{k=0}^t (-1)^k \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq t} N(P_{i_1}, P_{i_2}, \dots, P_{i_k}).$$

Величина N_0 равна числу наборов $(l_1, l_2, \dots, l_s)$, для которых выполняются соотношения (66), и следовательно, совпадает с $\varphi^{[s]}(m)$. Поскольку

$$N(P_{i_1}, P_{i_2}, \dots, P_{i_k}) = \binom{m/(p_{i_1} p_{i_2} \dots p_{i_k}) - 1}{s},$$

согласно определению функции Мебиуса

$$\begin{aligned}\varphi^{[s]}(m) &= \sum_{k=0}^t (-1)^k \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq t} \binom{m/(p_{i_1} p_{i_2} \dots p_{i_k}) - 1}{s} \\ &= \sum_{d|m} \mu(d) \binom{m/d - 1}{s}.\end{aligned}$$

Лемма доказана.

Теперь сформулируем и докажем основной результат этого параграфа.

Теорема 7. Во введенных обозначениях число $N(\mathfrak{A}^\beta)$ основных состояний регистра $\mathfrak{A}^\beta$ может быть вычислено по формуле

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

где μ — функция Мебиуса.

Доказательство. Комбинируя лемму 19 и лемму 20, получаем, что

$$\begin{aligned}N(\mathfrak{A}^\beta) &= 2^{m(n-1)} (2^m - 1) \sum_{s=1}^{m-1} (2^{m(n-1)} - 1)^s \varphi^{[s]}(m) \\ &= (2^m - 1) \sum_{d|m} \mu(d) 2^{m(n-1)} \sum_{s=1}^{m-1} (2^{m(n-1)} - 1)^s \binom{m/d - 1}{s} \\ &= (2^m - 1) \sum_{d|m} \mu(d) 2^{m(n-1)} \sum_{s=0}^{m/d-1} (2^{m(n-1)} - 1)^s \binom{m/d - 1}{s} \\ &\quad - (2^m - 1) \sum_{d|m} \mu(d) 2^{m(n-1)} \\ &= (2^m - 1) \sum_{d|m} \mu(d) 2^{m(n-1)} (2^{m(n-1)})^{m/d-1} \\ &= (2^m - 1) \sum_{d|m} \mu(d) (2^{m(n-1)})^{m/d} = (2^m - 1) \sum_{d|m} \mu(m/d) 2^{m(n-1)d}.\end{aligned}$$

Теорема доказана.

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

Список литературы

1. Бурбаки Н., *Алгебра II. Модули, кольца, формы*. Наука, Москва, 1966.
2. Глухов М. М., Елизаров В. П., Нечаев А. А., *Алгебра*. Гелиос, Москва, 2003.
3. Елизаров В. П., *Конечные кольца. Основы теории*. Гелиос, Москва, 2006.
4. Кузьмин А. С., Куракин В. Л., Нечаев А. А., Псевдослучайные и полилинейные последовательности. *Труды по дискретной математике* (1997) **1**, 139–202.
5. Куракин В. Л., Нечаев А. А., Периодический многочлен. В сб.: *Энциклопедия «Дискретная математика»*. Большая Российская энциклопедия, Москва, 2004, с. 201.
6. Лидл Р., Нидеррайтер Г., *Конечные поля*. Мир, Москва, 1988.
7. Михайлов Д. А., Унитарные полилинейные регистры сдвига и их периоды. *Дискретная математика* (2002) **14**, №1, 30–59.
8. Нечаев А. А., Многомерные регистры сдвига и сложность мультипоследовательностей. *Труды по дискретной математике* (2003) **6**, 150–165.
9. Нечаев А. А., О подобии матриц над коммутативным локальным артиновым кольцом. *Труды семинара им. И. Г. Петровского* (1983) **9**, 81–101.
10. Нечаев А. А., Цикловые типы линейных подстановок над конечными коммутативными кольцами. *Матем. сб.* (1993) **184**, №3, 21–56.
11. Сачков В. Н., *Введение в комбинаторные методы дискретной математики*. Наука, Москва, 1982.
12. Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A., Linear recurring sequences over rings and modules. *J. Math. Sci.* (1995) **76**, №6, 2793–2915.
13. Macdonald B. R., *Finite rings with identity*. Marcel Dekker, New York, 1974.
14. Zsigmondy K., Zur Theorie der Potenzreste.. *Monatsh. Math. Phys.* (1892) **3**, 265–284.

Статья поступила 17.11.2006.