А. В. Михалев, А. А. Нечаев, Цикловые типы семейств полилинейных рекуррент и датчики псевдослучайных чисел, *Матем. вопр. криптогр.*, 2014, том 5, выпуск 1, 95–125

https://www.mathnet.ru/mvk109

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2014 Т. 5 № 1 С. 95–125

УДК: 519.217.2

Цикловые типы семейств полилинейных рекуррент и датчики псевдослучайных чисел

А. В. Михалев[1], **А. А. Нечаев**[2]

[1]Московский государственный университет им. М. В. Ломоносова, Москва
[2]Академия криптографии Российской Федерации, Москва

Получено 20.IV.2012

Изучается возможность использования автомата, реализующего семейство полилинейных рекуррент, для построения генератора псевдослучайных последовательностей. В качестве характеристик, описывающих потенциально возможные периоды выходных последовательностей такого генератора, рассматриваются цикловой тип и функция периодов. Приводятся описания этих характеристик для семейств полилинейных геометрических, арифметических и конгруэнтных последовательностей над конечным полем.

Ключевые слова: полилинейные рекурренты, конечные поля, псевдослучайные последовательности, цикловой тип

Cyclic types of families of polylinear recurrent sequences and generators of pseudorandom numbers

A. V. Mikhalev[1], **A. A. Nechaev**[2]

[1]*Lomonosov Moscow State University, Moscow*
[2]*Academy of Cryptography of the Russian Federation, Moscow*

Abstract. We investigate the approach to the construction of the generator of pseudorandom sequences by means of an automaton realizing the family of polylinear recurrent sequences. As characteristics describing potentially possible periods of output sequences of such generator we consider the cyclic type and the function of periods. Descriptions of these characteristics for families of geometric, arithmetic and congruent polylinear sequences over finite field are provided.

Key words: polylinear recurrent sequences, finite fields, pseudorandom sequences, cycle type

Citation: *Mathematical Aspects of Cryptography*, 2014, vol. 5, no. 1, pp. 95–125 (Russian).

1. Введение. Базовый автомат над модулем

Один из перспективных способов построения псевдослучайных последовательностей (ПСП) связан с использованием линейных и полилинейных рекуррент над конечными модулями [1–5, 8, 9, 11, 16].

Основная идея метода, который более подробно описан ниже, состоит в том, что для произвольного конечного кольца A по некоторому семейству k-линейных рекуррентных последовательностей (*k-ЛРП-семейству*, см. ниже раздел 3.2) над точным модулем ${}_AM$ строится линейный неавтономный автомат без выхода

$$\mathfrak{R} = (\mathcal{D}, \Phi). \tag{1}$$

Здесь $\mathcal{D} = M^{\mathcal{F}}$ — множество состояний автомата — декартова степень модуля M, $\mathcal{F}$ — конечное множество (в случае, когда автомат $\mathfrak{R}$ строится по семейству k-ЛРП, $\mathcal{F}$ — конечное подмножество множества $\mathbb{N}_0^k$, $\mathbb{N}_0 = \{0, 1, 2, \dots\}$, являющееся диаграммой Ферре (см. ниже раздел 3.2)); $\Phi = \{\varphi_1, \dots, \varphi_k\}$ — система частичных функций перехода автомата, состоящая из попарно перестановочных автоморфизмов модуля ${}_A\mathcal{D}$. Далее этот автомат называется *базовым*. В [5], [11] такой автомат строится для каждого k-ЛРП-семейства и называется *k-линейным регистром сдвига* (k-ЛРС) (см. ниже раздел 3).

Для построения по автомату $\mathfrak{R}$ датчика ПСП над алфавитом Ω задается некоторая функция выхода $\Psi\colon \mathcal{D} \longrightarrow \Omega$ и определяется закон изменения состояний, зависящий от текущего индекса $i \in \mathbb{N}_0$. Последний этап можно реализовать одним из следующих двух наиболее естественных способов.

Первый способ состоит в том, что на основе автомата $\mathfrak{R}$ строится управляемый автомат с выходом

$$\mathfrak{A} = (U, \mathcal{D}, \Omega, \Phi, \Psi),$$

в котором входной алфавит есть $U = \mathbb{Z}_{\sigma_1} \times \dots \times \mathbb{Z}_{\sigma_k}$, где $\sigma_j = \operatorname{ord} \varphi_j$, $j \in \in \{1, 2, \dots, k\}$. Если автомат управляется последовательностью $\mathbf{u} \in U^{\mathbb{N}_0}$, i-й знак которой есть

$$\mathbf{u}(i) = (u_1(i), \dots, u_k(i)),$$

и в такте $i \in \mathbb{N}_0$ находится в состоянии $\delta(i) \in \mathcal{D}$, то автомат переходит из состояния $\delta(i)$ в состояние

$$\delta(i+1) = \varphi_1^{u_1(i)} \circ \dots \circ \varphi_k^{u_k(i)}(\delta(i)) = \overrightarrow{\varphi}^{\mathbf{u}(i)}(\delta(i)), \tag{2}$$

при этом выходной знак автомата в такте i получается с помощью *функции выхода* $\Psi\colon \mathcal{D} \to \Omega$ как элемент *выходного алфавита* Ω:

$$\xi(i) = \Psi(\delta(i)). \tag{3}$$

Второй способ сводится к построению на основе автомата $\mathfrak{R}$ автономного автомата

$$\mathfrak{B} = (\mathcal{D}, \Omega, \Phi/\rho, \Psi),$$

где $\rho\colon \mathcal{D} \longrightarrow \mathbb{Z}_{\sigma_1} \times \ldots \times \mathbb{Z}_{\sigma_k}$ — *функция самоуправления*, которая в i-м такте переводит автомат из состояния $\delta(i)$ в состояние

$$\delta(i+1) = \overrightarrow{\varphi}^{\rho(\delta(i))}(\delta(i)). \tag{4}$$

Периодические свойства выходных последовательностей указанных датчиков ПСП связаны со свойствами исходного автомата $\mathfrak{R}$. Здесь мы рассматриваем лишь *реверсивные* автоматы $\mathfrak{R}$, т. е. автоматы, удовлетворяющие условию

$$\forall d \in \mathcal{D},\ \mathbf{i} \in \mathbb{N}_0^k\ \ \exists \mathbf{j} \in \mathbb{N}_0^k\colon\ \overrightarrow{\varphi}^{\mathbf{j}}(\overrightarrow{\varphi}^{\mathbf{i}}(d)) = d.$$

Реверсивность автомата $\mathfrak{R}$ обеспечивается тем, что выбранные частичные функции перехода $\varphi_1, \ldots, \varphi_k$ суть попарно перестановочные автоморфизмы конечного порядка.

Назовем строку $\mathbf{t} = (t_1, \ldots, t_k) \in \mathbb{N}_0^k$ *вектор-периодом* состояния $d \in \mathcal{D}$ автомата $\mathfrak{R}$, если $\overrightarrow{\varphi}^{\mathbf{t}}(d) = d$, и назовем *группой вектор-периодов* этого состояния подгруппу

$$\mathfrak{P}(d) = \mathfrak{P}\mathfrak{R}(d)$$

группы $(\mathbb{Z}^k, +)$, порожденную всеми вектор-периодами состояния d. Заметим, что $\mathfrak{P}(d)$ — подгруппа ранга k, так как каждый из автоморфизмов φ_j имеет конечный порядок, и по определению эта подгруппа порождается множеством $\mathfrak{P}^+(d)$ всех своих векторов с неотрицательными координатами. Конечную абелеву группу

$$\mathfrak{T}(d) = \mathbb{Z}^k/\mathfrak{P}(d)$$

назовем *цикловой группой состояния* d, а ее порядок $T(d) = |\mathfrak{T}(d)| = |\mathbb{Z}^k : \mathfrak{P}(d)|$ — *потенциальным периодом* этого состояния.

Пусть $\langle\Phi\rangle = \langle\varphi_1, \ldots, \varphi_k\rangle$ — группа подстановок на множестве $\mathcal{D}$ с системой образующих $\{\varphi_1, \ldots, \varphi_k\}$ и $\mathcal{O}(d)$ — орбита элемента $d \in \mathcal{D}$ относительно группы подстановок $\langle\Phi\rangle$. Будем называть эту орбиту также *потенциальным циклом* состояния d.

Лемма 1.1. *Для любого элемента $d \in \mathcal{D}$ справедливо равенство $T(d) = |\mathcal{O}(d)|$. При этом для любого элемента $d' \in \mathcal{O}(d)$ справедливы равенства $\mathcal{O}(d') = \mathcal{O}(d), \mathfrak{P}(d') = \mathfrak{P}(d), T(d') = T(d)$.*

Доказательство. Для любых $\mathbf{s}, \mathbf{t} \in \mathbb{Z}^k$ равенство $\overrightarrow{\varphi}^{\mathbf{s}}(d) = \overrightarrow{\varphi}^{\mathbf{t}}(d)$ эквивалентно равенству $\overrightarrow{\varphi}^{\mathbf{s}-\mathbf{t}}(d) = d$, т. е. условию $\mathbf{s} - \mathbf{t} \in \mathfrak{P}(d)$. □

Теорема 1.2. *Пусть ξ — выходная последовательность автомата $\mathfrak{A}$, полученная под воздействием управляющей реверсивной последовательности $\mathbf{u}$ из начального состояния $\delta(0) = d$. Тогда ξ — реверсивная последовательность периода*

$$T(\xi) \leq T(\mathbf{u})T(d). \tag{5}$$

Доказательство. Пусть $T(\mathbf{u}) = l, |\mathcal{O}(d)| = t$. Рассмотрим последовательность состояний автомата

$$\delta = (\delta(0), \delta(1), \ldots, \delta(i), \ldots), \quad \delta(i) = \overrightarrow{\varphi}^{\mathbf{u}(0)+\ldots+\mathbf{u}(i-1)}(d), \tag{6}$$

и покажем, что это — реверсивная последовательность периода, не превосходящего tl. Тогда, очевидно, этому условию удовлетворяет и последовательность $\xi = \Phi(\delta)$.

Из (6), полагая $\overrightarrow{\varphi}^{\mathbf{u}(0)+\ldots+\mathbf{u}(l-1)} = \psi$ и пользуясь равенством $T(\mathbf{u}) = l$, получаем

$$\delta(ml) = \psi^m(d) \in \mathcal{O}(d), \quad m \in \mathbb{N}_0.$$

Так как ψ — подстановка на $\mathcal{D}$, то $d, \psi(d), \ldots, \psi^m(d), \ldots$ — реверсивная последовательность периода $s \leq t$. Отсюда, пользуясь (6), получаем, что для любого $i \in \mathbb{N}_0$

$$\delta(sl + i) = \overrightarrow{\varphi}^{\mathbf{u}(sl)+\ldots+\mathbf{u}(sl+i-1)}(\delta(sl)),$$

и так как $T(\mathbf{u}) = l, \delta(sl) = \psi^s(d) = d = \delta(0)$, то

$$\delta(sl + i) = \overrightarrow{\varphi}^{\mathbf{u}(0)+\ldots+\mathbf{u}(i-1)}(d) = \delta(i).$$

Следовательно, δ — реверсивная последовательность, период которой делит sl, причем $sl \leq tl$. $\square$

Теорема 1.3. *Пусть ξ — выходная последовательность автомата $\mathfrak{B}$, полученная из начального состояния $\delta(0) = d$. Тогда*

$$T(\xi) \leq T(d). \tag{7}$$

Доказательство. Рассмотрим последовательность δ состояний автомата, полученную по правилу (4) из начального состояния $\delta(0) = d$. Положим

$$\mathbf{t}_0 = 0, \quad \mathbf{t}_i = \rho(\delta(0)) + \ldots + \rho(\delta(i-1)), \quad i \in \mathbb{N}.$$

Тогда $\delta(i) = \overrightarrow{\varphi}^{\mathbf{t}_i}(d)$, $i \in \mathbb{N}_0$, и для некоторых $0 \le u < v \le T(d) - 1$ выполняется соотношение $\mathbf{t}_u \equiv \mathbf{t}_v (\mod \mathfrak{P}(d))$, влекущее равенство $\delta(u) = \delta(v)$. Так как $\mathfrak{B}$ — автономный автомат, последнее равенство означает, что $T(\delta) | v - u$, а значит, и $T(\xi) | v - u$. □

Таким образом, периодические свойства выходных последовательностей автоматов $\mathfrak{A}$ и $\mathfrak{B}$ в значительной степени определяются потенциальными периодами состояний исходного автомата $\mathfrak{R}$, и изучение этих периодов представляется важной первичной задачей. В прикладном аспекте интересно также научиться строить указанные автоматы так, чтобы неравенства (5) и (7) обращались в равенства. Заметим, что в [16] построен пример такого автономного автомата на основе 2-линейного регистра сдвига над кольцом Галуа $\mathrm{GR}(2^{rn}, 2^n)$.

2. Цикловой тип и функция периодов реверсивного автомата

В связи с приведенными выше результатами представляется интересной следующая интегральная характеристика автомата $\mathfrak{R}$.

Пусть $\mathcal{H}_k$ есть множество всех подгрупп $G \le (\mathbb{Z}^k, +)$ свободной абелевой группы $\mathbb{Z}^k$ ранга k, имеющих конечный индекс, т. е. ранг k, и таких, что группа G порождается множеством G^+ ее неотрицательных векторов. (Открытая проблема: насколько множество $\mathcal{H}_k$ отличается от множества всех подгрупп ранга k группы $\mathbb{Z}^k$?)

Согласно [2, лемма 7.12], множество $\mathcal{H}_k$ есть полугруппа относительно операции пересечения $\cap$.

Цикловым типом автомата $\mathfrak{R}$ назовем элемент полугрупповой алгебры $(\mathbb{Z}\mathcal{H}_k, +, \cdot)$

$$\mathbf{Z}\mathfrak{R} = \sum_{G \in \mathcal{H}_k} c_{\mathfrak{R}}(G) G, \tag{8}$$

где $c_{\mathfrak{R}}(G) \in \mathbb{N}_0$ есть число таких орбит $\mathcal{O}(d) \subseteq \mathcal{D}$ группы $\langle \Phi \rangle$, что $\mathfrak{P}(d) = G$. Заметим, что этот элемент является также элементом полукольца $(\mathbb{N}_0\mathcal{H}_k, +, \cdot)$ и элементом кольца $\mathbb{Q}\mathcal{H}_k$. Поэтому его можно представить в виде суммы

$$\mathbf{Z}\mathfrak{R} = \sum_{d \in \mathcal{D}} \frac{1}{|\mathcal{O}(d)|} \mathfrak{P}(d). \tag{9}$$

Для любого элемента $G \in \mathcal{H}_k$ введем обозначение $\operatorname{ind} G = |\mathbb{Z}^k : G|$ — индекс подгруппы G в группе $\mathbb{Z}^k$. Тогда ввиду очевидного условия

$$|\mathcal{O}(d)| = \operatorname{ind} \mathfrak{P}(d), \quad d \in \mathcal{D}, \tag{10}$$

цикловой тип автомата $\mathfrak{R}$ можно записать также в виде

$$\mathbf{Z}\mathfrak{R} = \sum_{d\in\mathcal{D}} \frac{1}{\operatorname{ind}\mathfrak{P}(d)}\mathfrak{P}(d). \tag{11}$$

При оценке возможного периода выходной последовательности реверсивного автомата, например, с использованием теорем 1.2, 1.3, вместо функции (8) иногда удобнее использовать еще более интегральную ее характеристику — *функцию периодов автомата* $\mathfrak{R}$, которая определяется как многочлен из $\mathbb{Z}[y]$ равенством

$$\mathrm{T}\mathfrak{R}(y) = \sum_{t\in\mathbb{N}} n_{\mathfrak{R}}(t)y^t, \tag{12}$$

где $n_{\mathfrak{R}}(t)$ — число орбит мощности t группы $\langle\Phi\rangle$. Ввиду (10) из (8) следуют равенства

$$\mathrm{T}\mathfrak{R}(y) = \sum_{G\in\mathcal{H}_k} c_{\mathfrak{R}}(G)y^{\operatorname{ind}G} = \sum_{d\in D} \frac{1}{|\mathcal{O}(d)|}y^{|\mathcal{O}(d)|}. \tag{13}$$

Правая часть равенства (12) получается из правой части равенства (13) приведением подобных членов. Таким образом, вообще говоря, цикловой тип автомата $\mathfrak{R}$ не восстанавливается однозначно по его функции периодов.

Однако в случае $k = 1$ функция (12), по сути, совпадает с цикловым типом автомата $\mathfrak{R}$, точнее, представляет собой несколько иную запись циклового типа, поскольку любая ненулевая подгруппа $G \leq \mathbb{Z}$ является циклической ($G = \langle t\rangle$, $t > 0$), и однозначно определяется своим индексом $\operatorname{ind}G = t$, следовательно, в правой части равенства (13) нет подобных членов, т. е. $n_{\mathfrak{R}}(t) = c_{\mathfrak{R}}(\langle t\rangle)$.

Допустим теперь, что в автомате $\mathfrak{R}$ модуль ${}_A\mathcal{D}$ раскладывается в прямую сумму A–подмодулей

$$\mathcal{D} = \mathcal{D}_1 \dotplus \mathcal{D}_2, \tag{14}$$

каждый из которых инвариантен относительно каждого из автоморфизмов системы Φ. В этой ситуации, обозначая через φ_{ij} ограничение автоморфизма φ_j на подмодуль $\mathcal{D}_i$, для $i \in \{1,2\}$, $j \in \{1,\ldots,k\}$, и полагая $\Phi_i = \{\varphi_{i1},\ldots,\varphi_{ik}\}$, будем говорить, что автомат $\mathfrak{R}$ есть *прямое произведение автоматов* $\mathfrak{R}_i = (\mathcal{D}_i, \Phi_i)$, $i \in \{1,2\}$, и писать

$$\mathfrak{R} = \mathfrak{R}_1 \times \mathfrak{R}_2. \tag{15}$$

При этом условии цикловой тип автомата $\mathfrak{R}$ выражается через цикловые типы автоматов $\mathfrak{R}_1, \mathfrak{R}_2$ следующим образом.

Определим *композицию* $*$ *элементов*

$$A = \sum_{G \in \mathcal{H}_k} a_G G, \quad B = \sum_{G \in \mathcal{H}_k} b_G G \in \mathbb{Z}\mathcal{H}_k$$

равенством

$$A * B = C = \sum_{G \in \mathcal{H}_k} c_G G, \ \text{ где } c_G = \sum_{G_1 \cap G_2 = G} \frac{\operatorname{ind} G_1 \operatorname{ind} G_2}{\operatorname{ind} G} a_{G_1} b_{G_2}. \tag{16}$$

В [2] доказано, что алгебра $(\mathbb{Z}\mathcal{H}_k, +, *)$ есть коммутативное кольцо с единицей.

Теорема 2.1. *При условии* (15) *справедливо равенство*

$$\mathbf{Z}\mathfrak{R} = \mathbf{Z}\mathfrak{R}_1 * \mathbf{Z}\mathfrak{R}_2.$$

Доказательство. Представляя произвольный элемент $d \in \mathcal{D} = \mathcal{D}_1 \dot{+} \mathcal{D}_2$ в виде $d = d_1 + d_2$, $d_i \in \mathcal{D}_i$, и пользуясь условием (15), получаем, что для любого $\mathbf{t} \in \mathbb{N}_0^k$

$$\overrightarrow{\varphi}^{\mathbf{t}}(d) = \overrightarrow{\varphi_1}^{\mathbf{t}}(d_1) + \overrightarrow{\varphi_2}^{\mathbf{t}}(d_2).$$

Отсюда ввиду условия (14) получаем, что

$$\overrightarrow{\varphi}^{\mathbf{t}}(d) = d \iff \overrightarrow{\varphi_1}^{\mathbf{t}}(d_1) = d_1, \quad \overrightarrow{\varphi_2}^{\mathbf{t}}(d_2) = d_2,$$

и

$$\mathfrak{PR}(d) = \mathfrak{PR}_1(d_1) \cap \mathfrak{PR}_2(d_2).$$

Теперь, пользуясь определением (11), имеем равенства

$$\begin{aligned} Z\mathfrak{R} &= \sum_{d_1 \in \mathcal{D}_1} \sum_{d_2 \in \mathcal{D}_2} \frac{1}{\operatorname{ind}\left(\mathfrak{PR}_1(d_1) \cap \mathfrak{PR}_2(d_2)\right)} \left(\mathfrak{PR}_1(d_1) \cap \mathfrak{PR}_2(d_2)\right) = \\ &= \sum_{d_1 \in \mathcal{D}_1} \sum_{d_2 \in \mathcal{D}_2} \frac{\operatorname{ind} \mathfrak{PR}_1(d_1) \operatorname{ind} \mathfrak{PR}_2(d_2)}{\operatorname{ind}\left(\mathfrak{PR}_1(d_1) \cap \mathfrak{PR}_2(d_2)\right)} \frac{1}{\operatorname{ind} \mathfrak{PR}_1(d_1) \operatorname{ind} \mathfrak{PR}_2(d_2)} \times \\ &\qquad \times \left(\mathfrak{PR}_1(d_1) \cap \mathfrak{PR}_2(d_2)\right) = Z\mathfrak{R}_1 * Z\mathfrak{R}_2. \quad \square \end{aligned}$$

В связи с этим результатом представляет интерес проблема описания неразложимых цикловых типов в полукольце $(\mathbb{N}\mathcal{H}_k, +, *)$ и соответствующих им базовых автоматов (в случае существования таковых).

Отметим, что при условии (15) функцию периодов автомата $\mathfrak{R}$, вообще говоря, нельзя выписать, имея только функции периодов автоматов $\mathfrak{R}_1$, $\mathfrak{R}_2$.

В данной работе изучаются цикловые типы полилинейных регистров сдвига — базовых автоматов, соответствующих семействам полилинейных рекуррентных последовательностей.

3. Полилинейные рекурренты и регистры сдвига

3.1. Общее определение полилинейной рекурренты

Пусть $(M, +)$ — конечная абелева группа. Произвольную функцию

$$u\colon \mathbb{N}_0^k \to M$$

назовем *k-последовательностью над M*. Через $M^{\langle k\rangle}$ обозначим группу всех k-последовательностей над M (с обычной операцией сложения функций).

Предположим, что на M задана структура левого модуля над кольцом A с единицей e. Тогда абелева группа $(M^{\langle k\rangle}, +)$ также превращается в левый A-модуль. Всюду далее предполагается, что ${}_AM$ — точный модуль. Исключение составляет лишь случай, когда мы рассматриваем M как $\mathbb{Z}$-модуль.

Скажем, что последовательность $u \in M^{\langle 1\rangle}$ (1-последовательность) есть *линейная рекуррентная последовательность (ЛРП) над модулем ${}_AM$*, если для некоторого $m \in \mathbb{N}_0$ существуют такие элементы $c_0, \ldots, c_{m-1} \in A$, что

$$u(i+m) = c_{m-1}u(i+m-1) + \ldots + c_1u(i+1) + c_0u(i), \quad i \geq 0. \tag{17}$$

Наименьшее $m \in \mathbb{N}_0$ с этим свойством назовем *рангом ЛРП u*. Ранг нулевой последовательности положим равным 0.

При фиксированном $k \in \mathbb{N}$ через 1_s обозначим s-ю строку единичной $k \times k$-матрицы над $\mathbb{Z}$, $1 \leq s \leq k$. Назовем k-последовательность $u \in M^{\langle k\rangle}$ *k-линейной* (*полилинейной*) *рекуррентной последовательностью* (*k-ЛРП или ПЛРП*) *над модулем ${}_AM$*, если для каждого $s \in \{1, \ldots, k\}$ существуют параметр $m_s \in \mathbb{N}_0$ и набор коэффициентов $c_{s0}, \ldots, c_{s,m_s-1} \in A$, для которых

$$u(\mathbf{i}+m_s1_s) = c_{s,m_s-1}u(\mathbf{i}+(m_s-1)1_s)+\ldots+c_{s1}u(\mathbf{i}+1_s)+c_{s0}u(\mathbf{i}), \quad \mathbf{i} \in \mathbb{N}_0^k. \tag{18}$$

Приведем некоторые результаты о полилинейных рекуррентах, изложенные в [2, 5, 8], адаптируя их к рассматриваемому частному случаю, когда M — конечный модуль.

Пусть $\mathcal{A}_k = A[\mathbf{x}] = A[x_1, \ldots, x_k]$ — кольцо многочленов от k переменных над кольцом A. Для произвольного $\mathbf{i} = (i_1, \ldots, i_k) \in \mathbb{N}_0^k$ положим $\mathbf{x}^{\mathbf{i}} = x_1^{i_1} \ldots x_k^{i_k}$. Определим произведение многочлена $H(\mathbf{x}) = \sum\limits_{\mathbf{j}\in\mathbb{N}_0^k} h_{\mathbf{j}}\mathbf{x}^{\mathbf{j}} \in \mathcal{A}_k$ на k-последовательность $u \in M^{\langle k\rangle}$ равенством

$$H(\mathbf{x})u = v \in M^{\langle k\rangle}, \quad v(\mathbf{i}) = \sum_{\mathbf{j}\in\mathbb{N}_0^k} h_{\mathbf{j}}v(\mathbf{i}+\mathbf{j}), \quad \mathbf{i} \in \mathbb{N}_0^k. \tag{19}$$

Таким образом, на $M^{\langle k\rangle}$ задается структура левого $\mathcal{A}_k$-модуля. При этом в случае $k = 1$ условие (17) равносильно условию

$$F(x)u = 0, \quad \text{где} \quad F(x) = x^m - c_{m-1}x^{m-1} - \ldots - c_1x - c_0 \in \mathcal{A}_1, \tag{20}$$

а в случае $k > 1$ условие (18) равносильно условию

$$F_s(x_s)u = 0,$$
$$\text{где } F_s(x_s) = x_s^{m_s} - c_{s,m_s-1}x_s^{m_s-1} - \ldots - c_{s1}x_s - c_{s0} \in \mathcal{A}_k,\ 1 \le s \le k. \tag{21}$$

При $k = 1$ унитарный многочлен $F(x) \in \mathcal{A}_1$, удовлетворяющий условию (20), называется *характеристическим многочленом* последовательности u. При $k > 1$ система унитарных многочленов $F_1(x_1), \ldots, F_k(x_k) \in \mathcal{A}_k$, удовлетворяющих условиям (21), называется системой *элементарных характеристических многочленов* k-последовательности u. Множество всех k-ЛРП над модулем ${}_AM$ будем обозначать $\mathcal{L}_A M^{\langle k\rangle}$. Ввиду конечности модуля M множество $\mathcal{L}_A M^{\langle k\rangle}$ есть подмодуль модуля ${}_{\mathcal{A}_k}M^{\langle k\rangle}$ [5, предложение 3.7].

Абелеву группу $(M, +)$ можно рассматривать как модуль ${}_AM$ над различными кольцами A с единицей, которым соответствуют разные классы линейных рекуррент $\mathcal{L}_A M^{\langle k\rangle}$. Крайними случаями при этом являются класс $\mathcal{L}_{\mathbb{Z}} M^{\langle k\rangle}$, когда группа M рассматривается как модуль над кольцом $\mathbb{Z}$ целых чисел, и класс $\mathcal{L}_{\mathbb{E}} M^{\langle k\rangle}$, где $\mathbb{E} = \mathrm{End}(M, +)$ — кольцо эндоморфизмов абелевой группы $(M, +)$ со стандартным определением произведения элемента $\alpha \in M$ на элемент $\varepsilon \in \mathbb{E}$ по правилу

$$\varepsilon\alpha = \varepsilon(\alpha).$$

Говоря об этих классах как о крайних случаях, мы имеем в виду следующее утверждение.

Предложение 3.1. *Пусть задан модуль* ${}_AM$, $Z = Z(A)$ *— центр кольца* A *и* $E = \mathrm{End}({}_ZM)$. *Тогда*

$$\mathcal{L}_{\mathbb{Z}} M^{\langle k\rangle} \subseteq \mathcal{L}_A M^{\langle k\rangle} \subseteq \mathcal{L}_E M^{\langle k\rangle} \subseteq \mathcal{L}_{\mathbb{E}} M^{\langle k\rangle}.$$

3.2. ЛРП-семейство и его определяющий полиэдр. Диаграмма Ферре

Назовем идеал (левый или правый) кольца $\mathcal{A}_k$ *унитарным*, если он содержит некоторую систему унитарных многочленов $F_1(x_1), \ldots, F_k(x_k) \in \mathcal{A}_k$. Под-

множество $\chi \subset \mathcal{A}_k$ назовем *унитарным слева*, если левый идеал $\mathcal{A}_k\chi$, порожденный этим подмножеством в $\mathcal{A}_k$, является унитарным. Для произвольного подмножества $T \subset M^{\langle k\rangle}$ определим его (*левый*) *аннулятор в кольце* $\mathcal{A}_k$ равенством

$$l(T) = l_{\mathcal{A}_k}(T) = \mathrm{Ann}_{\mathcal{A}_k}(T) = \{H(\mathbf{x}) \in \mathcal{A}_k \colon H(\mathbf{x})\mu = 0 \quad \forall \mu \in T\}. \tag{22}$$

Очевидно, $l(T)$ есть левый идеал кольца $\mathcal{A}_k$, и справедливо следующее утверждение.

Предложение 3.2. *Последовательность $\mu \in M^{\langle k\rangle}$ есть k-ЛРП над кольцом A тогда и только тогда, когда $l(\mu)$ есть унитарный левый идеал кольца $\mathcal{A}_k$.*

Обратно, для произвольного подмножества $\chi \subset \mathcal{A}_k$ можно определить его (*правый*) *аннулятор в* $M^{\langle k\rangle}$ равенством

$$r(\chi) = L_M(\chi) = \{\mu \in M^{\langle k\rangle} \,:\, H(\mathbf{x})\mu = 0 \;\; \forall H(\mathbf{x}) \in \chi\}. \tag{23}$$

Ясно, что $r(\chi)$ есть подгруппа в $(M^{\langle k\rangle}, +)$, и $r(\chi) = r(I)$, где $I = \mathcal{A}_k\chi$ — левый идеал, порожденный множеством χ в кольце $\mathcal{A}_k$. Более того, пусть $Z = Z(A)$ — центр кольца A и $\mathcal{Z}_k = Z[x_1, \ldots, x_k]$ — кольцо многочленов над Z. Тогда $L_M(\chi)$ есть подмодуль модуля ${}_{\mathcal{Z}_k}M^{\langle k\rangle}$, поскольку все многочлены из $\mathcal{Z}_k$ перестановочны с многочленами из χ.

Если χ — унитарное слева подмножество в $\mathcal{A}_k$, то $L_M(\chi)$ есть некоторое множество полилинейных рекуррент над M, которое мы будем называть *k-ЛРП семейством с характеристическим множеством* χ. Всякое такое семейство удовлетворяет некоторым условиям «конечности», использующим следующие понятия.

Произвольное конечное подмножество

$$\mathcal{F} = \{\mathbf{i}_1, \ldots, \mathbf{i}_n\} \subseteq \mathbb{N}_0^k \tag{24}$$

назовем *полиэдром*. На множестве $\mathbb{N}_0^k$ зададим отношение $\leq$ частичного порядка следующим образом: если $\mathbf{i} = (i_1, \ldots, i_k)$, $\mathbf{j} = (j_1, \ldots, j_k) \in \mathbb{N}_0^k$, то $\mathbf{i} \leq \mathbf{j}$ тогда и только тогда, когда $i_s \leq j_s$ при всех $s \in \{1, \ldots, k\}$. Назовем полиэдр $\mathcal{F}$ *диаграммой Ферре*, если

$$\forall \mathbf{i}, \mathbf{j} \in \mathbb{N}_0^k \quad (\mathbf{i} \in \mathcal{F},\ \mathbf{j} \leq \mathbf{i}) \quad \Rightarrow \quad (\mathbf{j} \in \mathcal{F}).$$

Важным частным случаем диаграммы Ферре является *параллелепипед* Π *размеров* $m_1 \times \ldots \times m_k$ в $\mathbb{N}_0^k$, $m_1, \ldots, m_k \in \mathbb{N}$, определяемый равенством

$$\Pi = \Pi(\boldsymbol{m}) = \Pi(m_1, \ldots, m_k) = \{0, \ldots, m_1 - 1\} \times \ldots \times \{0, \ldots, m_k - 1\}.$$

Если $k = 1$, то $\Pi(m)$ есть просто отрезок натурального ряда: $\Pi(m) = \{0, \dots, m-1\}$, и такими отрезками исчерпываются все диаграммы Ферре.

Пусть $\mathcal{F}$ — полиэдр вида (24) и $M^{\mathcal{F}}$ — A-модуль всех функций $\delta\colon \mathcal{F} \to M$. Любая такая функция однозначно определяется *диаграммой значений* $\delta[\mathcal{F}] = (\delta(\mathbf{i}_1), \dots, \delta(\mathbf{i}_n)) \in M^n$, $n = |\mathcal{F}|$. Очевидно, модуль ${}_AM^{\mathcal{F}}$ изоморфен модулю ${}_AM^n = {}_AM^{|\mathcal{F}|}$, и его можно также рассматривать как Z-модуль, где $Z = Z(A)$ — центр кольца A.

Диаграммой значений k-последовательности $\mu \in M^{\langle k\rangle}$ на $\mathcal{F}$ назовем вектор $\mu[\mathcal{F}] = (\mu(\mathbf{i}_1), \dots, \mu(\mathbf{i}_n))$. Для любого подмножества $\chi \subset \mathcal{A}_k$ семейству $L_M(\chi)$ поставим в соответствие Z-подмодуль

$$L_M^{\mathcal{F}}(\chi) = \{\mu[\mathcal{F}]\colon \mu \in L_M(\chi)\} < {}_ZM^{|\mathcal{F}|}.$$

Очевидно, что отображение

$$\sigma_{\mathcal{F}}\colon L_M(\chi) \to L_M^{\mathcal{F}}(\chi) \subset M^{\mathcal{F}}, \quad \sigma_{\mathcal{F}}(\mu) = \mu[\mathcal{F}], \tag{25}$$

есть эпиморфизм Z-модулей.

Если эпиморфизм $\sigma_{\mathcal{F}}$ есть изоморфизм Z-модулей, или, другими словами, гомоморфизм

$$\sigma_{\mathcal{F}}\colon L_M(\chi) \to M^{\mathcal{F}}, \quad \sigma_{\mathcal{F}}(\mu) = \mu[\mathcal{F}], \tag{26}$$

есть вложение, то будем говорить, что множество многочленов χ и семейство $L_M(\chi)$ *рекурсивно-конечно-представимы* (над модулем M) и $\mathcal{F}$ *— определяющий полиэдр* множества χ и семейства $L_M(\chi)$. Примерами множеств, не являющихся рекурсивно-конечно-представимыми, являются $\chi = \{0\}$ (тогда $L_M(\chi) = M^{\langle k\rangle}$) и $\chi = \{x_1, \dots, x_{k-1}\}$ при $k > 1$. Так как любой полиэдр $\mathcal{F} \subset \mathbb{N}_0^k$ принадлежит некоторому параллелепипеду, то ясно, что любое рекурсивно-конечно-представимое множество $\chi \subset \mathcal{A}_k$ имеет определяющий полиэдр, являющийся диаграммой Ферре (и даже параллелепипедом).

Предложение 3.3. *Пусть $\chi \subset \mathcal{A}_k$ — такое унитарное слева множество, что левый идеал $\mathcal{A}_k\chi$ содержит систему унитарных многочленов $F_1(x_1), \dots, F_k(x_k) \in \mathcal{A}_k$ степеней $m_1, \dots, m_k$ соответственно. Тогда k-ЛРП-семейство $L_M(\chi)$ рекурсивно-конечно-представимо, и полиэдр $\Pi(m_1, \dots, m_k)$ является определяющим для этого семейства. В частности, если M — конечный модуль, то $|L_M(\chi)| \le |M|^{m_1 \dots m_k}$.*

Предложение 3.3 является следствием определений (18), (21) и (23).

3.3. Рекурсивный линейный автомат, соответствующий ЛРП-семейству

Таким образом, каждому ЛРП-семейству $L_M(\chi)$ соответствует конечный автомат

$$\mathfrak{R}L_M(\chi) = (L_M(\chi), \mathbf{x}) \tag{27}$$

со множеством состояний $L_M(\chi)$ и набором частичных функций перехода $\mathbf{x} = (x_1, \ldots, x_k)$, в котором x_t идентифицируется с оператором умножения всех ЛРП из $L_M(\chi)$ на x_t. Мы будем называть его *рекурсивным линейным автоматом* (*РЛ-автоматом*) *над модулем M с характеристическим множеством χ*. Заметим, что так как для идеала $I = \mathcal{A}_k\chi$ выполняется равенство $L_M(\chi) = L_M(I)$, то автомат (27) можно записать в виде $\mathfrak{R}L_M(\chi) = \mathfrak{R}L_M(I)$.

Введенная выше общая терминология, используемая для описания циклового типа произвольного конечного автомата (1), выглядит в рассматриваемом случае следующим образом.

Траекторией последовательности $\mu \in M^{\langle k\rangle}$ называется множество

$$\mathcal{O}(\mu) = \{\mathbf{x}^{\mathbf{i}}\mu | \mathbf{i} \in \mathbb{N}_0^k\}.$$

Последовательность $\mu \in M^{\langle k\rangle}$ называется *периодической*, если ее траектория есть конечное множество, и *реверсивной*, если $\mathcal{O}(\mu) = \mathcal{O}(\mathbf{x}^{\mathbf{i}}\mu)$ для любого $\mathbf{i} \in \mathbb{N}_0^k$.

Идеал $I \leq \mathcal{A}_k$ называется *периодическим* (*реверсивным*), если найдутся такие целые неотрицательные числа $d_1, \ldots, d_k \in \mathbb{N}_0$ и натуральные числа $t_1, \ldots, t_k \in \mathbb{N}$, что

$$\forall s \in \{1, \ldots, k\}\colon x^{d_s}(x_s^{t_s} - e) \in I \quad \left(\text{соответственно} \quad x_s^{t_s} - e \in I\right).$$

Предложение 3.4 ([2]). *Для любой k-последовательности μ над конечным модулем ${}_AM$ следующие утверждения равносильны:*

(a) $\mathrm{Ann}(\mu)$ — унитарный идеал;

(b) $\mathrm{Ann}(\mu)$ — периодический идеал;

(c) μ — периодическая последовательность;

(d) μ — k-ЛРП над ${}_AM$.

Предложение 3.5 ([2]). *Для любой k-ЛРП μ над конечным модулем ${}_AM$ следующие утверждения равносильны:*

(a) $\mathrm{Ann}(\mu)$ — унитарный идеал, содержащий такие унитарные многочлены $F_1(x_1), \ldots, F_k(x_k)$, что $F_s(0) \in A^*$, $1 \leqslant s \leqslant k$;

(b) $\mathrm{Ann}(\mu)$ — реверсивный идеал;

(c) μ — реверсивная последовательность;

$(d)\ \forall\, \mathbf{i} \in \mathbb{N}_0^k \quad \exists \mathbf{j} \in \mathbb{N}_0^k\colon \mathbf{x}^{\mathbf{j}}(\mathbf{x}^{\mathbf{i}}\mu) = \mu.$

Для периодической последовательности μ множество $\mathcal{R}(\mu)$ всех реверсивных элементов ее траектории $\mathcal{O}(\mu)$, назовем ее (*потенциальным*) *циклом*, а число $T(\mu) = |\mathcal{R}(\mu)|$ — ее (*потенциальным*) *периодом*.

Из предложения 3.5(a, b) следует, что для реверсивной последовательности μ существуют векторы $\mathbf{t} \in \mathbb{N}_0^k$ со свойством $\mathbf{x}^{\mathbf{t}}\mu = \mu$, называемые *вектор-периодами* этой последовательности, и потому $\mathcal{O}(\mu) = \mathcal{R}(\mu)$. Подгруппу $\mathfrak{P}(\mu)$ группы $(\mathbb{Z}^k, +)$, порожденную всеми вектор-периодами реверсивной k-последовательности μ, назовем *группой вектор-периодов*, а фактор-группу $\mathfrak{T}(\mu) = \mathbb{Z}^k/\mathfrak{P}(\mu)$ — *цикловой группой* k-ЛРП μ.

Предложение 3.6 ([2]). *Для любой реверсивной k-ЛРП μ справедливо равенство*

$$T(\mu) = |\mathfrak{T}(\mu)| = \operatorname{ind}\mathfrak{P}(\mu).$$

Заметим, что если $\mu \in M^k$ есть k-ЛРП, то все введенные в данном разделе понятия совпадают с одноименными понятиями, сформулированными во введении для μ как для состояния автомата (27).

Однако изучение группы вектор-периодов некоторой k-ЛРП оказывается иногда более простой задачей, чем изучение этой группы для состояния реверсивного автомата общего вида, ввиду возможности использования аппарата колец многочленов.

Для реверсивного идеала $I \leq \mathcal{A}_k$ описанным выше стандартным способом определяются *вектор-период, группа вектор-периодов* $\mathfrak{P}(I)$*, цикловая группа* $\mathfrak{T}(I) = \mathbb{Z}^k/\mathfrak{P}(I)$ *и потенциальный период* $T(I) = |\mathfrak{T}(I)|$.

Пусть $I \leq \mathcal{A}_k$ — реверсивный левый идеал. Тогда любая ЛРП $\mu \in L_M(I)$ реверсивна, поскольку $I \subseteq \operatorname{Ann}(\mu)$. Цикловой тип автомата $\mathfrak{R}L_M(I)$, определенный в разделе 2, совпадает с *цикловым типом реверсивного семейства* $L_M(I)$, который определен в [2] как элемент полугрупповой алгебры $(\mathbb{Z}\mathcal{H}_k, +, \cdot)$:

$$\mathbf{Z}_I^M = \sum_{G \in \mathcal{H}_k} c_I^M(G)G = \sum_{\mu \in L_M(I)} \frac{1}{\operatorname{ind}\mathfrak{P}(\mu)}\mathfrak{P}(\mu), \tag{28}$$

где $c_I^M(G) \in \mathbb{N}_0$ — число таких орбит $\mathcal{O}(\mu) \subseteq L_M(I)$, что $\mathfrak{P}(\mu) = G$.

Далее для любого унитарного множества $\chi \in \mathcal{A}_k$, порождающего левый унитарный идеал $I = \mathcal{A}_k\chi \leq {}_{\mathcal{A}_k}\mathcal{A}_k$, будем использовать обозначения

$$\mathbf{Z}_\chi^M = \mathbf{Z}_I^M = \mathbf{Z}\mathfrak{R}L_M(\chi) = \mathbf{Z}\mathfrak{R}L_M(I).$$

В рассматриваемой ситуации предложение 2.1 имеет следующую интерпретацию.

Предложение 3.7. *Если модуль ${}_AM$ раскладывается в прямую сумму подмодулей ${}_AM = {}_AM_1 \dotplus {}_AM_2$, то справедливы соотношения*

$$L_M(I) = L_{M_1}(I) \dotplus L_{M_2}(I),$$
$$\mathfrak{R}L_M(I) \cong \mathfrak{R}L_{M_1}(I) \times \mathfrak{R}L_{M_2}(I),$$
$$\mathbf{Z}_I^M = \mathbf{Z}_I^{M_1} * \mathbf{Z}_I^{M_2}.$$

Таким образом, задача описания возможных цикловых типов РЛ-автоматов сводится к случаю, когда ${}_AM$ — неразложимый модуль. Заметим, что ввиду эквивалентности условий c), d) предложения 3.4 мы можем рассматривать любую k-ЛРП над модулем ${}_AM$ как k-ЛРП над модулем M с коммутативным кольцом коэффициентов, рассматривая в качестве такого кольца, например, центр $Z(A)$ кольца A.

Если кольцо A коммутативно, то *кольцом операторов идеала* $I \lhd \mathcal{A}_k$ называется фактор-кольцо $S = \mathcal{A}_k/I$. Если при этом I *— несингулярный идеал* кольца $\mathcal{A}_k$, т. е. $I \cap A = \{0\}$, то кольцо S можно представить как расширение кольца A: $S = A[\vartheta_1, \ldots, \vartheta_k]$, где $\vartheta_s = x_s + I$. В этой ситуации можно рассматривать семейство $L_M(\chi)$ как точный левый S-модуль, представляя произвольный элемент $\alpha \in S$ в виде $\alpha = h(\vartheta_1, \ldots, \vartheta_k)$, где $h(x_1, \ldots, x_k) \in \mathcal{A}_k$, и определяя произведение $\mu \in L_M(\chi)$ на α равенством

$$\alpha\mu = h(x_1, \ldots, x_k)\mu.$$

Если $I = \mathrm{Ann}(\mu) = \{h(\mathbf{x}) \in \mathcal{A}_k \colon h(\mathbf{x})\mu = 0\}$ — характеристический идеал некоторой последовательности $\mu \in M^{\langle k \rangle}$, то кольцо S называется также *кольцом операторов последовательности* μ.

Теорема 3.8 ([2]). *Пусть A — конечное коммутативное кольцо с единицей и I — реверсивный несингулярный идеал кольца $\mathcal{A}_k$. Тогда*

(a) элементы $\vartheta_1, \ldots, \vartheta_k$ обратимы в S и имеет место изоморфизм групп

$$\mathfrak{T}(I) \cong \mathcal{T}(I) = \langle \vartheta_1, \ldots, \vartheta_k \rangle \leqslant S^*, \tag{29}$$

(b) каждая рекуррента $\mu \in L_M(I)$ реверсивна и удовлетворяет условиям

$$\mathfrak{P}(I) \leq \mathfrak{P}(\mu), \tag{30}$$
$$\mathcal{R}(\mu) = \mathcal{T}(I)\mu, \tag{31}$$
$$T(\mu) | T(I), \tag{32}$$

(*c*) *если к тому же* $I = \mathrm{Ann}(\mu)$, *то*

$$\mathfrak{P}(I) = \mathfrak{P}(\mu), \quad T(\mu) = T(I).$$

Естественный изоморфизм (29), который существует в силу теоремы об эпиморфизме, если последний имеет вид

$$\psi\colon \mathbb{Z}^k \to \mathcal{T}(I), \quad \psi((t_1, \ldots, t_k)) = \vartheta_1^{t_1} \cdot \ldots \cdot \vartheta_k^{t_k},$$

позволяет называть группу $\mathcal{T}(I) = \langle \vartheta_1, \ldots, \vartheta_k \rangle$ также *цикловой группой идеала* I.

Применяя методы теории идеалов к рассматриваемому классу автоматов, можно дополнить предложение 2.1 еще одним способом разложения циклового типа рекурсивного линейного автомата в композицию цикловых типов более простых автоматов.

Предложение 3.9. *Если* A *— конечное коммутативное кольцо с единицей и* I *— реверсивный несингулярный идеал кольца* $\mathcal{A}_k$, *представимый в виде пересечения* $I = I_1 \cap I_2$ *взаимно простых идеалов, то справедливы соотношения*

$$L_M(I) = L_M(I_1) \dotplus L_M(I_2), \mathfrak{R}L_M(I) \cong \mathfrak{R}L_M(I_1) \times \mathfrak{R}L_M(I_2), \mathbf{Z}_I^M = \mathbf{Z}_{I_1}^M * \mathbf{Z}_{I_2}^M.$$

Из предложений 3.7 и 3.9 следует, что если кольцо A коммутативно, то задача описания возможных цикловых типов РЛ-автоматов $L_M(I)$ над ${}_AM$ сводится к случаю, когда M — неразложимый A-модуль и I — примарный идеал кольца $\mathcal{A}_k$.

3.4. Полилинейный регистр сдвига

Хорошо известно [2, 6, 12], что любая 1-ЛРП над ${}_AM$ может быть представлена как выходная последовательность специального линейного автомата, называемого *линейным регистром сдвига* (ЛРС). Минимум длин таких регистров называется *линейной сложностью 1-ЛРП*. Обобщение указанных понятий, предложенное в [5, 11], выглядит следующим образом.

Назовем рекурсивно-конечно-представимое множество многочленов $\chi \subset \mathcal{A}_k$ *систематическим*, если оно имеет такой определяющий полиэдр $\mathcal{F}$, что гомоморфизм (26) является не только вложением, но и изоморфизмом. Если к тому же полиэдр $\mathcal{F}$ есть диаграмма Ферре, то будем говорить, что

пара объектов $\langle \mathcal{F}, L_M(\chi)\rangle$ *задает k-линейный регистр сдвига* (k-ЛРС) или *$\mathcal{F}$-линейный регистр сдвига* ($\mathcal{F}$-ЛРС) над модулем ${}_AM$.

Остается открытым вопрос: можно ли для любого систематического множества многочленов $\chi \subset \mathcal{A}_k$ указать такую диаграмму Ферре $\mathcal{F}$, что гомоморфизм (26) есть изоморфизм?

По определению k-ЛРП-семейство $L_M(\chi)$ для любой диаграммы значений $\delta[\mathcal{F}] \in M^{\mathcal{F}}$ содержит единственную такую k-последовательность μ, что $\mu[\mathcal{F}] = \delta[\mathcal{F}]$. Последнее свойство, очевидно, эквивалентно тому, что пара $\langle \mathcal{F}, L_M(\chi)\rangle$ задает k-ЛРС над модулем ${}_AM$. Отметим, что введенное здесь определение $\mathcal{F}$-ЛРС-семейства несколько отличается от определения, данного ранее в [6], однако по существу оно выделяет тот же класс семейств k-последовательностей над M. А именно, k-ЛРС-семейство в смысле [6] есть k-ЛРС-семейство над M_B, где $B = \mathrm{End}({}_AM)$.

Если $\langle \mathcal{F}, L_M(\chi)\rangle$ есть k-ЛРС-семейство над модулем ${}_AM$, то произвольную k-последовательность $\mu \in L_M(\chi)$ мы будем называть последовательностью, *порождаемой этим k-ЛРС*, а также *$\langle \mathcal{F}, L_M(\chi)\rangle$-ЛРС-последовательностью* (*k-ЛРС-последовательностью*). Множество всех k-ЛРС-последовательностей над модулем ${}_AM$ будем обозначать через $LSR_A M^{\langle k\rangle}$.

Предложение 3.10. *Имеют место включения*

$$LSR_{\mathbb{Z}} M^{\langle k\rangle} \subseteq LSR_A M^{\langle k\rangle} \subseteq LSR_E M^{\langle k\rangle} \subseteq LSR_{\mathbb{E}} M^{\langle k\rangle}.$$

Предложение 3.10 доказывается так же, как предложение 3.1.

Ясно, что для данного $\mathcal{F}$-ЛРС-семейства $\langle \mathcal{F}, L_M(\chi)\rangle$ над модулем ${}_AM$ могут существовать другая диаграмма Ферре $\mathcal{F}_1$ и другое характеристическое множество χ_1, принадлежащее кольцу $\mathbb{E}_k$ многочленов над кольцом $\mathbb{E}$, удовлетворяющие условию $L_M(\chi) = L_M(\chi_1)$. В таком случае будем называть k-ЛРС-семейства $\langle \mathcal{F}, L_M(\chi)\rangle$ и $\langle \mathcal{F}_1, L_M(\chi_1)\rangle$ *эквивалентными*. Точнее, если A_1 — расширение кольца A, содержащее коэффициенты многочленов из χ_1, то будем говорить, что указанные ЛРС *A_1-эквивалентны*.

Очевидно, в случае, когда $M = A = P$ — поле, любой 1-ЛРС есть $\overline{0, m-1}$-ЛРС вида $\langle \overline{0, m-1}, L_M(\chi)\rangle$, где $\chi \subset P[x]$, $m \in \mathbb{N}$, и он эквивалентен над полем P единственному ЛРС-семейству вида $\langle \overline{0, m-1}, L_M(F(x))\rangle$, где $F(x)$ — унитарный многочлен степени m (НОД многочленов из множества χ). В общем случае подобного рода «каноническое» ЛРС-семейство, эквивалентное заданному, также существует, но строится, вообще говоря, неоднозначно и существенно сложнее.

Назовем (*внешней*) *границей диаграммы Ферре* $\mathcal{F} \subset \mathbb{N}_0^k$ *по направлению* 1_s, $s \in \{1, \ldots, k\}$, множество

$$\Delta_s \mathcal{F} = \{\mathbf{r} \in \mathbb{N}_0^k \colon \mathbf{r} \notin \mathcal{F},\ \mathbf{r} - 1_s \in \mathcal{F}\}. \tag{33}$$

Множество $\Delta\mathcal{F} = \bigcup\limits_{s=1}^{k} \Delta_s \mathcal{F}$ назовем *внешней границей диаграммы* $\mathcal{F}$. Многочлен $H(\mathbf{x}) \in \mathcal{A}_k$ назовем *$\mathcal{F}$-унитарным*, если для некоторого $\mathbf{r} \in \Delta\mathcal{F}$ он имеет вид

$$H(\mathbf{x}) = \mathbf{x}^{\mathbf{r}} - \sum_{\mathbf{i} \in \mathcal{F}} h_{\mathbf{i}} \mathbf{x}^{\mathbf{i}}. \tag{34}$$

При $k = 1$ любой унитарный многочлен $H(x) \in \mathcal{A}_1$ степени m является $\overline{0, m-1}$-унитарным. Систему $\mathbf{H} \subset \mathcal{A}_k$ из $|\Delta\mathcal{F}|$ многочленов назовем *полной системой $\mathcal{F}$-унитарных многочленов*, если для каждого $\mathbf{r} \in \Delta\mathcal{F}$ эта система содержит единственный многочлен вида (34), т. е. если $\mathbf{H}$ имеет вид

$$\mathbf{H} = \left\{ H_{\mathbf{r}}(\mathbf{x}) = \mathbf{x}^{\mathbf{r}} - \sum_{\mathbf{i} \in \mathcal{F}} h_{\mathbf{r},\mathbf{i}} \mathbf{x}^{\mathbf{i}} \colon \mathbf{r} \in \Delta\mathcal{F} \right\}. \tag{35}$$

Каждой полной системе $\mathcal{F}$-унитарных многочленов (35) соответствует система из k эндоморфизмов $\varphi_1, \ldots, \varphi_k$ Z-модуля $M^{\mathcal{F}}$, определяемых следующим образом:

$$\forall \delta \in M^{\mathcal{F}} \quad \varphi_s(\delta) = \lambda_s \in M^{\mathcal{F}}, \tag{36}$$

где

$$\forall \mathbf{j} \in \mathcal{F} \quad \lambda_s(\mathbf{j}) = \begin{cases} \delta(\mathbf{j} + 1_s), & \text{если } \mathbf{j} + 1_s \in \mathcal{F}, \\ \sum\limits_{\mathbf{i} \in \mathcal{F}} h_{\mathbf{r},\mathbf{i}} \delta(\mathbf{i}), & \text{если } \mathbf{j} + 1_s = \mathbf{r} \in \Delta\mathcal{F}. \end{cases} \tag{37}$$

Будем называть $\varphi_1, \ldots, \varphi_k$ *сопровождающими эндоморфизмами* системы многочленов (35). Приведем один из основных результатов работы [5].

Теорема 3.11. *Любое $\mathcal{F}$-ЛРС-семейство $\langle \mathcal{F}, L_M(\chi) \rangle$ над модулем ${}_AM$ эквивалентно такому $\mathcal{F}$-ЛРС-семейству $\langle \mathcal{F}, L_M(\mathbf{H}) \rangle$ над модулем ${}_EM$, что $\mathbf{H}$ — полная система $\mathcal{F}$-унитарных многочленов из кольца $\mathcal{E}_k$ многочленов над кольцом $E = \mathrm{End}({}_ZM)$ и ее сопровождающие эндоморфизмы $\varphi_1, \ldots, \varphi_k$ попарно перестановочны.*

Следующее обращение теоремы 3.11 дает критерий того, что пара $\langle \mathcal{F}, L_M(\chi) \rangle$ вида (35) задает линейный регистр сдвига.

Теорема 3.12 ([5]). *Пусть $\mathcal{F} \subset \mathbb{N}_0^k$ — диаграмма Ферре и $\mathbf{H} \subset \mathcal{A}_k$ есть такая полная система $\mathcal{F}$-унитарных многочленов вида (35), что ее сопровождающие эндоморфизмы $\varphi_1, \ldots, \varphi_k$ попарно перестановочны. Тогда пара $\langle \mathcal{F}, L_M(\mathbf{H}) \rangle$ есть $\mathcal{F}$-ЛРС-семейство над модулем ${}_AM$. При этом справедлива теорема Гамильтона–Кэли: для каждого многочлена $H_{\mathbf{r}}(\mathbf{x}) \in \mathbf{H}$ выполняется равенство $H_{\mathbf{r}}(\varphi_1, \ldots, \varphi_k) = 0$.*

В дальнейшем будем называть k-ЛРС-семейство $\langle \mathcal{F}, L_M(\mathbf{H}) \rangle$, удовлетворяющее условиям теоремы 3.12, *каноническим $\mathcal{F}$-ЛРС-семейством над модулем ${}_AM$*. Отметим, что для такого ЛРС-семейства справедливы соотношения

$$\forall \mu \in L_M(\mathbf{H}),\ C(\mathbf{x}) \in \mathcal{A}_k \colon (C(\mathbf{x})\mu)[\mathcal{F}] = C(\varphi_1, \ldots, \varphi_k)(\mu[\mathcal{F}]). \qquad (38)$$

Так как по предположению ${}_AM$ — точный модуль, то существует изоморфное вложение кольца A в кольцо $\mathbb{E} = \mathrm{End}(M, +)$, ставящее в соответствие каждому элементу $a \in A$ левую трансляцию $\widehat{a} \colon M \to M$, действующую на элементах $\alpha \in M$ по правилу $\widehat{a}(\alpha) = a\alpha$. Через $\widehat{A}$ будем обозначать подкольцо всех таких трансляций в $\mathbb{E}$.

Пусть $A' = \mathrm{End}({}_AM)^{op}$ — кольцо, противоположное кольцу эндоморфизмов $\mathrm{End}({}_AM)$, т. е. кольцо, в котором сумма $\sigma + \tau$ эндоморфизмов $\sigma, \tau \in \mathrm{End}({}_AM)$ определена по-прежнему, а операция умножения задается равенством $\sigma \cdot \tau = \tau \circ \sigma$. Тогда модуль ${}_AM$ можно рассматривать как бимодуль ${}_AM_{A'}$ и справедливо включение

$$\widehat{A} \subseteq A'' = \mathrm{End}(M_{A'}).$$

Назовем модуль ${}_AM$ *сбалансированным*, если $\widehat{A} = A''$. Сбалансированными являются, в частности, все свободные конечнопорожденные модули ${}_AM$ и все квазифробениусовы бимодули ${}_AM_B$ (см., например, [11]).

Теорема 3.13. *Если ${}_AM$ — сбалансированный модуль, то любое k-ЛРС семейство $\langle \mathcal{F}, L_M(\chi) \rangle$ эквивалентно некоторому каноническому k-ЛРС семейству $\langle \mathcal{F}, L_M(\mathbf{H}) \rangle$ над ${}_AM$ с диаграммой Ферре $\mathcal{F}$.*

3.5. Перечисление канонических ЛРС

По-прежнему полагаем, что ${}_AM$ — точный модуль. Справедлив следующий общий критерий того, что пара $\langle \mathcal{F}, L_M(\mathbf{H}) \rangle$, где $\mathbf{H}$ — полная система $\mathcal{F}$-унитарных многочленов (35), есть $\mathcal{F}$-линейный регистр сдвига, т. е. соответствующие сопровождающие эндоморфизмы попарно перестановочны.

Внутренностью и *внутренней границей* диаграммы Ферре $\mathcal{F} \subset \mathbb{N}_0^k$ в направлении 1_s, $s \in \{1, \ldots, k\}$, назовем соответственно множества

$$\mathcal{F}_s = \{\mathbf{r} \in \mathcal{F} \mid \mathbf{r} + 1_s \in \mathcal{F}\}, \quad \partial_s \mathcal{F} = \mathcal{F} \setminus \mathcal{F}_s.$$

Определенная выше внешняя граница диаграммы $\mathcal{F}$ в направлении 1_s связана с внутренней границей естественным соотношением: $\Delta_s \mathcal{F} = \partial_s \mathcal{F} + 1_s$ (см. рис. 1).

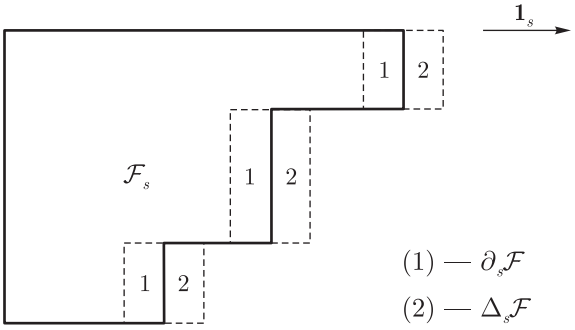

Рис. 1. Диаграмма Ферре

Теорема 3.14 ([11]). *Пусть $\mathcal{F}$ — диаграмма Ферре и $\mathbf{H}$ — полная система $\mathcal{F}$-унитарных полиномов из $\mathcal{A}_k$ вида* (35). *Тогда соответствующие системе $\mathbf{H}$ сопровождающие эндоморфизмы $\varphi_1, \ldots, \varphi_k$ попарно перестановочны (т. е. пара $\langle \mathcal{F}, L_M(\mathbf{H}) \rangle$ есть канонический ЛРС) тогда и только тогда, когда для любых $s, t \in \{1, \ldots, k\}$, $s \neq t$, выполняются следующие условия:*

$$H_{\mathbf{j}+1_s+1_s} = H_{\mathbf{j}+1_s} x_t + \sum_{\mathbf{k} \in \partial_t \mathcal{F}} h_{\mathbf{j}+1_s, \mathbf{k}} H_{\mathbf{k}+1_t} \quad \text{для } \mathbf{j} \in \partial_s \mathcal{F} \cap \mathcal{F}_t, \tag{39}$$

$$H_{\mathbf{j}+1_s} x_t + \sum_{\mathbf{k} \in \partial_t \mathcal{F}} h_{\mathbf{j}+1_s, \mathbf{k}} H_{\mathbf{k}+1_t} = H_{\mathbf{j}+1_t} x_s + \sum_{\mathbf{k} \in \partial_s \mathcal{F}} h_{\mathbf{j}+1_t, \mathbf{k}} H_{\mathbf{k}+1_s} \quad \text{для } \mathbf{j} \in \partial_s \mathcal{F} \cap \partial_t \mathcal{F}. \tag{40}$$

Следствие 3.15 ([5]). *Пусть диаграмма Ферре $\mathcal{F}$ есть параллелепипед $\Pi = \Pi(m_1, \ldots, m_k)$ и характеристическое множество χ состоит из элементарных унитарных многочленов над кольцом A:*

$$\chi = \{F_1(x_1), \ldots, F_k(x_k)\}, \text{ где } F_s(x_s) = x_s^{m_s} - \sum_{i=0}^{m_s - 1} f_{si} x_s^i, \quad 1 \leq s \leq k. \tag{41}$$

Тогда $\langle \Pi, L_M(\chi)\rangle$ *есть* k*-ЛРС над модулем* ${}_AM$ *в том и только в том случае, когда для любых различных* $s, t \in \{1, \ldots, k\}$ *выполнены условия*

$$\forall i \in \{0, \ldots, m_s - 1\}\ \forall j \in \{0, \ldots, m_t - 1\} \quad f_{si} f_{tj} = f_{tj} f_{si}. \tag{42}$$

Теорема 3.14 позволяет построить все канонические регистры сдвига над модулем ${}_AM$ на данной диаграмме Ферре $\mathcal{F}$.

Например, в [11] с помощью компьютерных вычислений было доказано, что если $k = 2$ и диаграмма Ферре имеет вид

$$\mathcal{F} = \{(0,0),\ (1,0),\ (0,1)\}, \tag{43}$$

то на ней можно построить ровно 64 различных канонических регистра сдвига над кольцом $\mathbb{Z}_2$ (эти регистры перечисляются) и 4096 регистров сдвига с опорной диаграммой Ферре $\mathcal{F}$ над кольцом $\mathbb{Z}_4$.

3.6. Базовый автомат, соответствующий каноническому ЛРС

Поставим в соответствие каноническому ЛРС $\langle \mathcal{F}, L_M(\mathbf{H})\rangle$ над модулем ${}_AM$ основной объект изучения данной работы — базовый автомат

$$\mathfrak{R}\mathbf{H} = (M^{\mathcal{F}}, \Phi\mathbf{H}), \tag{44}$$

где $\Phi\mathbf{H} = \{\varphi_1, \ldots, \varphi_k\}$ — набор сопровождающих эндоморфизмов рассматриваемого ЛРС (см. (36), (37)). Мы будем называть этот автомат так же, как и пару $\langle \mathcal{F}, L_M(\mathbf{H})\rangle$: *каноническим ЛРС с опорной диаграммой Ферре* $\mathcal{F}$.

Предложение 3.16. *Автомат* (44) *изоморфен автомату*

$$L\mathfrak{R}\mathbf{H} = (L_M(\mathbf{H}), \mathbf{x}). \tag{45}$$

Доказательство. По определению k-ЛРС отображение $\psi\colon L_M(\mathbf{H}) \to M^{\mathcal{F}}$, действующее по правилу

$$\forall \mu \in L_M(\mathbf{H})\colon \psi(\mu) = \mu[\mathcal{F}],$$

есть биекция. Зададим также биекцию $\varphi\colon \{x_1, \ldots, x_k\} \to \Phi$ правилом $\varphi(x_t) = \varphi_t$, $t \in \{1, \ldots, k\}$. Тогда пара отображений (ψ, φ) задает изоморфизм автоматов

$$(\psi, \varphi)\colon (L_M(\mathbf{H}), \mathbf{x}) \to (M^{\mathcal{F}}, \Phi\mathbf{H}),$$

поскольку в соответствии с (38) справедливы соотношения

$$\psi(x_t\mu) = (x_t\mu)[\mathcal{F}] = \varphi_t(\mu[\mathcal{F}]) = \varphi(x_t)(\mu[\mathcal{F}]) = \varphi(x_t)(\psi(\mu)).\ \square$$

4. Цикловые типы простейших линейных рекурсивных автоматов

Представляется интересным изучить цикловые типы описанных базовых автоматов, являющихся полилинейными регистрами сдвига (44). Здесь в качестве первого шага описаны цикловые типы и функции периодов следующих ЛРП-семейств над полем $P = \mathrm{GF}(q)$, $q = p^l$, $p = \mathrm{char}\, P$, которые мы называем *простейшими*:

(1) семейство *k-геометрических прогрессий*

$$L_g = L_P(x_1 - g_1, \ldots, x_k - g_k) \text{ для некоторых } g_1, \ldots, g_k \in P^*, \tag{46}$$

(2) семейство *k-арифметических прогрессий*

$$L_a = L_P((x_1 - e)^2, \ldots, (x_k - e)^2), \tag{47}$$

состоящее, согласно [2, 3, 15], из всех последовательностей

$$u(\mathbf{z}) = a_0 + a_1 z_1 + \ldots + a_k z_k, \quad a_0, \ldots, a_k \in P, \tag{48}$$

(3) ЛРП-семейство *k-конгруэнтных последовательностей*

$$L_c = L_P((x_1 - e)(x_1 - g_1), \ldots, (x_k - e)(x_k - g_k)), \tag{49}$$

состоящее (при фиксированных $g_1, \ldots, g_k \in P^* \setminus \{e\}$) из всех k-последовательностей $u(\mathbf{z})$ со свойствами

$$\begin{gathered} u(\mathbf{z} + 1_s) = g_s u(\mathbf{z}) + a_s, \quad a_s \in P, \quad g_s \in P^*, \\ (g_s - 1)a_t = (g_t - 1)a_s, \quad s, t \in \{1, \ldots, k\}. \end{gathered} \tag{50}$$

4.1. Цикловой тип семейства k-геометрических прогрессий.

Пусть $P = \mathrm{GF}(q)$ — поле мощности $q = p^l$ и характеристики p. Опишем цикловой тип ЛРП-семейства (46).

Теорема 4.1. *Пусть $g_1, \ldots, g_k \in P^*$ — элементы порядков $d_1, \ldots, d_k$ соответственно, и $I = {}_{\mathcal{P}_k}(x_1 - g_1, \ldots, x_k - g_k)\triangleleft\mathcal{P}_k$. Тогда верны следующие утверждения.*

(a) Семейство $L_g = L_P(I)$ состоит из всех k-последовательностей $u \in P^k$ вида

$$u(i_1, \ldots, i_k) = c g_1^{i_1} \ldots g_k^{i_k}, \quad c \in P. \tag{51}$$

(*b*) *Автомат* $\mathfrak{R}_g = (L_P(I), \mathbf{x})$ *изоморфен каноническому ЛРС* (44) *с опорной диаграммой Ферре* $\mathcal{F} = \{\vec{0}\}$ *и системой* $\mathcal{F}$*-унитарных многочленов* $\mathbf{H} = \{x_1 - g_1, \ldots, x_k - g_k\}$. *Цикловой тип этого автомата есть*

$$\mathbf{Z}\mathfrak{R}_g = \mathbb{Z}^k + \frac{q-1}{m} G(g_1, \ldots, g_k), \tag{52}$$

где $m = [d_1, \ldots, d_k]$, $G(g_1, \ldots, g_k) = \{\vec{t} \in \mathbb{Z}^k : g_1^{t_1} \cdot \ldots \cdot g_k^{t_k} = e\}$.

(*c*) *Функция периодов* (12) *рассматриваемого автомата имеет вид*

$$\mathrm{T}\mathfrak{R}_g = y^1 + \frac{q-1}{m} y^m. \tag{53}$$

Доказательство. (*a*) Очевидно, каждая последовательность $u \in L_P(I)$ представляется в виде (51) при $c = u(\vec{0})$, и наоборот.

(*b*) Первое утверждение пункта (*b*) теперь очевидно. Заметим еще, что любая последовательность (51) при любых $\vec{i}, \vec{t} \in \mathbb{Z}^k$ удовлетворяет условию $u(\vec{i} + \vec{t}) = u(\vec{i})\vec{g}^{\vec{t}}$, т. е. $\vec{x}^{\vec{t}} u = \vec{g}^{\vec{t}} u$. Очевидно, что если $c \neq 0$, то для рассматриваемой последовательности справедливы импликации

$$\vec{x}^{\vec{t}} u = u \iff \vec{g}^{\vec{t}} = e \iff \vec{t} \in G(g_1, \ldots, g_k).$$

Следовательно, $\mathfrak{P}(u) = G(g_1, \ldots, g_k)$. Количество таких последовательностей u равно, очевидно, $q-1$, и каждая из них порождает орбиту $\mathcal{O}(u) = \mathcal{R}(u)$ мощности $T(u) = |\mathbb{Z}_k/\mathfrak{P}(u)| = m$. Отсюда следует (52).

(*c*) Равенство (53) следует из (12) и (52) ввиду условия

$$\forall u \in L_P(I) \setminus \{0\} : |\mathcal{O}(u)| = |\mathbb{Z}_k/\mathfrak{P}(u)| = m. \quad \square$$

4.2. Цикловой тип семейства k-арифметических прогрессий

4.2.1. Формулировки основных результатов

Опишем цикловой тип линейного рекурсивного автомата

$$\mathfrak{R}_a = (L_a, \mathbf{x}) \tag{54}$$

со множеством состояний $L_a = L_P((x_1 - e)^2, \ldots, (x_k - e)^2)$ и набором частичных функций перехода $\mathbf{x} = (x_1, \ldots, x_k)$. Напомним, что искомый цикловой тип имеет вид

$$\mathbf{Z}\mathfrak{R}_a = \sum_{u \in L_a} \frac{1}{\operatorname{ind} \mathfrak{P}(u)} \mathfrak{P}(u), \tag{55}$$

где $\mathfrak{P}(u)$ — группа вектор-периодов k-ЛРП u.

По-прежнему предполагается, что $P = \mathrm{GF}(q)$, $q = p^l$, $p = \operatorname{char} P$. Пусть $A = \mathrm{GF}(p)$ — простое подполе поля P. В таком случае $\dim_A P = l$.

Для формулировки основного результата этого раздела введем некоторые обозначения. Для произвольной $(l \times k)$-матрицы C над полем A обозначим через $\mathcal{S}(C)$ подпространство пространства ${}_AA^k$, состоящее из решений системы линейных уравнений $Cx^{\downarrow} = 0^{\downarrow}$.

Заметим, что поле A есть естественный правый $\mathbb{Z}$-модуль, и в рамках этой конструкции можно говорить о подгруппе $\mathcal{S}_{\mathbb{Z}}(C)$ всех решений в $\mathbb{Z}^k$ системы линейных уравнений

$$Cx^{\downarrow} = 0^{\downarrow}. \tag{56}$$

Назовем $(l \times k)$-матрицу K над A *матрицей* (*в форме*) *Гаусса*, или *приведенной ступенчатой* матрицей ранга $r \le l$ [12], если

(a) последние $l - r$ ее строк равны нулю,

(b) каждая из ее первых r строк отлична от нуля,

(c) если $i_1, \ldots, i_r$ — номера первых ненулевых элементов в строках с номерами $1, \ldots, r$ соответственно, то $1 \le i_1 < \ldots < i_r \le k$;

(d) матрица, составленная из столбцов матрицы K с номерами $i_1, \ldots, i_r$, имеет вид $\left(K_{i_1}^{\downarrow}, \ldots, K_{i_r}^{\downarrow}\right) = \left(E_1^{\downarrow}, \ldots, E_r^{\downarrow}\right)$, где $E_s^{\downarrow}$ — s-й столбец единичной $(l \times l)$-матрицы.

Пусть $\mathcal{G}_{l,k}$ — множество всех $(l \times k)$-матриц Гаусса над A и $\mathcal{G}_{l,k}^{(r)}$ — его подмножество, состоящее из всех матриц ранга r, $0 \le r \le m = \min\{l, k\}$. Сформулируем основные результаты этого раздела.

Теорема 4.2. *Цикловой тип семейства k-арифметических прогрессий*

$$L_P((x_1 - e)^2, \ldots, (x_k - e)^2)$$

над полем $P = \mathrm{GF}(p^l)$ имеет вид

$$\mathbf{Z}\mathfrak{R}_a = \mathbb{Z}^k + \sum_{r=1}^{m} \sum_{K \in \mathcal{G}_{l,k}^{(r)}} (p^l - 1)(p^l - p) \ldots (p^l - p^{r-1}) \mathcal{S}_{\mathbb{Z}}(K), m = \min\{l, k\}. \tag{57}$$

Теорема 4.3. *Функция периодов семейства k-арифметических прогрессий*

$$L_P((x_1 - e)^2, \ldots, (x_k - e)^2)$$

имеет вид

$$\mathrm{T}\mathfrak{R}_a(y) = y + \sum_{r=1}^{m} \left(\prod_{i=0}^{r} \frac{(p^l - p^i)(p^k - p^i)}{p^r - p^i} \right) y^{p^r}, \quad m = \min\{l, k\}. \tag{58}$$

4.2.2. Доказательства

Доказательство теоремы 4.2. Заметим, что порожденная элементами $a_1, \ldots, a_t \in P$ подгруппа $\langle a_1, \ldots, a_t \rangle$ группы $(P, +)$ совпадает с подпространством пространства ${}_AP$, порожденным этими элементами, и положим

$$\operatorname{rk}\{a_1, \ldots, a_t\} = \dim_A \langle a_1, \ldots, a_t \rangle, \quad \operatorname{def}\{a_1, \ldots, a_t\} = l - \operatorname{rk}\{a_1, \ldots, a_t\}.$$

Лемма 4.4. *Для любой k-арифметической ЛРП* (48) *справедливы соотношения*

$$p\mathbb{Z}^k \le \mathfrak{P}(u) = \{\mathbf{t} \in \mathbb{Z}^k : a_1 t_1 + \ldots + a_k t_k = 0\}, \tag{59}$$

$$\operatorname{ind} \mathfrak{P}(u) = p^r, \text{ где } r = \operatorname{rk}\{a_1, \ldots, a_k\}. \tag{60}$$

Доказательство. Соотношения (59) легко получаются из условия $\operatorname{char} P = p$ и определения $\mathfrak{P}(u)$.

Докажем (60). Рассмотрим эпиморфизм колец

$$\psi : \mathbb{Z}^k \to A^k \quad \left[\psi(\mathbf{t}) = \psi((t_1, \ldots, t_k)) = (t_1 e, \ldots, t_k e) = \overline{\mathbf{t}}\right].$$

Обозначим образ подгруппы $\mathfrak{P}(u)$ при этом эпиморфизме через $\overline{\mathfrak{P}}(u)$. Заметим, что $\operatorname{Ker} \psi = p\mathbb{Z}^k \le \mathfrak{P}(u)$, поэтому

$$\operatorname{ind} \mathfrak{P}(u) = |A^k : \overline{\mathfrak{P}}(u)| = \frac{p^k}{|\overline{\mathfrak{P}}(u)|}. \tag{61}$$

Зафиксируем базис $\mathbf{e} = (e_1, \ldots, e_l)$ пространства ${}_AP$, и для каждого элемента $a \in P$ через $a^{\downarrow}$ обозначим столбец его координат в этом базисе: $a = \mathbf{e}a^{\downarrow}$. Произвольной системе элементов $\mathbf{a} = (a_1, \ldots, a_k) \in P^k$ поставим в соответствие матрицу

$$C(\mathbf{a}) = \left(a_1^{\downarrow} \ldots a_k^{\downarrow}\right)_{l \times k}. \tag{62}$$

Очевидно, $\operatorname{rk} C(\mathbf{a}) = \operatorname{rk}\{a_1, \ldots, a_k\}$ и $\overline{\mathfrak{P}}(u) = \mathcal{S}(C(\mathbf{a}))$ — пространство решений в A^k системы линейных уравнений

$$C(\mathbf{a})x^{\downarrow} = 0^{\downarrow}. \tag{63}$$

Поэтому $|\overline{\mathfrak{P}}(u)| = p^{\operatorname{def} C(\mathbf{a})}$, и ввиду (61) $\operatorname{ind} \mathfrak{P}(u) = p^r$, где $r = k - \operatorname{def} C(\mathbf{a}) = k - \operatorname{def}\{a_1, \ldots, a_t\} = \operatorname{rk}\{a_1, \ldots, a_t\}$, т. е. верно (60). $\square$

Нетрудно видеть, что для всякой $k-$ЛРП $u \in L_P((x_1 - e)^2, \ldots, (x_k - e)^2)$

$$\overline{\mathfrak{P}}(u) = \mathcal{S}(C(\mathbf{a})) \Leftrightarrow \; = \mathfrak{P}(u) = \psi^{-1}(\mathcal{S}(C(\mathbf{a}))) = \mathcal{S}_{\mathbb{Z}}(C(\mathbf{a})). \tag{64}$$

Пользуясь представлением (48), выражение (55) для циклового типа автомата $\mathfrak{R}_a$ можно преобразовать следующим образом:

$$\mathbf{Z}\mathfrak{R}_a = \sum_{a_0,a_1,\dots,a_k\in P} \frac{1}{\operatorname{ind}\mathcal{S}(C(\mathbf{a}))}\mathcal{S}_{\mathbb{Z}}(C(\mathbf{a})) = \sum_{\mathbf{a}\in A^k} \frac{p}{\operatorname{ind}\mathcal{S}(C(\mathbf{a}))}\mathcal{S}_{\mathbb{Z}}(C(\mathbf{a})). \quad (65)$$

Для того чтобы найти компактный вид суммы в правой части формулы (65), нужно описать все различные члены $\mathcal{S}_{\mathbb{Z}}(C(\mathbf{a}))$ в ней и привести подобные члены. Пользуясь введенными обозначениями, заметим, что ввиду включения (59)

$$\forall\, u, v \in L_P((x_1-e)^2,\dots,(x_k-e)^2)\colon \mathfrak{P}(u) = \mathfrak{P}(v) \Leftrightarrow \overline{\mathfrak{P}}(u) = \overline{\mathfrak{P}}(v), \quad (66)$$

другими словами,

$$\forall\, \mathbf{a}, \boldsymbol{b} \in A^k\colon \mathcal{S}_{\mathbb{Z}}(C(\mathbf{a})) = \mathcal{S}_{\mathbb{Z}}(C(\mathbf{b})) \Leftrightarrow \mathcal{S}(C(\mathbf{a})) = \mathcal{S}(C(\boldsymbol{b})). \quad (67)$$

Таким образом, задача сводится к описанию различных подпространств пространства ${}_AA^k$ вида $\mathcal{S}(C(\mathbf{a}))$.

Так как матрица $C(\mathbf{a})$ строчно эквивалентна единственной матрице Гаусса $K_{l\times k}$ над A, то справедлива следующая лемма.

Лемма 4.5. *Для каждого набора коэффициентов $\mathbf{a} \in A^k$ существует единственная матрица Гаусса $K_{l\times k}$, для которой $\mathcal{S}(C(\mathbf{a})) = \mathcal{S}(K)$ — пространство решений в A^k системы линейных уравнений*

$$Kx^{\downarrow} = 0^{\downarrow}. \quad (68)$$

Для каждой матрицы $K \in \mathcal{G}_{k,l}$ обозначим через $\lambda(K)$ число $(l\times k)$-матриц C над A, строчно эквивалентных матрице K. Тогда из (65) получаем:

$$\mathbf{Z}\mathfrak{R}_a = \sum_{K\in\mathcal{G}_{k,l}} \frac{p\lambda(K)}{\operatorname{ind}\mathcal{S}(K)}\mathcal{S}_{\mathbb{Z}}(K). \quad (69)$$

Коэффициенты последнего разложения подсчитываются явно.

Лемма 4.6. *Если $K_{l\times k}$ — матрица Гаусса ранга r, то*

$$\operatorname{ind}\mathcal{S}(K) = p^r, \quad (70)$$

$$\lambda(K) = \frac{i(l)}{p^{r(l-r)}i(l-r)}, \quad (71)$$

где $i(l) = |A^*_{l,l}|$ — порядок группы обратимых $(l\times l)$-матриц над A.

Доказательство. Если $\operatorname{rk} K = r$, то $\mathcal{S}(K)$ — подгруппа порядка p^{k-r} группы A^k порядка p^k и справедливо (70).

Пусть $I(K)$ — подгруппа группы $|A^*_{l,l}|$, состоящая из всех обратимых матриц U со свойством

$$UK = K. \tag{72}$$

Тогда, очевидно, $\lambda(K) = |A^*_{l,l} : I(K)|$. Нетрудно видеть, что условие (72) выполняется тогда и только тогда, когда

$$U = \begin{pmatrix} E_{r\times r} & C_{r\times(l-r)} \\ 0_{(l-r)\times r} & V_{(l-r)\times(l-r)} \end{pmatrix}, \quad C \in A_{r,(l-r)}, \quad V \in A^*_{(l-r),(l-r)}. \tag{73}$$

Таким образом, $|I(K)| = p^{r(l-r)} i(l-r)$, откуда и следует (71). □

Теперь утверждение теоремы 4.2 легко выводится из (69) и леммы 4.6.

Доказательство теоремы 4.3. Так как для каждой матрицы $K \in \mathcal{G}^{(r)}_{l,k}$ справедливо равенство $\operatorname{ind} \mathcal{S}(K) = p^r$, то из (57) следует равенство

$$\mathrm{T}\mathfrak{R}_a = \mathbb{Z}^k + \sum_{r=1}^{m} (p^l - 1)(p^l - p)\dots(p^l - p^{r-1}) |\mathcal{G}^{(r)}_{l,k}| y^{p^r}. \tag{74}$$

Остается подсчитать мощность множества $\mathcal{G}^{(r)}_{l,k}$.

Заметим, что система из первых r строк матрицы $K \in \mathcal{G}^{(r)}_{l,k}$ порождает подпространство пространства ${}_A A^k$ размерности r, и обратно, любое подпространство размерности r пространства ${}_A A^k$ содержит единственный базис, составляющий систему первых r строк некоторой матрицы $K \in \mathcal{G}^{(r)}_{l,k}$. Таким образом, множество $\mathcal{G}^{(r)}_{l,k}$ равномощно множеству подпространств размерности r пространства ${}_A A^k$:

$$|\mathcal{G}^{(r)}_{l,k}| = \frac{(p^k - 1)(p^k - p)\dots(p^k - p^{r-1})}{(p^r - 1)(p^r - p)\dots(p^r - p^{r-1})}.$$

Отсюда и из (74) следует утверждение теоремы 4.3.

4.3. Цикловой тип семейства k-конгруэнтных последовательностей

Нас интересует цикловой тип семейства (49), т. е. цикловой тип автомата

$$\mathfrak{R}_c = (L_c, \mathbf{x}), \quad L_c = L_P((x_1 - e)(x_1 - g_1), \dots, (x_k - e)(x_k - g_k)), \tag{75}$$

который, согласно (28), имеет вид

$$\mathbf{Z}\mathfrak{R}_c = \sum_{u \in L_c} \frac{1}{\operatorname{ind} \mathfrak{P}(u)} \mathfrak{P}(u) = \sum_{G \in \mathcal{H}_k} c_{\mathfrak{R}_c}(G) G, \tag{76}$$

где $c^M_I(G) \in \mathbb{N}_0$ — число таких орбит $\mathcal{O}(u) \subseteq L_c$, что $\mathfrak{P}(u) = G$.

Здесь дается описание тех элементов $G \in \mathcal{H}_k$, которые входят в разложение (76) с ненулевыми коэффициентами, и вычисляются главные члены этого разложения и соответствующей функции периодов.

4.3.1. Группа вектор-периодов конгруэнтной последовательности

Семейство k-ЛРП вида (49) есть пространство над полем P. Согласно [2, 15], базисом этого пространства является система *биномиальных последовательностей*:

$$\mathbf{e}, \quad u_{i_1\dots i_r}(\mathbf{z}) = g_{i_1}^{z_{i_1}} \dots g_{i_r}^{z_{i_r}}, \quad 1 \le i_1 < \dots < i_r \le k, \quad r \in \{1, \dots, k\}, \qquad (77)$$

где $\mathbf{e} = \mathbf{e}(\mathbf{z})$ — k-последовательность, тождественно равная единице e поля P. Таким образом, любая k-ЛРП $u \in L_c$ однозначно представляется в виде линейной комбинации над полем P:

$$u(\mathbf{z}) = c_0 + \sum_{r=1}^{k} \sum_{1 \le i_1 < \dots < i_r \le k} c_{i_1\dots i_r} u_{i_1\dots i_r}(\mathbf{z}). \qquad (78)$$

Рассмотрим подгруппу

$$\Pi_{i_1\dots i_r} = \Pi_{i_1\dots i_r}(g_1, \dots, g_k) = \{\mathbf{t} = (t_1, \dots, t_k) \in \mathbb{Z}^k : g_{i_1}^{t_{i_1}} \dots g_{i_r}^{t_{i_r}} = e\} \qquad (79)$$

группы $(\mathbb{Z}^k, +)$, и подгруппу $\langle g_{i_1}, \dots, g_{i_r}\rangle$ группы P^*.

Лемма 4.7. *Для биномиальной конгруэнтной последовательности* (77) *справедливы соотношения*

$$\mathfrak{P}(u_{i_1\dots i_r}) = \Pi_{i_1\dots i_r}, \quad \operatorname{ind}\mathfrak{P}(u_{i_1\dots i_r}) = |\langle g_{i_1}, \dots, g_{i_r}\rangle|. \qquad (80)$$

Доказательство. Для любого $\mathbf{t} \in \mathbb{N}_0^k$ справедливо равенство $u_{i_1\dots i_r}(\mathbf{z}+\mathbf{t}) = u_{i_1\dots i_r}(\mathbf{z}) g_{i_1}^{t_{i_1}} \dots g_{i_r}^{t_{i_r}}$, и потому

$$u_{i_1\dots i_r}(\mathbf{z}+\mathbf{t}) = u_{i_1\dots i_r}(\mathbf{z}) \iff \mathbf{t} \in \Pi_{i_1\dots i_r}.$$

Отсюда следует включение $\mathfrak{P}(u_{i_1\dots i_r}) \subseteq \Pi_{i_1\dots i_r}$. Так как ввиду конечности порядков элементов $g_1, \dots, g_k$ группа $\Pi_{i_1\dots i_r}$ порождается своими неотрицательными векторами, то справедливо и обратное включение.

Рассмотрим эпиморфизм групп

$$\xi\colon \mathbb{Z}^k \to \langle g_{i_1}, \dots, g_{i_r}\rangle, \quad [\mathbf{t} \to \xi(\mathbf{t}) = g_{i_1}^{t_{i_1}} \dots g_{i_r}^{t_{i_r}}].$$

Его ядро равно $\Pi_{i_1\dots i_r}$. Отсюда следует второе равенство в (80). $\square$

Определим *носитель* k-конгруэнтной последовательности (78) равенством

$$\mathrm{Sup}(u) = \{(i_1, \ldots, i_r) \colon 1 \le i_1 < \ldots < i_r \le k, r \in \{1, \ldots k\}, c_{i_1 \ldots i_r} \ne 0\}.$$

Лемма 4.8. *Группа вектор-периодов k-последовательности* (78) *имеет вид*

$$\mathfrak{P}(u) = \cap_{(i_1,\ldots,i_r)\in \mathrm{Sup}(u)} \Pi_{i_1 \ldots i_r}. \tag{81}$$

Доказательство. Для любого $\mathbf{t} \in \mathbb{N}_0^k$ справедливо равенство

$$u(\mathbf{z} + \mathbf{t}) = c_0 + \sum_{(i_1,\ldots,i_r)\in \mathrm{Sup}(u)} c_{i_1 \ldots i_r} g_{i_1}^{t_{i_1}} \ldots g_{i_r}^{t_{i_r}} u_{i_1 \ldots i_r}(\mathbf{z}).$$

Сравнивая это с равенством (78), которое можно записать в виде

$$u(\mathbf{z}) = c_0 + \sum_{(i_1,\ldots,i_r)\in \mathrm{Sup}(u)} c_{i_1 \ldots i_r} u_{i_1 \ldots i_r}(\mathbf{z}),$$

и пользуясь линейной независимостью системы последовательностей (77), получаем, что условие $u(\mathbf{z} + \mathbf{t}) = u(\mathbf{z})$ эквивалентно системе условий

$$\mathbf{t} \in \Pi_{i_1 \ldots i_r}, \quad (i_1, \ldots, i_r) \in \mathrm{Sup}(u).$$

Таким образом, верно (81). □

4.3.2. О цикловом типе и функции периодов семейства L_c

Согласно [2, лемма 7.12], множество $\mathcal{H}_k$ есть полугруппа относительно операции пересечения $\cap$. В рассматриваемом случае можно точно указать те подгруппы $G \in \mathcal{H}_k$, которые входят в разложение (8) с ненулевыми коэффициентами.

Обозначим через $\mathcal{H}_k(g_1, \ldots, g_k) = \mathcal{H}_k(\mathbf{g})$ подполугруппу полугруппы $(\mathcal{H}_k, \cap)$, порожденную следующей системой из 2^k элементов:

$$\mathbb{Z}^k, \quad \Pi_{i_1,\ldots,ir}, \quad 1 \le i_1 < \ldots < i_r \le k, \quad r \in \{1, \ldots, k\}. \tag{82}$$

Очевидно, что $\mathcal{H}_k(\mathbf{g})$ — полугруппа порядка, не превосходящего 2^{2^k}.

Теорема 4.9. *Цикловой тип автомата* (75) *имеет вид*

$$\mathbf{Z}_{\mathfrak{R}_c} = \sum_{G\in \mathcal{H}_k(\mathbf{g})} c_{\mathfrak{R}_c}(G) G, \tag{83}$$

причем в этом разложении все коэффициенты отличны от нуля.

Доказательство. По лемме 4.8 группа вектор-периодов каждого состояния u автомата (75) принадлежит $\mathcal{H}_k(\mathbf{g})$, и каждая группа $G \in \mathcal{H}_k(\mathbf{g})$ есть группа вектор-периодов некоторого состояния этого автомата. $\square$

Более точное описание множества $\mathcal{H}_k(\mathbf{g})$ коэффициентов в разложении (83) существенно зависит от выбора элементов $g_1, \ldots, g_k$ и представляет собой предмет самостоятельного исследования. Мы здесь ограничимся лишь оценкой главного члена в этом разложении.

Рассмотрим подгруппу

$$T = T(\mathbf{g}) = \langle d_1 1_1, \ldots, d_k 1_k \rangle \leq \mathbb{Z}^k, \quad d_i = \operatorname{ord} g_i, \quad i \in \{1, \ldots k\}.$$

Заметим, что отношение $\leq$ («быть подгруппой») есть отношение частичного порядка на множестве $\mathcal{H}_k(\mathbf{g})$.

Лемма 4.10. *Полугруппа $(\mathcal{H}_k(\mathbf{g}), \cap)$ есть конечная полугруппа с нулем $T(\mathbf{g})$, который является ее минимальным элементом и удовлетворяет соотношениям*

$$T = \Pi_1 \cap \Pi_2 \cap \ldots \cap \Pi_k, \quad \operatorname{ind} T = d_1 \ldots . d_k. \tag{84}$$

Доказательство. Из (79), леммы 4.8 и определения полугруппы $\mathcal{H}_k(\mathbf{g})$ следует, что каждая группа $G \in \mathcal{H}_k(\mathbf{g})$ содержит каждый из образующих $d_s 1_s$ группы T, и потому $T \leq G$.

Рассмотрим k-ЛРП

$$u(\mathbf{z}) = g_1^{z_1} + \ldots + g_k^{z_k} \in L_P((x_1 - e)(x_1 - g_1), \ldots, (x_k - e)(x_k - g_k)).$$

Для любого $\mathbf{t} \in \mathbb{Z}^k$ справедливо равенство

$$u(\mathbf{z} + \mathbf{t}) = g_1^{t_1} g_1^{z_1} + \ldots + g_k^{t_k} g_k^{z_k}.$$

Отсюда ввиду линейной независимости системы последовательностей (77) имеем

$$\mathbf{t} \in \mathfrak{P}(u) \Leftrightarrow d_1 | t_1, \ldots, d_k | t_k \Leftrightarrow \mathbf{t} \in T.$$

Таким образом, $T = \mathfrak{P}(u) \in \mathcal{H}_k$ — минимальный элемент частично упорядоченного множества $(\mathcal{H}_k, \leq)$, более того, $T = \Pi_1 \cap \ldots \cap \Pi_k$ ввиду леммы 4.8. Последнее равенство в (84) следует из определения группы T. $\square$

Следствие 4.11. *Справедливо соотношение*

$$\forall G \in \mathcal{H}_k \setminus \{T\} \colon \operatorname{ind} G \mid \operatorname{ind} T = d_1 \ldots d_k.$$

Назовем слагаемое $c_{\mathfrak{R}_c}(T)T$ *главным членом* разложения (8).

Теперь, полагая $\tau = d_1 \dots d_k$, функцию периодов автомата $\mathfrak{R}_c$ можно записать в виде

$$\mathrm{T}\mathfrak{R}_c(y) = \sum_{t|\tau} n_{\mathfrak{R}_c}(t) y^t, \tag{85}$$

где $n_{\mathfrak{R}_c}(t)$ — количество орбит мощности t группы подстановок $\langle \widehat{x}_1, \dots, \widehat{x}_k \rangle$ на множестве $L_P(I_c)$. При условии (8)

$$n_{\mathfrak{R}_c}(t) = \sum_{G \in \mathcal{H}_k(\mathbf{g}), \operatorname{ind} G = t} c_{\mathfrak{R}_c}(G). \tag{86}$$

В частности, $n_{\mathfrak{R}_c}(\tau) = c_{\mathfrak{R}_c}(T)$. Мы будем называть слагаемое $n_{\mathfrak{R}_c}(\tau) y^\tau$ *главным членом* разложения (85). Изложенные выше результаты позволяют оценить коэффициент $n_{\mathfrak{R}_c}(\tau)$.

Предложение 4.12. *Имеет место оценка* $n_{\mathfrak{R}_c}(\tau) \geq \frac{(q-1)^k}{\tau} q^{2^k - k}$.

Доказательство. По определению число $\tau n_{\mathfrak{R}_c}(\tau)$ равно числу различных k-ЛРП u вида (78), удовлетворяющих условию $\operatorname{ind} \mathfrak{P}(u) = \tau$. По леммам 4.8, 4.10 и следствию 4.11 этому условию заведомо удовлетворяют последовательности (78), для которых $c_1, c_2, \dots, c_k \in P^*$. Число таких последовательностей равно $(q-1)^k q^{2^k - k}$. Отсюда следует нужное неравенство. □

Следствие 4.13. *При случайном равновероятном выборе последовательности* $u \in L_c$ *вероятность того, что она удовлетворяет условию* $\operatorname{ind} \mathfrak{P}(u) = \tau$, *не меньше* $\left(\frac{q-1}{q}\right)^k$.

Список литературы

1. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. — М.: Гелиос-АРВ, 2002.
2. *Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A.* Linear recurring sequences over rings and modules // J. Math. Sci. — 1995. — V. 76. № 6. — P. 2793–2915.
3. *Кузьмин А. С., Куракин В. Л., Нечаев А. А.* Псевдослучайные и полилинейные последовательности // В сб.: Труды по дискретной математике, т. 1. — М.: ТВП, 1997. — С. 139–202.

4. *Кузьмин А. С., Куракин В. Л., Нечаев А. А.* Свойства линейных и полилинейных рекуррент над кольцами Галуа (I) // В сб.: Труды по дискретной математике, т. 2. — М.: ТВП, 1998. — С. 191–222.
5. *Kurakin V. L., Mikhalev A. V., Nechaev A. A., and Tsypyschev V. N.* Linear and polylinear recurring sequences over abelian groups and modules // J. Math. Sci. — 2000. — V. 102. № 6. — P. 4598–4627.
6. *Кузьмин А. С., Куракин В. Л., Нечаев А. А.* Свойства линейных и полилинейных рекуррент над кольцами Галуа (II) // Обозр. прикл. и промышл. матем. — 2000. — Т. 7. Вып. 1. С. 5–59.
7. *Нечаев А. А.* Конечные квазифробениусовы модули, приложения к кодам и линейным рекуррентам // Фунд. и прикл. матем. — М. : МГУ, 1995. — Т. 1. Вып. 1. — С. 229–254.
8. *Нечаев А. А.* Многомерные регистры сдвига и сложность мультипоследовательностей // В сб.: Труды по дискретной математике, т. 6. — М.: Физматлит, 2002. — С. 150–164.
9. *Кузьмин А. С., Куракин В. Л., Марков В. Т., Михалев А. В., Нечаев А. А.* Линейные рекуррентные последовательности и их приложения // Московский университет и развитие криптографии в России. — М.: МЦНМО, 2003. — С. 122–174.
10. *Нечаев А. А.* Конечные фробениусовы бимодули в теории линейных кодов // В сб.: Труды по дискретной математике, т. 8. — М.: Физматлит, 2004. — С. 187–215.
11. *Нечаев А. А., Горбатов Е. В.* Конечные квазифробениусовы бимодули и полилинейные регистры сдвига // В сб.: Труды по дискретной математике, т. 9. — М.: Физматлит, 2006. — С. 164–189.
12. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра: Учебник. В 2-х т. Т. II. — М.: Гелиос АРВ, 2003.
13. *Каш Ф.* Модули и кольца. — М.: Мир, 1981.
14. *Михалев А. В., Нечаев А. А., Прудников А. В., Староверов М. С., Выдрин А. С.* Полукольца цикловых типов // Фунд. и прикл. матем. — М.: МГУ, 2006. — Т. 12. Вып. 2. — С. 175–192.
15. *Куракин В. Л.* Биномиальная линейная сложность полилинейных последовательностей // В сб.: Труды по дискретной математике, т. 6. — М.: Физматлит, 2002. — С. 82–138.
16. *Козлитин О. А.* 2-линейный регистр сдвига над кольцом Галуа четной характеристики // Математические вопросы криптографии. — 2012. — Т. 3. Вып. 2. — С. 27–61.