Math-Net.Ru

Общероссийский математический портал

Д. А. Михайлов, Унитарные полилинейные регистры сдвига и их периоды, *Дискрет. матем.*, 2002, том 14, выпуск 1, 30–59

DOI: <https://doi.org/10.4213/dm229>

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

Параметры загрузки:

IP: 54.237.206.68

26 апреля 2023 г., 08:51:54

Унитарные полилинейные регистры сдвига и их периоды

© 2002 г. Д. А. Михайлов

В работе изучается введенное ранее понятие k -линейного регистра сдвига (k -ЛРС) над модулем ${}_R M$, где R — коммутативное артиново кольцо с единицей. Такой регистр задается унитарным идеалом $I \triangleleft R[x_1, \dots, x_k]$ и диаграммой Ферре $\mathcal{F} \subset N_0^k$. Описан класс идеалов I , вместе с некоторой диаграммой Ферре задающих k -ЛРС. В частности, построен класс идеалов I , задающих k -ЛРС на фиксированной диаграмме Ферре. Получена нижняя оценка периодов построенных k -ЛРС и показана ее достижимость в некоторых частных случаях.

1. Введение

Напомним некоторые определения из [11]. Всюду далее, если не оговорено обратное, R — коммутативное артиново кольцо с единицей e , ${}_R M$ — левый R -модуль. Для $k \in \mathbb{N}$ произвольная функция $\mu: N_0^k \rightarrow M$ называется k -последовательностью над M . Будем писать $\mu = \mu(\mathbf{z})$, где $\mathbf{z} = (z_1, \dots, z_k)$ вектор независимых переменных на N_0^k . Через $M^{(k)}$ обозначим множество всех k -последовательностей над M . Пусть $\mathcal{R}_k = R[x_1, \dots, x_k]$ — кольцо многочленов от k переменных над R . Для произвольного вектора $\mathbf{s} = (s_1, \dots, s_k) \in N_0^k$ положим $\mathbf{x}^{\mathbf{s}} = x_1^{s_1} \dots x_k^{s_k}$. Тогда произвольный элемент $F(\mathbf{x}) \in \mathcal{R}_k$ имеет вид

$$F(\mathbf{x}) = \sum_{\mathbf{s} \in N_0^k} f_{\mathbf{s}} \mathbf{x}^{\mathbf{s}}.$$

Теперь можно определить операцию умножения k -последовательности μ над M слева на произвольный многочлен

$$F(\mathbf{x}) = \sum_{\mathbf{s} \in N_0^k} f_{\mathbf{s}} \mathbf{x}^{\mathbf{s}} \in \mathcal{R}_k$$

следующим образом:

$$F(\mathbf{x})\mu = \nu$$

где

$$\nu \in M^{(k)}, \quad \nu(\mathbf{z}) = \sum_{\mathbf{s} \in N_0^k} f_{\mathbf{s}} \mu(\mathbf{z} + \mathbf{s}).$$

Рис. 1.

Таким образом, на $M^{(k)}$ задана структура левого $\mathcal{R}_k$ -модуля. Пусть μ — произвольная k -последовательность. Идеал

$$\text{Ann}(\mu) = \{F(\mathbf{x}) \in \mathcal{R}_k : F(\mathbf{x})\mu = 0\} \triangleleft \mathcal{R}_k$$

называется аннулятором последовательности μ . Назовем $\mu \in M^{(k)}$ k -линейно рекуррентной последовательностью, если существуют унитарные многочлены

$$F_1(x_1), \dots, F_k(x_k) \in \mathcal{R}_k$$

(от одной переменной), называемые элементарными, такие, что $F_t(x_t)\mu = 0$ для любого $t = 1, \dots, k$. Идеал $I \triangleleft \mathcal{R}_k$, содержащий такой набор многочленов, называется унитарным.

Для произвольного унитарного идеала $I \triangleleft \mathcal{R}_k$ левый $\mathcal{R}_k$ -подмодуль

$$L_M(I) = \{\mu \in M^{(k)} : I\mu = 0\}$$

модуля $M^{(k)}$ называется k -ЛРП-семейством над M с характеристическим идеалом I . Произвольное конечное подмножество $\mathcal{F} = \{i_1, \dots, i_n\} \subset \mathbf{N}_0^k$ назовем диаграммой Ферре, если для любых двух векторов $\mathbf{i} \in \mathcal{F}$ и $\mathbf{j} \in \mathbf{N}_0^k$ из условия $\mathbf{j} \leq \mathbf{i}$ (покоординатно) следует, что $\mathbf{j} \in \mathcal{F}$.

На рис. 1 приведены примеры диаграмм Ферре. Важным частным случаем диаграммы Ферре является параллелепипед

$$\Pi(m_1, \dots, m_k) = \{0, \dots, m_1 - 1\} \times \dots \times \{0, \dots, m_k - 1\}$$

(рис. 1 (в)). Для $j = 1, \dots, k$ обозначим через $\mathbf{1}_j$ вектор $(0, \dots, 0, 1, 0, \dots, 0)$, в котором 1 стоит на j -ом месте. Множество

$$\Delta\mathcal{F} = \{\mathbf{i} \in \mathbf{N}_0^k \setminus \mathcal{F} \mid \exists t \in \{1, \dots, k\} : \mathbf{i} - \mathbf{1}_t \in \mathcal{F}\}$$

называется границей диаграммы Ферре $\mathcal{F}$. Для произвольных $\mu \in M^{(k)}$ и диаграммы Ферре $\mathcal{F} \subset \mathbf{N}_0^k$ положим $\mu[\mathcal{F}] = (\mu(i_1), \dots, \mu(i_n)) \in M^n$. Скажем, что $\mu[\mathcal{F}]$ — диаграмма значений k -последовательности μ на диаграмме Ферре $\mathcal{F}$.

Пусть $I \triangleleft \mathcal{R}_k$ — унитарный идеал, $\mathcal{F} \subset \mathbf{N}_0^k$ — диаграмма Ферре. В [11, 12] пара $\langle I, \mathcal{F} \rangle$ называется k -линейным (полилинейным) регистром сдвига (k -ЛРС) или $\mathcal{F}$ -ЛРС над ${}_R M$, если для любого вектора $\mathbf{s} \in M^n$ существует единственная k -последовательность $\mu \in L_M(I)$ такая, что $\mu[\mathcal{F}] = \mathbf{s}$. Для данного ЛРС $\langle I, \mathcal{F} \rangle$ над ${}_R M$

будем говорить, что диаграмма $\mathcal{F}$ является его носителем, а идеал I — характеристическим идеалом. В этом случае множество $L_M(I)$ называется семейством выходных последовательностей ЛРС. Полилинейный регистр сдвига можно рассматривать как неавтономный автомат, вырабатывающий заданное семейство полилинейных последовательностей. В параграфе 5 мы поясним данное утверждение. Регистры сдвига называются эквивалентными, если множества их выходных последовательностей совпадают.

Задача построения по унитарному идеалу $I \triangleleft \mathcal{R}_k$ диаграммы Ферре $\mathcal{F} \subset \mathbb{N}_0^k$ такой, что пара $\langle I, \mathcal{F} \rangle$ образует k -ЛРС решалась в [11] и [13]. В [11] для случая, когда идеал I порожден некоторой системой $\{F_i(x_i) \in R[x_i] : i = 1, \dots, k\}$ унитарных многочленов, зависящих от одной переменной, построен параллелепипед $\Pi \subset \mathbb{N}_0^k$ такой, что пара $\langle I, \Pi \rangle$ образует k -ЛРС (в [11] кольцо R даже не обязательно коммутативно). В [13] в случае, когда R есть поле P , данная задача решена для произвольного унитарного идеала $I \triangleleft P[x_1, \dots, x_k]$ с использованием теории базисов Гребнера.

В данной работе для произвольного унитарного идеала $I \triangleleft \mathcal{R}_k$, имеющего стандартный базис (базис Гребнера) специального вида, построена диаграмма Ферре $\mathcal{F} \subset \mathbb{N}_0^k$ такая, что пара $\langle I, \mathcal{F} \rangle$ образует k -ЛРС. Опираясь на данный результат, построены некоторые достаточно широкие классы k -линейных регистров сдвига: унитарные k -ЛРС, призматические k -ЛРС и мономиальные k -ЛРС. В частности, построен класс унитарных идеалов $I \triangleleft \mathcal{R}_k$, задающих k -линейный регистр сдвига на фиксированной диаграмме Ферре. Получены формулы, описывающие периоды построенных k -ЛРС.

Следует отметить, что в [14] и [15] для случаев $R = GF(q)$ и $R = \mathbb{Z}_m$, изучалась конструкция k -LFSR, подобная рассматриваемой нами конструкции k -линейного регистра сдвига, там же указывалась связь k -LFSR и базиса Гребнера полиномиального идеала над полем. Поэтому некоторые результаты данной статьи можно рассматривать как обобщение соответствующих им результатов из [14] на случай коммутативного артинова кольца.

2. Построение k -ЛРС по стандартному базису полиномиального идеала. Унитарные регистры сдвига

В данном параграфе обобщается на случай коммутативного артинова кольца с единицей результат из [13] относительно связи полилинейных регистров сдвига и стандартных базисов идеалов из $\mathcal{R}_k$. Нам потребуются следующие определения (см. [13]).

Пусть $\mathcal{F} \subset \mathbb{N}_0^k$ — некоторая диаграмма Ферре. Множество $\overline{\mathcal{F}} = \mathbb{N}_0^k \setminus \mathcal{F}$ называется дополнением к диаграмме Ферре $\mathcal{F}$. Для каждого $i \in \mathbb{N}_0^k$ назовем k -массивом с начальной точкой i множество

$$\mathcal{P}(i) = \{j \in \mathbb{N}_0^k : i \leq j\}.$$

Будем говорить также, что $\mathcal{P}(i)$ — массив с номером i . Это бесконечный параллелепипед в $\mathbb{N}_0^k$ с единственным минимальным (по отношению $\leq$) элементом i ($\mathcal{P}(i) = i + \mathbb{N}_0^k$). Тогда из определения диаграммы Ферре $\mathcal{F}$ следует, что

(а) если $i \in \overline{\mathcal{F}}$, то $\mathcal{P}(i) \subset \overline{\mathcal{F}}$.

(b) $\overline{\mathcal{F}}$ есть объединение конечного числа k -массивов:

$$\overline{\mathcal{F}} = \bigcup_{i \in \Delta \mathcal{F}} \mathcal{P}(i).$$

Назовем k -массив $\mathcal{P}(i) \subset \overline{\mathcal{F}}$ максимальным в $\overline{\mathcal{F}}$, если для любого $j \in \overline{\mathcal{F}}$

$$\mathcal{P}(i) \subseteq \mathcal{P}(j) \Rightarrow \mathcal{P}(j) = \mathcal{P}(i).$$

Заметим, что если $\mathcal{P}(i)$ — максимальный k -массив в $\overline{\mathcal{F}}$, то $i \in \Delta \mathcal{F}$. Таким образом, в $\overline{\mathcal{F}}$ существует лишь конечное число максимальных k -массивов. Отметим, что каждый k -массив из $\overline{\mathcal{F}}$ принадлежит некоторому максимальному k -массиву из $\overline{\mathcal{F}}$, и дополнение $\overline{\mathcal{F}}$ диаграммы Ферре $\mathcal{F}$ есть объединение своих максимальных k -массивов.

Определение 1. Множеством (внешних) углов диаграммы Ферре $\mathcal{F}$ назовем множество

$$\mathcal{KF} = \{j_1, \dots, j_m\} \subset \mathbb{N}_0^k$$

начальных точек (номеров) максимальных k -массивов из $\overline{\mathcal{F}}$.

Тогда

$$\overline{\mathcal{F}} = \bigcup_{i \in \mathcal{KF}} \mathcal{P}(i). \quad (1)$$

Лемма 1. Пусть $\mathbf{r} = (r_1, \dots, r_k) \in \Delta \mathcal{F}$ и $r_j > 0$ для некоторого $j \in \{1, \dots, k\}$. Тогда $\mathbf{r}' = \mathbf{r} - \mathbf{1}_j$ лежит либо в $\mathcal{F}$, либо в $\Delta \mathcal{F}$.

Следующее предложение дает еще одно описание множества $\mathcal{KF}$.

Предложение 1. Вектор $\mathbf{r} = (r_1, \dots, r_k) \in \Delta \mathcal{F}$ принадлежит $\mathcal{KF}$ тогда и только тогда, когда для любого $j = \{1, \dots, k\}$ такого, что $r_j > 0$ вектор $\mathbf{r}' = \mathbf{r} - \mathbf{1}_j$ принадлежит $\mathcal{F}$.

Если задано некоторое представление множества $\overline{\mathcal{F}}$ в виде объединения k -массивов

$$\overline{\mathcal{F}} = \bigcup_{i \in \mathcal{L}} \mathcal{P}(i),$$

то $\mathcal{KF} \subseteq \mathcal{L}$. Таким образом, (1) — единственное несократимое представление $\overline{\mathcal{F}}$ в виде объединения k -массивов, и любая диаграмма Ферре $\mathcal{F}$ однозначно задается своим множеством углов $\mathcal{KF}$:

$$\mathcal{F} = \mathbb{N}_0^k \setminus \bigcup_{i \in \mathcal{KF}} \mathcal{P}(i).$$

Следствие 1. Множество $\mathcal{KF}$ содержит k векторов вида

$$h_1 \mathbf{1}_1, \dots, h_k \mathbf{1}_k,$$

для некоторых $h_1, \dots, h_k \in \mathbb{N}$.

Доказательство. Пусть вектор $s = (s_1, \dots, s_k) \in \mathcal{F}$ таков, что его i -я координата s_i есть максимум i -х координат всех векторов из $\mathcal{F}$. Так как

$$u_i = (0, \dots, 0, s_i, 0, \dots, 0) \leq s \in \mathcal{F},$$

то $v_i = (0, \dots, 0, s_i + 1, 0, \dots, 0) \in \Delta\mathcal{F}$. Положим $h_i = s_i + 1$. Тогда согласно предложению 1 вектор $v_i = h_i \cdot 1_i$ принадлежит $\mathcal{H}\mathcal{F}$.

В [14, 15] была показана целесообразность использования базисов Гребнера полиномиальных идеалов для построения k -LFSR. Используемая в [5, 11] конструкция k -ЛРС шире k -LFSR, однако, и здесь возможно приложение теории стандартных базисов полиномиальных идеалов. В связи с этим приведем ряд необходимых для дальнейшего изложения определений и результатов, касающихся стандартных базисов (базисов Гребнера) полиномиальных идеалов (см., например, [2]).

Определение 2. Отношение линейного порядка $\preccurlyeq$ на множестве N_0^k называется мономиальным (допустимым), если оно обладает следующими двумя свойствами:

- (1) $0 \preccurlyeq i$ для всех ненулевых i из N_0^k ,
- (2) $s \preccurlyeq t$, то $s + u \preccurlyeq t + u$, для любых u, s, t из N_0^k .

Важными примерами мономиальных отношений на множестве N_0^k являются чисто лексикографическое упорядочение множества N_0^k и упорядочение по полной степени. Напомним, что данные отношения задаются следующим образом: для двух произвольных векторов $i = (i_1, \dots, i_k)$, $j = (j_1, \dots, j_k)$ из N_0^k соотношение $i \preccurlyeq j$ выполняется тогда и только тогда, когда в первом случае первая ненулевая из разностей $j_k - i_k, \dots, j_1 - i_1$ положительна, а во втором случае первая ненулевая из разностей

$$(j_1 + \dots + j_k) - (i_1 + \dots + i_k), j_k - i_k, \dots, j_1 - i_1$$

положительна.

Всюду далее $\preccurlyeq$ — некоторое мономиальное отношение.

Отношение линейного порядка $\preccurlyeq$, заданное на N_0^k , распространим естественным образом на мономы из кольца $\mathcal{R}_k$, полагая $ax^i \preccurlyeq bx^j$, если $a = 0$ или $b \neq 0$ и $i \preccurlyeq j$. При этом для произвольного многочлена A из кольца $\mathcal{R}_k$ будем использовать, следуя [4], следующие обозначения.

Пусть $Lt(A)$ — старшее (относительно $\preccurlyeq$) произведение степеней переменных (терм), входящее в A с ненулевым коэффициентом, $Cf(A, x^i)$ — коэффициент при x^i в многочлене A , $Lc(A)$ — коэффициент при $Lt(A)$ в многочлене A . Если $Lc(A) = e$, то многочлен A называется унитарным (относительно $\preccurlyeq$). По определению положим $Lt(0) = 0$, $Lc(0) = 0$.

Конечное множество

$$\mathcal{F}(A) = \{i \in N_0^k: Cf(A, x^i) \neq 0\}$$

назовем носителем многочлена A . Это множество обозначается также $\text{supp}(A)$. Мы будем использовать более короткое обозначение $\mathcal{F}(A)$. Относительно выбранного упорядочения $\preccurlyeq$ множество $\mathcal{F}(A)$ имеет максимальный элемент, который называется мультистепенью многочлена A и обозначается $\text{mdg } A$. Заметим, что

$$x^{\text{mdg } A} = Lt(A).$$

Определение 3. Будем говорить, что многочлен A редуцируется к многочлену $F \in \mathcal{R}_k$ с помощью многочлена $G \in \mathcal{R}_k$, элемента $b \in R$ и вектора $\mathbf{i} \in \mathbf{N}_0^k$ и писать

$$A \xrightarrow{(G, b, \mathbf{i})} F,$$

если $\text{Cf}(A, \mathbf{x}^{\mathbf{i}} \text{Lt}(G)) = b \text{Lc}(G) \neq 0$ и $F = A - b\mathbf{x}^{\mathbf{i}}G$.

Отметим, что при редуцировании всегда происходит сокращение некоторого монома исходного многочлена. Пусть χ — некоторое конечное подмножество $\mathcal{R}_k$.

Определение 4. Будем говорить, что многочлен A редуцируется к многочлену $F \in \mathcal{R}_k$ по модулю множества χ и писать $A \xrightarrow{\chi} F$, если для некоторого $d \in \mathbf{N}$ найдутся такие многочлены $G_j \in \chi$, $H_j \in \mathcal{R}_k$, элементы $b_j \in R$ и векторы $\mathbf{i}_j \in \mathbf{N}_0^k$, $j = 1, \dots, d$, что

$$A \xrightarrow{(G_1, b_1, \mathbf{i}_1)} H_1 \xrightarrow{(G_2, b_2, \mathbf{i}_2)} H_2 \xrightarrow{(G_3, b_3, \mathbf{i}_3)} \dots \xrightarrow{(G_d, b_d, \mathbf{i}_d)} H_d = F.$$

Определение 5. Будем говорить, что многочлен A является нормальным по модулю множества χ , если не существует такого многочлена H , что $A \xrightarrow{\chi} H$. Через $N(\chi)$ обозначим множество всех многочленов, нормальных по модулю множества χ .

Определение 6. Многочлен H называется нормальной формой многочлена A по модулю χ , если H является нормальным по модулю множества χ и либо $A = H$, либо многочлен A редуцируется по модулю множества χ к многочлену H . Через $NF(A, \chi)$ обозначим множество всех нормальных форм многочлена A по модулю χ .

Для любого многочлена A множество $NF(A, \chi)$ не пусто. Это гарантируется следующим результатом [2, 9, 10].

Лемма 2. Пусть $\chi \subset \mathcal{R}_k$ — некоторое конечное множество, $A \in \mathcal{R}_k$ — произвольный многочлен. Тогда либо A является нормальным по модулю множества χ , либо существует алгоритм редуцирования многочлена A по модулю множества χ , при котором $A \xrightarrow{\chi} H$, где H является нормальным по модулю множества χ .

Определение 7. Конечное множество многочленов $\chi \subset \mathcal{R}_k$ будем называть стандартным базисом идеала $I = \mathcal{R}_k\chi$ относительно мономиального упорядочения $\preccurlyeq$ множества $\mathbf{N}_0^k$, если любой ненулевой многочлен из идеала I редуцируется по модулю множества χ к 0. Стандартный базис χ называется редуцированным, если любой многочлен $G \in \chi$ является нормальным по модулю множества $\chi \setminus \{G\}$. Редуцированный стандартный базис, состоящий из унитарных многочленов, назовем унитарным.

Всюду далее, если не оговорено обратное, $I \triangleleft \mathcal{R}_k$ — унитарный идеал, содержащий элементарные многочлены $F_1(x_1), \dots, F_k(x_k)$ степеней $h_1, \dots, h_k$, соответственно.

Предложение 2. Пусть $I \triangleleft \mathcal{R}_k$ — унитарный идеал и существует унитарный стандартный базис χ идеала I относительно упорядочения $\preccurlyeq$. Тогда существует диаграмма Ферре $\mathcal{F} \subset \mathbf{N}_0^k$ такая, что

$$\mathcal{H}\mathcal{F} = \{\text{mdg } G : G \in \chi\}$$

и базис χ имеет вид

$$\chi = \{G(\mathbf{x}) \in I \mid \text{Lc}(G) = e, \text{mdg } G \in \mathcal{KF}, \mathcal{F}(G) \setminus \{\text{mdg } G\} \subset \mathcal{F}\}, \quad (2)$$

где $\mathcal{KF}$ — множество углов диаграммы Ферре $\mathcal{F}$.

Доказательство. Пусть $B = \{\text{mdg } G : G \in \chi\}$. Так как унитарный стандартный базис χ является редуцированным, конечное множество B состоит из попарно несравнимых по отношению $\leq$ векторов из N_0^k . Положим

$$\mathcal{F} = N_0^k \setminus \bigcup_{i \in B} \mathcal{P}(i). \quad (3)$$

Покажем, что $\mathcal{F}$ — диаграмма Ферре. Так как $F_i(x_i) \in I$ для любого $i = 1, \dots, k$, базис χ содержит многочлен $G(\mathbf{x})$ такой, что $\text{mdg } G = \mathbf{j} \leq (0, \dots, 0, h_i, 0, \dots, 0)$. Отсюда и из попарной несравнимости по отношению $\leq$ векторов из B следует, что для любого $\mathbf{t} = (t_1, \dots, t_k) \in B$ выполняются условия $t_i \leq h_i$, $i = 1, \dots, k$. Тогда $\mathcal{F} \subseteq \mathcal{P}(h_1 + 1, \dots, h_k + 1)$. Пусть $\mathbf{s}, \mathbf{t} \in N_0^k$, $\mathbf{s} \leq \mathbf{t}$ и $\mathbf{s} \notin \mathcal{F}$. Существует $\mathbf{i} \in B$ такой, что $\mathbf{s} \in \mathcal{P}(\mathbf{i})$, а значит, и $\mathbf{t} \in \mathcal{P}(\mathbf{i})$, то есть $\mathbf{t} \notin \mathcal{F}$. Итак $\mathcal{F}$ — действительно диаграмма Ферре.

Покажем, теперь, что множество B есть множество углов диаграммы Ферре $\mathcal{F}$. Для этого ввиду (3) достаточно доказать, что k -массив $\mathcal{P}(\mathbf{s})$ является максимальным в $\overline{\mathcal{F}}$ для любого $\mathbf{s} \in B$. Пусть $\mathbf{s} \in B$, $\mathbf{j} \in \overline{\mathcal{F}} \setminus \{\mathbf{s}\}$. Поскольку

$$\overline{\mathcal{F}} = \bigcup_{i \in B} \mathcal{P}(i),$$

существует $\mathbf{t} \in B$ такой, что $\mathbf{j} \in \mathcal{P}(\mathbf{t})$, а значит, и $\mathcal{P}(\mathbf{j}) \subseteq \mathcal{P}(\mathbf{t})$. Рассмотрим два случая. Если $\mathbf{t} = \mathbf{s}$, то $\mathcal{P}(\mathbf{s}) \not\subseteq \mathcal{P}(\mathbf{j})$, так как $\mathcal{P}(\mathbf{j}) \subseteq \mathcal{P}(\mathbf{s})$ и $\mathbf{j} \neq \mathbf{s}$. Если $\mathbf{t} \neq \mathbf{s}$, то $\mathcal{P}(\mathbf{s}) \not\subseteq \mathcal{P}(\mathbf{j})$, так как $\mathcal{P}(\mathbf{j}) \subseteq \mathcal{P}(\mathbf{t})$ и векторы $\mathbf{t}, \mathbf{s} \in B$ попарно несравнимы по отношению $\leq$. Таким образом, в обоих случаях не выполняется включение $\mathcal{P}(\mathbf{s}) \subseteq \mathcal{P}(\mathbf{j})$, значит, k -массив $\mathcal{P}(\mathbf{s})$ является максимальным в $\overline{\mathcal{F}}$.

В условиях предложения 2 диаграмму Ферре $\mathcal{F}$ будем называть (опорной) диаграммой Ферре базиса χ и обозначать $\mathcal{F}_\chi$. Легко доказать следующее утверждение.

Предложение 3. Многочлен $A \in \mathcal{R}_k$ является нормальным по модулю множества χ вида (2) тогда и только тогда, когда $\mathcal{F}(A) \subseteq \mathcal{F}$.

Следующий результат позволяет использовать теорию стандартных базисов для построения k -ЛРС.

Теорема 1. Пусть I — унитарный идеал в $\mathcal{R}_k$ и существует мономидальное упорядочение $\preceq$ множества N_0^k , относительно которого идеал I имеет унитарный стандартный базис χ с опорной диаграммой Ферре $\mathcal{F} \subset N_0^k$. Тогда пара $\langle I, \mathcal{F} \rangle$ образует регистр сдвига.

Доказательство. Рассмотрим факторкольцо $S = \mathcal{R}_k/I$. Хорошо известно (см., например, [8]), что в случае, когда кольцо R конечно, унитарность идеала I является критерием конечности кольца S . При естественном задании операций сложения элементов из S и внешнего умножения слева элемента из S на элемент кольца R

возникает структура левого R -модуля ${}_R S$. Напомним, что факторкольцо $S = \mathbb{R}_k/I$ имеет представление

$$S = R[\vartheta_1, \dots, \vartheta_k] = \{F(\vartheta) : F(\mathbf{x}) \in \mathbb{R}_k\},$$

где $\vartheta_1 = x_1 + I, \dots, \vartheta_k = x_k + I, \vartheta = (\vartheta_1, \dots, \vartheta_k)$. Легко видеть (см., например, теорему 2.3 в [13]), что для доказательства теоремы достаточно показать, что множество $\Omega = \{\vartheta^i : i \in \mathcal{F}\}$ есть линейно независимая система образующих модуля ${}_R S$.

Покажем, что Ω — линейно независимая система. Допустим, что существует набор $h[\mathcal{F}]$ из $R^{|\mathcal{F}|}$ такой, что

$$\sum_{j \in \mathcal{F}} h_j \vartheta^j = 0.$$

Последнее равенство равносильно наличию в идеале I многочлена

$$H = \sum_{j \in \mathcal{F}} h_j \mathbf{x}^j. \quad (4)$$

Согласно предложению 3 многочлен H является нормальным по модулю χ . Поэтому из определения 7 следует, что многочлен H может быть только нулевым. Значит, Ω — линейно независимая система.

Покажем, что Ω является системой образующих модуля ${}_R S$. Пусть $i \in \overline{\mathcal{F}}$ и $H_i \in NF(\mathbf{x}^i, \chi)$. Тогда согласно предложению 3 выполняется включение $\mathcal{F}(H_i) \subseteq \mathcal{F}$, то есть многочлен H_i имеет вид (4). Так как $\mathbf{x}^i - H_i \in I$, то $\vartheta^i - H_i(\vartheta) = 0$ и

$$\vartheta^i = \sum_{j \in \mathcal{F}} h_j \vartheta^j.$$

Таким образом, пара $\langle I, \mathcal{F} \rangle$ образует k -ЛРС.

Полилинейный регистр сдвига $\langle I, \mathcal{F} \rangle$ назовем унитарным, если существует мономиальное упорядочение множества $\mathbf{N}_0^k$, относительно которого идеал I имеет унитарный стандартный базис χ такой, что $\mathcal{F}_\chi = \mathcal{F}$. Другими словами, унитарный регистр сдвига — это регистр, который может быть построен с помощью теоремы 1.

Далее мы приведем пример, показывающий, что существуют не унитарные k -ЛРС. Напомним некоторые определения из [11]. Пусть $\mathcal{F} \subset \mathbf{N}_0^k$ — диаграмма Ферре. Система многочленов вида

$$\Phi = \left\{ H_i = \mathbf{x}^i - \sum_{j \in \mathcal{F}} h_{i,j} \mathbf{x}^j \in \mathbb{R}_k : i \in \Delta \mathcal{F} \right\}$$

называется полной системой $\mathcal{F}$ -унитарных многочленов. Множеству многочленов Φ соответствует система k эндоморфизмов $\Phi_1, \dots, \Phi_k$ модуля ${}_R M^{|\mathcal{F}|}$, определяемых следующим образом. Пусть $t \in \{1, \dots, k\}$, тогда для любого набора

$$\delta[\mathcal{F}] = (\delta(i_1), \dots, \delta(i_n)) \in M^{|\mathcal{F}|}$$

полагаем

$$\Phi_t(\delta[\mathcal{F}]) = \lambda_t[\mathcal{F}] \in M^{|\mathcal{F}|}, \quad (5)$$

где для любого вектора $i \in \mathcal{F}$

$$\lambda_t(i) = \begin{cases} \delta(i + 1_t), & \text{если } i + 1_t \in \mathcal{F}, \\ \sum_{j \in \mathcal{F}} h_{i+1_t, j} \delta(j), & \text{если } i + 1_t \in \Delta \mathcal{F}. \end{cases}$$

Эти эндоморфизмы называются сопровождающими для системы многочленов Φ . Пусть унитарный идеал $I \triangleleft \mathcal{R}_k$ порожден множеством многочленов Φ . Тогда согласно критерию, предложенному в [11], для доказательства того факта, что пара $\langle I, \mathcal{F} \rangle$ есть k -ЛРС, достаточно показать попарную перестановочность сопровождающих эндоморфизмов $\Phi_1, \Phi_2, \dots, \Phi_k$ модуля ${}_R M^{|\mathcal{F}|}$.

Пример 1. Пусть $R = GF(2)$, $k = 2$, множество

$$\mathcal{F} = \{(0, 0), (0, 1), (1, 0), (0, 2), (2, 0)\}$$

— диаграмма Ферре (см. рис. 1 (б)),

$$\Delta \mathcal{F} = \{(3, 0), (2, 1), (1, 1), (1, 2), (0, 3)\}$$

— граница диаграммы Ферре $\mathcal{F}$, $\mathcal{H}\mathcal{F} = \{(3, 0), (1, 1), (0, 3)\}$ — множество углов диаграммы Ферре $\mathcal{F}$, $\Phi = \{F_r: r \in \Delta \mathcal{F}\}$ — полная система $\mathcal{F}$ -унитарных многочленов,

$$\chi = \{F \in \Phi: \text{mdg } F \in \mathcal{H}\mathcal{F}\}, \quad I = \mathcal{R}_2 \Phi,$$

многочлены

$$\begin{aligned} F_{(3,0)} &= x_1^3 + x_1^2, \\ F_{(2,1)} &= x_1^2 x_2 + x_1^2 + x_2^2, \\ F_{(1,1)} &= x_1 x_2 + x_1^2 + x_2^2, \\ F_{(1,2)} &= x_1 x_2^2 + x_2^2, \\ F_{(0,3)} &= x_2^3 + x_1^2 \end{aligned}$$

составляют систему Φ . Тогда I — унитарный идеал и пара $\langle I, \mathcal{F} \rangle$ есть k -ЛРС, причем не существует допустимого упорядочения множества N_0^2 , относительно которого множество χ является унитарным стандартным базисом (редуцированным базисом Гребнера) идеала I .

Покажем, что I — унитарный идеал. Так как I содержит унитарный многочлен $F_{(3,0)} = x_1^3 + x_1^2$, достаточно показать, что в I существует некоторый унитарный многочлен $F(x_2)$, зависящий лишь от x_2 . Пусть

$$F(x) = F_{(1,2)} + x_2(F_{(1,1)} + F_{(0,3)}).$$

Тогда $F(x) = x_2^2(x_2^2 + x_2 + 1)$, то есть I — унитарный идеал.

Пусть $u(0, 0), \dots, u(0, 2)$ — произвольные элементы модуля M . Тогда сопровождающие эндоморфизмы Φ_1 и Φ_2 выглядят следующим образом:

$$\begin{aligned} \Phi_1(u(0, 0), \dots, u(0, 2)) &= (u(1, 0), u(2, 0), u(2, 0), u(0, 2) + u(2, 0), u(0, 2)), \\ \Phi_2(u(0, 0), \dots, u(0, 2)) &= (u(0, 1), u(0, 2) + u(2, 0), u(0, 2) + u(2, 0), u(0, 2), u(2, 0)). \end{aligned}$$

Проверим перестановочность данных эндоморфизмов. Нетрудно видеть, что

$$\begin{aligned}\Phi_1(\Phi_2(u(0,0), \dots, u(0,2))) \\ = (u(0,2) + u(2,0), u(0,2) + u(2,0), u(0,2) + u(2,0), u(0,2), u(2,0)),\end{aligned}$$

и

$$\begin{aligned}\Phi_2(\Phi_1(u(0,0), \dots, u(0,2))) \\ = (u(0,2) + u(2,0), u(0,2) + u(2,0), u(0,2) + u(2,0), u(0,2), u(2,0)),\end{aligned}$$

то есть эндоморфизмы Φ_1 и Φ_2 перестановочны, а значит, пара $\langle I, \mathcal{F} \rangle$ есть 2-ЛРС.

Пусть $\preccurlyeq$ — некоторое допустимое отношение на N_0^2 . Покажем, что $\text{Lt}(F_{(1,1)})$ не равно x_1x_2 . Так как $\preccurlyeq$ есть линейное упорядочение, то либо $(1,0) \preccurlyeq (0,1)$, либо $(0,1) \preccurlyeq (1,0)$. Пусть $(1,0) \preccurlyeq (0,1)$. Согласно определению 2, выполняется импликация

$$(1,0) \preccurlyeq (0,1) \Rightarrow (1,1) \preccurlyeq (0,2),$$

то есть $x_1x_2 \preccurlyeq x_2^2$, значит, $\text{Lt}(F_{(1,1)}) \neq x_1x_2$. Аналогично рассматривается ситуация $(0,1) \preccurlyeq (1,0)$. Итак, $\text{Lt}(F_{(1,1)})$ равен x_1^2 или x_2^2 , а значит, система χ не является унитарным стандартным базисом (редуцированным базисом Гребнера) идеала I .

Рассмотрим еще один регистр сдвига.

Пример 2. Пусть $R = GF(2)$, $k = 2$, множество

$$\mathcal{F}' = \{(0,0), (0,1), (1,0), (0,2), (1,1)\}$$

есть диаграмма Ферре (см. рис. 2),

$$\Delta\mathcal{F}' = \{(3,0), (2,1), (1,2), (0,2)\}$$

— граница диаграммы Ферре $\mathcal{F}'$, $\mathcal{K}\mathcal{F}' = \{(3,0), (2,1), (0,2)\}$ — множество углов диаграммы Ферре $\mathcal{F}'$, $\Phi' = \{G_r : r \in \Delta\mathcal{F}'\}$ — полная система $\mathcal{F}'$ -унитарных многочленов,

$$\chi' = \{G \in \Phi' : \text{mdg } G \in \mathcal{K}\mathcal{F}'\}, \quad I' = \mathcal{R}_2\Phi',$$

многочлены

$$\begin{aligned}G_{(3,0)} &= x_1^3 + x_1^2, \\ G_{(2,1)} &= x_1^2x_2 + x_1x_2, \\ G_{(1,2)} &= x_1x_2^2 + x_1^2 + x_1x_2, \\ G_{(0,2)} &= x_2^2 + x_1^2 + x_1x_2\end{aligned}$$

составляют систему Φ' .

Тогда I' — унитарный идеал и пара $\langle I', \mathcal{F}' \rangle$ есть k -ЛРС, эквивалентный регистру $\langle I, \mathcal{F} \rangle$ из примера 1, причем множество $\chi' = \{G_{(3,0)}, G_{(2,1)}, G_{(0,2)}\}$ является редуцированным базисом Гребнера идеала $I' = I$ при чисто лексикографическом упорядочении множества N_0^2 .

Рис. 2.

Покажем, что $I' = I$. Для этого достаточно выразить все многочлены из χ через множество χ' и наоборот. Легко заметить, что

$$\begin{aligned}
 G_{(3,0)} &= F_{(3,0)}, \\
 G_{(2,1)} &= F_{(2,1)} + F_{(1,1)}, \\
 G_{(1,2)} &= F_{(1,1)} + F_{(1,2)}, \\
 G_{(0,2)} &= F_{(0,2)}, \\
 F_{(3,0)} &= G_{(3,0)}, \\
 F_{(2,1)} &= G_{(2,1)} + G_{(0,2)}, \\
 F_{(1,1)} &= G_{(0,2)}, \\
 F_{(1,2)} &= G_{(1,2)} + G_{(0,2)}, \\
 F_{(0,3)} &= x_2 G_{(0,2)} + G_{(2,1)} + G_{(1,2)}.
 \end{aligned}$$

Таким образом, идеалы I' и I совпадают.

Так как верно равенство $G_{(1,2)} = x_1 G_{(0,2)} + G_{(3,0)} + G_{(2,1)}$, идеал I порождается системой многочленов χ' .

Докажем теперь, что χ' является редуцированным базисом Гребнера идеала $I = \mathfrak{R}_2 \chi'$. Для этого стандартным образом покажем редуцируемость к 0 по модулю множества χ' всех трех возможных S -полиномов:

$$\begin{aligned}
 SP(G_{(3,0)}, G_{(2,1)}) &= x_1^3 x_2 + x_1^2 x_2 + x_1^3 x_2 + x_1^2 x_2 = 0, \\
 SP(G_{(3,0)}, G_{(0,2)}) &= x_1^3 x_2^2 + x_1^2 x_2^2 + x_1^3 x_2^2 + x_1^5 + x_1^4 x_2 \\
 &= x_2(G_{(2,1)} + x_1 x_2) + x_1^5 + x_1^4 x_2 \\
 &= x_2 G_{(2,1)} + x_1 G_{(0,2)} + x_1^3 + x_1^2 x_2 + x_1^5 + x_1^4 x_2 \\
 &= x_2 G_{(2,1)} + x_1 G_{(0,2)} + x_1^2 G_{(2,1)} + x_1^3 x_2 + x_1^3 + x_1^2 x_2 + x_1^5 \\
 &= x_2 G_{(2,1)} + x_1 G_{(0,2)} + x_1^2 G_{(2,1)} + x_1 G_{(2,1)} + x_1^5 + x_1^3 \\
 &= x_2 G_{(2,1)} + x_1 G_{(0,2)} + x_1^2 G_{(2,1)} + x_1 G_{(2,1)} + (x_1^2 + x_1) G_{(3,0)}, \\
 SP(G_{(2,1)}, G_{(0,2)}) &= x_1^2 x_2^2 + x_1 x_2^2 + x_1^2 x_2^2 + x_1^4 + x_1^3 x_2 \\
 &= x_1 G_{(0,2)} + x_1^3 + x_1^2 x_2^2 + x_1^4 + x_1^3 x_2 \\
 &= x_1 G_{(0,2)} + x_1 G_{(2,1)} + x_1^3 + x_1^4 \\
 &= x_1 G_{(0,2)} + x_1 G_{(2,1)} + x_1 G_{(3,0)}.
 \end{aligned}$$

Итак, все S -полиномы редуцируются к 0 по модулю множества χ' , значит, χ' —

редуцированный базис Гребнера идеала I . Тогда согласно теореме 1 пара $\langle I, \mathcal{F}' \rangle$ есть 2-ЛРС.

3. Один способ увеличения размерности k -ЛРС

В данном параграфе описан простой способ построения по исходному унитарному k -ЛРС унитарного регистра сдвига более высокой размерности.

Пусть $\preccurlyeq$ — некоторое отношение линейного порядка на множестве $\mathbf{N}_0^{k+t}$, $t > 0$. Линейное отношение $\preccurlyeq'$, заданное на $\mathbf{N}_0^k$ соотношением

$$\forall i, j \in \mathbf{N}_0^k (i \preccurlyeq' j) \iff ((i, 0) \preccurlyeq (j, 0)),$$

где $(i, 0), (j, 0) \in \mathbf{N}_0^{k+t}$, назовем ограничением отношения $\preccurlyeq$ на первые k координат. Аналогичным образом можно определить ограничение отношения $\preccurlyeq$ на произвольные k координат.

Для произвольного $A(\mathbf{x}) \in \mathcal{R}_k$ и унитарного $G(x_i) \in R[x_i]$, $i \in \{1, k\}$ естественным образом определим остаток от деления $\text{Res}(A(\mathbf{x})/G(x_i))$ многочлена $A(\mathbf{x})$ на $G(x_i)$. Многочлен $A(\mathbf{x})$ можно представить в виде

$$A = \sum_{\mathbf{j}=(j_1, \dots, j_{i-1}, j_{i+1}, \dots, j_k) \in \mathbf{N}_0^{k-1}} x_1^{j_1} \dots x_{i-1}^{j_{i-1}} x_{i+1}^{j_{i+1}} \dots x_k^{j_k} A_{\mathbf{j}}(x_i),$$

где $A_{\mathbf{j}}(x_i) \in R[x_i]$ для каждого $\mathbf{j} \in \mathbf{N}_0^{k-1}$. Положим

$$\begin{aligned} & \text{Res}(A(\mathbf{x})/G(x_i)) \\ &= \sum_{\mathbf{j}=(j_1, \dots, j_{i-1}, j_{i+1}, \dots, j_k) \in \mathbf{N}_0^{k-1}} x_1^{j_1} \dots x_{i-1}^{j_{i-1}} x_{i+1}^{j_{i+1}} \dots x_k^{j_k} \text{res}(A_{\mathbf{j}}(x_i)/G(x_i)), \end{aligned}$$

где $\text{res}(A_{\mathbf{j}}(x_i)/G(x_i))$ — остаток от деления в $R[x_i]$ многочлена $A_{\mathbf{j}}(x_i)$ на $G(x_i)$. Не сложно заметить, что для любого $A(\mathbf{x}) \in \mathcal{R}_k$ и унитарного $G(x_i) \in R[x_i]$ остаток $\text{Res}(A(\mathbf{x})/G(x_i))$ существует, однозначно определен и в случае $A(\mathbf{x}) \in R[x_i]$ совпадает с обычным остатком от деления данных многочленов в $R[x_i]$.

Лемма 3. Пусть $I' \triangleleft \mathcal{R}_k$ — унитарный идеал, χ' — унитарный стандартный базис идеала I' относительно некоторого мономиального упорядочения $\preccurlyeq'$ множества $\mathbf{N}_0^k$, $G_{k+1}(x) \in R[x]$ — некоторый унитарный многочлен, $\preccurlyeq$ — мономиальное упорядочение множества $\mathbf{N}_0^{k+1}$ такое, что отношение $\preccurlyeq'$ есть ограничение $\preccurlyeq$ на первые k координат. Тогда множество $\chi = \chi' \cup \{G_{k+1}(x_{k+1})\}$ есть унитарный стандартный базис идеала $I = \mathcal{R}_{k+1}\chi \triangleleft \mathcal{R}_{k+1}$ относительно упорядочения $\preccurlyeq$.

Доказательство. Пусть $\preccurlyeq$ — мономиальное упорядочение множества $\mathbf{N}_0^{k+1}$ такое, что отношение $\preccurlyeq'$ есть ограничение $\preccurlyeq$ на первые k координат. Такое отношение $\preccurlyeq$ найдется для любого $\preccurlyeq'$, поскольку, например, мономиальным на $\mathbf{N}_0^{k+1}$ является следующее отношение ϱ (см. [10]):

$$\begin{aligned} & \forall i = (i_1, \dots, i_{k+1}), j = (j_1, \dots, j_{k+1}) \in \mathbf{N}_0^{k+1} \\ & (i \varrho j) \iff ((i_{k+1} < j_{k+1}) \text{ или } (i_{k+1} = j_{k+1} \text{ и } (i_1, \dots, i_k) \preccurlyeq' (j_1, \dots, j_k))). \end{aligned}$$

Рассмотрим произвольный многочлен $G \in \chi$. Очевидно, что многочлен G является нормальным по модулю множества $\chi \setminus \{G\}$ и $\text{Lc}(G) = e$. Пусть $\deg(G_{k+1}) = h_{k+1}$, $\mathcal{F}' \subset \mathbf{N}_0^k$ — диаграмма Ферре базиса χ' . Несложно заметить, что множество $\mathcal{F} = \mathcal{F}' \times \{0, 1, \dots, h_{k+1} - 1\} \subset \mathbf{N}_0^{k+1}$ есть диаграмма Ферре, причем

$$\mathcal{H}\mathcal{F} = \{\mathcal{H}\mathcal{F}' \times \{0\}\} \cup \{(0, h_{k+1})\} = \{\text{mdg } G : G \in \chi\}.$$

Покажем, что любой ненулевой многочлен $F(\mathbf{x}) \in I$ редуцируется по модулю множества χ к 0. Согласно лемме 2 существует $H \in NF(F, \chi)$. Допустим, что $H \neq 0$. Из предложения 3 следует, что многочлен H имеет вид

$$H(\mathbf{x}) = \sum_{i \in \mathcal{F}} h_i \mathbf{x}^i. \quad (6)$$

Тогда справедливо равенство

$$H(\mathbf{x}) = \text{Res}(H(\mathbf{x})/G_{k+1}(x_{k+1})). \quad (7)$$

Пусть $l = \deg_{x_{k+1}}(H)$ — степень многочлена H по переменной x_{k+1} . Тогда (6) можно переписать следующим образом:

$$H(\mathbf{x}) = \sum_{i=0}^l H^{(i)}(x_1, \dots, x_k) x_{k+1}^i, \quad (8)$$

где $H^{(i)}(x_1, \dots, x_k)$, $i = 0, 1, \dots, l$, — соответствующие многочлены, зависящие от первых k переменных. Заметим, что $H_l \neq 0$. Пусть $\chi' = \{G_i : i \in \mathcal{H}\mathcal{F}'\}$. Так как $F \in I$ и $I = \mathcal{R}_{k+1}\chi$, то $NF(F, \chi) \subset I$ и многочлен H имеет следующее представление:

$$H(\mathbf{x}) = \sum_{i \in \mathcal{H}\mathcal{F}'} G_i(x_1, \dots, x_k) K_i(\mathbf{x}) + G_{k+1}(x_{k+1}) L_{k+1}(\mathbf{x}), \quad (9)$$

для соответствующих многочленов $K_i, L_{k+1} \in \mathcal{R}_{k+1}$. Отсюда и из (7) следует, что

$$H(\mathbf{x}) = \sum_{i \in \mathcal{H}\mathcal{F}'} G_i(x_1, \dots, x_k) L_i(\mathbf{x}), \quad (10)$$

где $L_i(\mathbf{x}) = \text{Res}(K_i/G_{k+1})$, $i \in \mathcal{H}\mathcal{F}'$. Для любого $i \in \mathcal{H}\mathcal{F}'$ многочлен L_i можно представить в виде

$$L_i = \sum_{j=0}^{\deg_{x_{k+1}}(L_i)} L_i^{(j)}(x_1, \dots, x_k) x_{k+1}^j.$$

Тогда из (8) и (10) следует, что

$$H^{(l)}(x_1, \dots, x_k) = \sum_{i \in \mathcal{H}\mathcal{F}'} G_i(x_1, \dots, x_k) L_i^{(l)}(x_1, \dots, x_k). \quad (11)$$

Отсюда видно, что $H^{(l)} \in \mathcal{R}_k \chi' = I'$. Тогда ненулевой многочлен $H^{(l)}$ редуцируется к 0 по модулю множества χ' , то есть он не является нормальным по модулю множества χ' , что согласно предложению 3 равносильно существованию $\bar{i} \in \bar{\mathcal{F}}' \subset \mathbf{N}_0^k$ такого, что $\text{Cf}(H^{(l)}, \mathbf{x}^{\bar{i}}) \neq 0$. Заметим, что $\bar{\mathcal{F}}' \times \{l\} \subset \bar{\mathcal{F}}$. Тогда $(\bar{i}, l) \in \bar{\mathcal{F}}$ и $\text{Cf}(H, \mathbf{x}^{\bar{i}} x_{k+1}^l) = \text{Cf}(H^{(l)}, \mathbf{x}^{\bar{i}}) \neq 0$, то есть согласно предложению 3 многочлен H не является нормальным по модулю множества χ . Получаем противоречие с условием $H \in N(\chi)$, значит, $H = 0$.

Таким образом, множество χ является стандартным базисом идеала I .

Рис. 3.

Предлагается следующий способ построения унитарных $k + t$ -ЛРС по имеющемуся унитарному k -ЛРС, основанный на лемме 3.

Способ 1. Пусть $\chi_k \subset \mathcal{R}_k$ — унитарный стандартный базис унитарного идеала I' относительно некоторого мономиального упорядочения $\preceq'$ множества $\mathbf{N}_0^k$, $F_{k+1}(x), \dots, F_{k+t}(x)$ — набор t унитарных многочленов из $R[x]$. Из леммы 3 следует, что множество

$$\chi = \chi_k \cup \{F_{k+1}(x_{k+1}), \dots, F_{k+t}(x_{k+t})\} \subset \mathcal{R}_{k+t}$$

есть унитарный стандартный базис идеала $I = \mathcal{R}_{k+t}\chi \triangleleft \mathcal{R}_{k+t}$ относительно некоторого мономиального упорядочения $\preceq$ множества $\mathbf{N}_0^{k+t}$ такого, что отношение $\preceq'$ является ограничением $\preceq$ на первые k координат. Пусть $\mathcal{F} \subset \mathbf{N}_0^{k+t}$ — диаграмма Ферре базиса χ . Тогда согласно теореме 1, пара $\langle I, \mathcal{F} \rangle$ образует $(k + t)$ -ЛРС.

Назовем унитарный стандартный базис χ унитарного идеала I призматическим с основанием размерности t или просто призматическим, если с точностью до переименования переменных базис χ имеет вид

$$\chi = \chi_t \cup \{F_{t+1}(x_{t+1}), \dots, F_k(x_k)\},$$

где $\chi_t \subset R[x_1, \dots, x_t]$ и $t = \{1, \dots, k-1\}$ выбрано минимально возможным. Согласно теореме 1 пара $\langle I, \mathcal{F} \rangle$ образует унитарный k -ЛРС, который мы будем называть призматическим. Другими словами, призматический регистр сдвига — это унитарный регистр сдвига, который может быть построен из некоторого унитарного регистра сдвига меньшей размерности с помощью Способа 1.

Заметим, что в случае $k = 2$ диаграмма Ферре произвольного призматического регистра сдвига представляет собой параллелепипед, а в случае $k = 3$ призму (см. рис. 3).

В следующем параграфе мы приведем пример призматического регистра сдвига, имеющего диаграмму Ферре, изображенную на рис. 3.

4. Некоторые классы полилинейных регистров сдвига

В данном параграфе вводятся два класса полилинейных регистров сдвига: правильные и мономиальные k -ЛРС и, в частности, дается положительный ответ на вопрос о существовании для произвольной диаграммы Ферре $\mathcal{F}$ регистра сдвига с носителем на данной диаграмме $\mathcal{F}$.

Введем понятие правильного k -ЛРС. Назовем унитарный стандартный базис χ унитарного идеала I правильным, если χ содержит систему из k многочленов $F_1(x_1), \dots, F_k(x_k)$, каждый из которых зависит только от одной переменной. Обозначим через $\mathcal{F}$ диаграмму Ферре базиса χ . Согласно теореме 1 пара $\langle I, \mathcal{F} \rangle$ образует k -ЛРС, который мы будем называть правильным. Ниже мы выделим важный подкласс правильных регистров сдвига — мономиальные k -ЛРС, и для произвольной диаграммы Ферре $\mathcal{F} \subset \mathbf{N}_0^k$ докажем существование мономиального k -ЛРС с носителем на данной диаграмме $\mathcal{F}$.

Сначала определим мономиальный в узком смысле полилинейный регистр сдвига. Напомним, что идеал, имеющий систему образующих, состоящую из мономов, называется мономиальным. Пусть $\mathcal{F} \subset \mathbf{N}_0^k$ — диаграмма Ферре, $\mathcal{KF}$ — ее множество углов, $\chi = \{\mathbf{x}^{\mathbf{i}} : \mathbf{i} \in \mathcal{KF}\}$, $I = \mathcal{R}_k \chi$. Рассмотрим пару $\langle I, \mathcal{F} \rangle$. Заметим, что любая k -последовательность $\mu \in L_M(I)$ обладает следующим свойством: $\mu(\mathbf{i}) = 0$ для любого $\mathbf{i} \in \overline{\mathcal{F}}$. Поэтому можно установить следующее взаимно однозначное соответствие ϕ между множествами $M^{|\mathcal{F}|}$ и $L_M(I)$:

$$\forall \delta \in M^{|\mathcal{F}|} \quad \phi(\delta) = \mu \in L_M(I) : \mu[\mathcal{F}] = \delta.$$

Значит, пара $\langle I, \mathcal{F} \rangle$ есть k -ЛРС. Такой регистр сдвига мы назовем мономиальным в узком смысле.

Определим мономиальный в широком смысле полилинейный регистр сдвига. Пусть $\mathcal{F} \subset \mathbf{N}_0^k$ — диаграмма Ферре с множеством углов $\mathcal{KF}$. Для $i = 1, \dots, k$ пусть D_i — множество различных значений i -х координат r_i строк $\mathbf{r} \in \mathcal{KF}$. Каждому $v \in D_i$ поставим в соответствие унитарный многочлен $F_v^{(i)}(x_i) \in \mathcal{R}_k$ степени $\deg F_v^{(i)}(x_i) = v$ так, чтобы совокупность получившихся многочленов

$$C_i = \{F_v^{(i)}(x_i) : v \in D_i\}$$

удовлетворяла условию

$$\forall v_1, v_2 \in D_i \quad (v_1 < v_2) \Rightarrow (F_{v_1}^{(i)}(x_i) \mid F_{v_2}^{(i)}(x_i)).$$

Для $i = 1, \dots, k$ через h_i обозначим максимальный элемент из D_i , а через l_i — минимальный. Отметим, что числа $h_1, \dots, h_k$ те же, что и в следствии 1.

Пользуясь множествами $C_1, \dots, C_k$ каждому вектору $\mathbf{r} = (r_1, \dots, r_k)$ из $\mathcal{KF}$ поставим в соответствие многочлен

$$F_{\mathbf{r}}(\mathbf{x}) = F_{r_1}^{(1)}(x_1) F_{r_2}^{(2)}(x_2) \dots F_{r_k}^{(k)}(x_k), \quad (12)$$

где для любого $i = 1, \dots, k$ многочлен $F_{r_i}^{(i)}(x_i)$ принадлежит множеству C_i .

Систему многочленов

$$\chi = \{F_{\mathbf{r}} : \mathbf{r} \in \mathcal{KF}\} \quad (13)$$

назовем согласованным с диаграммой Ферре $\mathcal{F}$ множеством мономиальных многочленов. Рассмотрим идеал

$$I = \mathcal{R}_k \chi. \quad (14)$$

Предложение 4. *Идеал I является унитарным.*

Доказательство. Согласно следствию 1 множество углов диаграммы Ферре $\mathcal{F}$ содержит векторы $h_1 \mathbf{1}_1, \dots, h_k \mathbf{1}_k$. Поэтому по построению множество χ содержит унитарные многочлены $F_{h_1}^{(1)}(x_1), \dots, F_{h_k}^{(k)}(x_k)$.

Согласно теореме 1 для доказательства того, что пара $\langle I, \mathcal{F} \rangle$ образует k -ЛРС, достаточно показать, что χ есть унитарный стандартный базис идеала I относительно некоторого мономиального упорядочения $\preccurlyeq$ множества N_0^k .

Теорема 2. *Множество χ является унитарным стандартным базисом идеала $I = \mathcal{R}_k \chi$ относительно любого мономиального упорядочения множества N_0^k .*

Доказательство. Пусть $\preccurlyeq$ — произвольное мономиальное упорядочение множества N_0^k . Заметим, что при любом $\mathbf{r} \in \mathcal{KF}$ для многочлена $F_{\mathbf{r}} \in \chi$ выполняется условие $\text{mdg } F_{\mathbf{r}} = \mathbf{r}$. Тогда по построению все многочлены множества χ унитарные.

Очевидно, что произвольный многочлен $F_{\mathbf{r}} \in \chi$ является нормальным по модулю множества $\chi \setminus \{F_{\mathbf{r}}\}$.

Пусть $F(\mathbf{x})$ — произвольный ненулевой многочлен из идеала I . Покажем, что F редуцируется к 0 по модулю множества χ . По лемме 2 существует $A \in NF(F, \chi)$. Тогда из предложения 3 следует, что $\mathcal{F}(A) \subseteq \mathcal{F}$. Так как $F \in I$, то и $A \in I$.

Далее для доказательства теоремы 2 нам потребуется следующая лемма.

Лемма 4. *Пусть $\mathcal{F} \subset N_0^k$ — диаграмма Ферре, $\chi \subset \mathcal{R}_k$ — некоторое согласованное с диаграммой Ферре $\mathcal{F}$ множество мономиальных многочленов, $A \in \mathcal{R}_k \chi$. Тогда из условия $\mathcal{F}(A) \subseteq \mathcal{F}$ следует, что $A = 0$.*

Доказательство. Докажем утверждение леммы индукцией по k .

Пусть $k = 1$. Тогда любая диаграмма Ферре $\mathcal{F}$ имеет вид $\{0, \dots, l-1\}$, при этом $\chi = \{F(x)\}$, где $\deg F(x) = l$, $I = \mathcal{R}_1 F(x)$. Тогда $A(x) = G(x)F(x)$. Из унитарности многочлена F следует, что условие $\deg A < \deg F$, равносильное условию $\mathcal{F}(A) \subseteq \mathcal{F}$, выполняется в точности если $G = A = 0$.

Допустим, что $n \geq 1$ и для $k = n$ утверждение верно. Докажем, что из данного предположения следует верность утверждения леммы для $k = n + 1$.

Пусть $\mathcal{F} \subset N_0^{n+1}$ — некоторая диаграмма Ферре, $\mathcal{KF}$ — ее множество углов, $\chi \subset \mathcal{R}_k$ — произвольное согласованное с диаграммой Ферре $\mathcal{F}$ множество мономиальных многочленов, $I = \mathcal{R}_k \chi$, $A(\mathbf{x}) \in I$ такой, что $\mathcal{F}(A) \subseteq \mathcal{F}$.

Дальнейшее доказательство проведем от противного. Допустим, что $A \neq 0$. Обозначим через $l = \deg_{x_k} A(\mathbf{x})$ — степень многочлена $A(\mathbf{x})$ по переменной x_k . Многочлен $A(\mathbf{x})$ можно представить в виде

$$A(\mathbf{x}) = \sum_{m=0}^l A_m(x_1, \dots, x_n) x_k^m, \quad (15)$$

где $A_m \in \mathcal{R}_n$ для $m = 0, 1, \dots, l$ — некоторые многочлены, зависящие от переменных $x_1, \dots, x_n$, причем $A_l \neq 0$. Тогда

$$\mathcal{F}(A) = \bigcup_{m=0}^l \{\mathcal{F}(A_m) \times \{m\}\}.$$

Рассмотрим множество

$$\mathcal{F}_l = \{(i_1, \dots, i_n) \in \mathbf{N}_0^n : (i_1, \dots, i_n, l) \in \mathcal{F}\}.$$

Данное множество непусто, поскольку $\mathcal{F}(A_l) \subseteq \mathcal{F}_l$. Легко заметить, что $\mathcal{F}_l \subset \mathbf{N}_0^n$ — диаграмма Ферре.

Идея дальнейшего доказательства состоит в следующем: для диаграммы Ферре $\mathcal{F}_l \subset \mathbf{N}_0^n$ строится согласованное с диаграммой Ферре $\mathcal{F}_l$ множество мономиальных многочленов $\chi' \subset \mathcal{R}_n$ такое, что ненулевой многочлен A_l принадлежит идеалу $I' = \mathcal{R}_n \chi'$. Многочлен A_l удовлетворяет условию $\mathcal{F}(A_l) \subseteq \mathcal{F}_l$, значит, по предположению индукции, $A_l = 0$. Получится противоречие с условием $A_l \neq 0$, а значит, и с исходным допущением, что $A \neq 0$.

Рассмотрим множество

$$U = \{\mathbf{r} = (r_1, \dots, r_k) \in \mathcal{KF} : r_k > l\}.$$

Данное множество непусто, так как там есть, по крайней мере, один элемент $h_k \mathbf{1}_k$ (см. следствие 1). Пусть $\mathbf{u} = (u_1, \dots, u_k)$ — элемент U такой, что для любого $\mathbf{r} = (r_1, \dots, r_k)$ из U выполняется неравенство $u_k \leq r_k$, то есть k -я координата вектора $\mathbf{u}$ есть минимум k -х координат векторов из U . Так как $\deg_{x_k} A(\mathbf{x}) = l < u_k$, то

$$A(\mathbf{x}) = \text{Res}(A(\mathbf{x})/F_{u_k}^{(k)}(x_k)). \quad (16)$$

Поскольку $A(\mathbf{x}) \in I$, существуют такие многочлены $H_{\mathbf{r}} \in \mathcal{R}_k$, $\mathbf{r} \in \mathcal{KF}$, что

$$A(\mathbf{x}) = \sum_{\mathbf{r} \in \mathcal{KF}} F_{\mathbf{r}} H_{\mathbf{r}} = \sum_{\mathbf{r} \in \mathcal{KF} \setminus U} F_{\mathbf{r}} H_{\mathbf{r}} + \sum_{\mathbf{r} \in U} F_{\mathbf{r}} H_{\mathbf{r}}. \quad (17)$$

Заметим, что $\text{Res}(F_{\mathbf{r}}/F_{u_k}^{(k)}(x_k)) = 0$ для любого $\mathbf{r} \in U$. Поэтому из (17) и (16) получим следующую цепочку равенств:

$$\begin{aligned} A(\mathbf{x}) &= \text{Res}(A(\mathbf{x})/F_{u_k}^{(k)}(x_k)) = \text{Res} \left(\sum_{\mathbf{r} \in \mathcal{KF} \setminus U} F_{\mathbf{r}} H_{\mathbf{r}} / F_{u_k}^{(k)}(x_k) \right) \\ &= \sum_{\mathbf{r} \in \mathcal{KF} \setminus U} \text{Res}(F_{r_1}^{(1)}(x_1) \dots F_{r_k}^{(k)}(x_k) H_{\mathbf{r}} / F_{u_k}^{(k)}(x_k)) \\ &= \sum_{\mathbf{r} \in \mathcal{KF} \setminus U} F_{r_1}^{(1)}(x_1) \dots F_{r_n}^{(n)}(x_n) \text{Res}(F_{r_k}^{(k)}(x_k) H_{\mathbf{r}} / F_{u_k}^{(k)}(x_k)). \end{aligned} \quad (18)$$

Пусть

$$V = \{\mathbf{v} \in \mathbf{N}_0^n \mid \exists v_k \in \{0, \dots, l\} : (\mathbf{v}, v_k) \in \mathcal{KF} \setminus U\}$$

— множество всех возможных наборов первых n координат векторов из $\mathcal{KF} \setminus U$. Далее нам потребуется следующая модификация обозначения (12):

$$F_v = F_{v_1}^{(1)}(x_1)F_{v_2}^{(2)}(x_2)\dots F_{v_n}^{(n)}(x_n),$$

где $v = (v_1, \dots, v_n) \in V$. Из попарной несравнимости векторов из $\mathcal{KF}$ по отношению $\leq$ следует, что для любого вектора $v = (v_1, \dots, v_n) \in V$ существует единственное число $v_k \in \{0, 1, \dots, l\}$ такое, что $(v_1, \dots, v_n, v_k) \in \mathcal{KF} \setminus U$. Тогда последнее равенство в (18) можно переписать следующим образом:

$$A(x) = \sum_{v \in V} F_v L_v, \quad (19)$$

где $F_v = F_{v_1}^{(1)}(x_1)F_{v_2}^{(2)}(x_2)\dots F_{v_n}^{(n)}(x_n) \in \mathcal{R}_n$, $L_v = \text{Res}(F_{v_k}^{(k)}(x_k)H_{(v, v_k)}/F_{u_k}^{(k)}(x_k))$ для $v = (v_1, \dots, v_n) \in V$ (здесь в качестве v_k взято то единственное число, при котором вектор (v, v_k) принадлежит множеству $\mathcal{KF} \setminus U$). Для любого $v \in V$ запишем многочлен L_v в виде

$$L_v = \sum_{m=0}^{u_k-1} L_v^{(m)} x_k^m,$$

где $L_v^{(m)} \in \mathcal{R}_n$. С учетом этого из (15) и (19) получаем, что

$$A_l = \sum_{v \in V} F_v L_v^{(l)}. \quad (20)$$

Рассмотрим множество

$$T = \{v \in V : \forall v' \in V \setminus \{v\} \quad v' \not\leq v\},$$

являющееся множеством всех минимальных векторов множества V (см. [10]). Для любого $v \in V$ существует вектор $t \in T$ такой, что $t \leq v$. Напомним, что если $t \leq v$, то $F_t \mid F_v$. Тогда (20) можно переписать следующим образом:

$$A_l = \sum_{t \in T} F_t G_t, \quad (21)$$

где $G_t \in \mathcal{R}_n$ для $t \in T$. Данное представление получается из (20) некоторой группировкой слагаемых. Покажем, что $T \subset \mathcal{KF}_l$. Для этого нам потребуется следующая лемма.

Лемма 5. Если $j = (j_1, \dots, j_n) \in \mathcal{KF}_l$, то существует $m \in \{0, 1, \dots, l\}$ такое, что вектор (j, m) принадлежит $\mathcal{KF}$.

Доказательство. Пусть $j = (j_1, \dots, j_n) \in \mathcal{KF}_l$. Заметим, что $(j, l) \in \Delta\mathcal{F}$ и поэтому, согласно лемме 1, для любого $m = 0, 1, \dots, l$ вектор (j, m) принадлежит $\mathcal{F} \cup \Delta\mathcal{F}$. Рассмотрим два случая.

Пусть для любого $m \in \{0, 1, \dots, l\}$ вектор (j, m) принадлежит $\Delta\mathcal{F}$. Для любого $t \in \{1, \dots, n\}$ такого, что $j_t > 0$, докажем верность включения $(j, 0) - 1_t \in \mathcal{F}$. Так как $j \in \mathcal{KF}_l$, согласно предложению 1 $(j_1, \dots, j_t - 1, \dots, j_n) \in \mathcal{F}_l$. Значит, $(j_1, \dots, j_t - 1, \dots, j_n, l) \in \mathcal{F}$. Справедливо неравенство

$$(j, 0) - 1_t \leq (j, l) - 1_t = (j_1, \dots, j_t - 1, \dots, j_n, l).$$

Тогда $(j, 0) - 1_t \in \mathcal{F}$ и из предложения 1 следует, что $(j, 0) \in \mathcal{KF}$.

Пусть существует $m \in \{0, 1, \dots, l-1\}$ такое, что $(j, m) \in \mathcal{F}$ и $(j, b) \in \Delta\mathcal{F}$ для любого $b = m+1, \dots, l-1$. Рассуждениями, аналогичными вышеприведенным, легко показать, что если $j_t > 0$ для некоторого $t \in \{1, \dots, n\}$, то $(j, m+1) - 1_t \in \mathcal{F}$. Тогда из предложения 1 следует, что вектор $(j, m+1)$ принадлежит $\mathcal{KF}$.

Продолжим доказательство леммы 2. Пусть $t \in T$. Допустим, что $t \notin \mathcal{KF}_l$. Тогда возможны две ситуации: либо $t \in \mathcal{F}_l$, либо $t \in \overline{\mathcal{F}_l} \setminus \mathcal{KF}_l$.

Рассмотрим случай $t \in \mathcal{F}_l$. Тогда $(t, l) \in \mathcal{F}$. Вектор t принадлежит множеству V , значит, существует число $v_k \in \{0, 1, \dots, l\}$ такое, что вектор $(t, v_k) \in \mathcal{KF}$. Справедливо неравенство $(t, v_k) \leq (t, l)$. Получено противоречие с условием $(t, l) \in \mathcal{F}$, значит, данная ситуация невозможна.

Пусть теперь $t \in \overline{\mathcal{F}_l} \setminus \mathcal{KF}_l$. Тогда существует вектор $j \in \mathcal{KF}_l$ такой, что $j \leq t$. Из леммы 5 следует, что существует $j_k \in \{0, 1, \dots, l\}$ такой, что $(j, j_k) \in \mathcal{KF}$. Так как $j_k \leq l$, то $(j, j_k) \in \mathcal{KF} \setminus U$ и $j \in V$. Получено противоречие с определением множества T , значит, и эта ситуация невозможна.

Таким образом, $T \subset \mathcal{KF}_l$ и из (21) следует, что

$$A_l = \sum_{t \in \mathcal{KF}_l} F_t H_t,$$

где

$$H_t = \begin{cases} G_t, & \text{если } t \in T, \\ 0, & \text{если } t \in \mathcal{KF}_l \setminus T. \end{cases}$$

Итак, обозначим через χ' множество многочленов $\{F_j : j \in \mathcal{KF}_l\} \subset \mathcal{R}_n$. Заметим, что множество χ' является согласованным с диаграммой Ферре $\mathcal{F}_l$ множеством мономиальных многочленов. Многочлен $A_l \in \mathcal{R}_n \chi'$ удовлетворяет условию $\mathcal{F}(A_l) \subseteq \mathcal{F}_l$, значит, по предположению индукции, $A_l = 0$. Получено противоречие с условием $A_l \neq 0$, а значит, и с исходным допущением $A \neq 0$. Таким образом, лемма 4 доказана.

Завершим доказательство теоремы 2. Многочлен $A \in NF(F, \chi) \subset I$ удовлетворяет условию $\mathcal{F}(A) \subseteq \mathcal{F}$. Тогда из леммы 4 следует, что $A = 0$. Таким образом, произвольный многочлен $F \in I \setminus \{0\}$ редуцируется по модулю множества χ к 0. Значит, множество χ является унитарным стандартным базисом идеала I .

Итак, из теорем 1 и 2 следует, что пара $\langle I, \mathcal{F} \rangle$ образует k -линейный регистр сдвига, который мы будем называть мономиальным в широком смысле.

Приведем примеры мономиального и призматического регистров сдвига.

Пример 3. Пусть $R = P = GF(2)$,

$$F_1 = (x_1 + 1)^3, \quad F_2 = (x_2 + 1)^3,$$

$$F_3 = (x_1 + 1)^2(x_2 + 1),$$

$$F_4 = (x_1 + 1)(x_2 + 1)^2,$$

$$F_5 = x_3^2 + x_3 + 1,$$

унитарный идеал $I_1 \triangleleft R[x_1, x_2]$ порожден набором многочленов $\{F_1, F_2, F_3, F_4\}$, унитарный идеал $I_2 \triangleleft R[x_1, x_2, x_3]$ порожден набором многочленов $\{F_1, F_2, F_3, F_4, F_5\}$, $\mathcal{F}_1$ — диаграмма Ферре с рис. 1 (а), $\mathcal{F}_2$ — диаграмма Ферре с рис. 3. Тогда пары $\langle I_1, \mathcal{F}_1 \rangle$ и $\langle I_2, \mathcal{F}_2 \rangle$ образуют мономиальный и призматический k -ЛРС, соответственно.

5. Периоды правильных k -линейных регистров сдвига

В данном параграфе рассматривается введенное в [5] понятие периода k -линейного регистра сдвига. Для случая $k = 1$, $R = GF(q)$ задача вычисления периода k -ЛРС представляет собой классическую задачу вычисления порядка (периода) многочлена из $\mathcal{R}$, решение которой можно найти, например, в [7]. Результаты [5, 11] позволяют эффективно вычислять период k -ЛРС в случае, когда $k = 1$, $R = GR(q^n, p^n)$ — кольцо Галуа. Однако, до настоящего времени не было результатов по вычислению периода полилинейного регистра сдвига для случая $k > 1$. В данном параграфе для коммутативного артинова кольца R с единицей e и произвольного $k \in \mathbf{N}$ решается задача вычисления периода правильного полилинейного регистра сдвига. Отдельно рассматриваются случаи, когда исходный правильный k -ЛРС является к тому же призматическим или мономиальным.

Определение 8 ([5]). Идеал $I \triangleleft \mathcal{R}_k$ называется периодическим, если существуют числа $d_1, \dots, d_k \in \mathbf{N}_0$, $t_1, \dots, t_k \in \mathbf{N}$ такие, что

$$x_s^{d_s}(x_s^{t_s} - 1) \in I, \quad s = 1, \dots, k,$$

и реверсивным, если существуют числа $t_1, \dots, t_k \in \mathbf{N}$ такие, что

$$x_s^{t_s} - 1 \in I, \quad s = 1, \dots, k.$$

Напомним некоторые введенные ранее обозначения:

$$S = \mathcal{R}_k/I = R[\vartheta_1, \dots, \vartheta_k], \quad \vartheta_i = x_i + I, \quad i = 1, \dots, k.$$

Следуя [5], подполугруппу $O(I) = \langle e, \vartheta_1, \dots, \vartheta_k \rangle$ полугруппы $(S, \cdot)$, порожденную элементами $e, \vartheta_1, \dots, \vartheta_k$, назовем орбитальной полугруппой идеала I . Если I — реверсивный идеал, то $O(I) = \langle \vartheta_1, \dots, \vartheta_k \rangle$ — подгруппа группы S^* . Для реверсивного идеала I параметр $T = |O(I)|$ называется его периодом. Всюду далее рассматриваются лишь реверсивные идеалы $I \triangleleft \mathcal{R}_k$. Периодом ЛРС $\langle I, \mathcal{F} \rangle$ назовем период идеала I .

Пусть далее $\preccurlyeq$ — некоторое чисто лексикографическое упорядочение множества $\mathbf{N}_0^k$. Не ограничивая общность излагаемых ниже результатов, будем считать, что $x_1 \prec x_2 \prec \dots \prec x_k$.

Пусть $I \triangleleft \mathcal{R}_k$ — некоторый унитарный идеал, χ — правильный стандартный базис идеала I относительно упорядочения $\preccurlyeq$, причем k содержащихся в χ унитарных многочлена $F_1(x_1), \dots, F_k(x_k)$, зависящих только от одной переменной, реверсивные, то есть удовлетворяют условию $F_1(0), \dots, F_k(0) \in R^*$. Легко заметить, что I — реверсивный идеал. Пусть $\mathcal{F}$ — опорная диаграмма Ферре базиса χ . Тогда пара $\langle I, \mathcal{F} \rangle$ образует правильный регистр сдвига (см. параграф 4). Ниже мы получим некоторую формулу для вычисления периода данного k -ЛРС.

Для каждого $t \in \{1, \dots, k\}$ через T_t обозначим порядок элемента ϑ_t в группе $O(I)$. Далее нам потребуется следующий результат.

Предложение 5. Для каждого $t \in \{1, \dots, k\}$ справедливо равенство

$$T_t = T(F_t(x_t)).$$

Доказательство. Пусть $t \in \{1, \dots, k\}$. Условие $\vartheta_t^{T_t} = e$ равносильно включению $x_t^{T_t} - e \in I$. Пусть $r_t(x_t) = \text{Res}(x_t^{T_t} - e/F_t(x_t))$. Заметим, что

$$r_t(x_t) \in NF(x_t^{T_t} - e, F_t(x_t)).$$

Легко показать, что $r_t(x_t) \in N(\chi)$. Значит, $r_t = 0$, то есть $F_t \mid x_t^{T_t} - e$. Отсюда $T(F_t) \mid T_t$. С другой стороны, так как $x_t^{T(F_t)} - e \in I$, то $T_t \mid T(F_t)$.

Определение 9. Пусть $\psi \subset R[x_1, \dots, x_t]$ и $\psi \not\subset R[x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_t]$ для любого $j = 1, \dots, t$. Тогда множеством мультипликаторов системы многочленов ψ назовем множество

$$\text{Mult}(\psi) = \{a \in R \mid \exists(i_1, \dots, i_t) \in \mathbf{N}_0^t: x_1^{i_1} \dots x_t^{i_t} \equiv a \pmod{\mathcal{R}_t \psi}\}.$$

Множество мультипликаторов системы многочленов $\psi \subset \mathcal{R}_t$ является подполугруппой полугруппы $(R, \cdot)$, а если $\mathcal{R}_t \psi$ — реверсивный идеал в $\mathcal{R}_t$, то $\text{Mult}(\psi)$ — подгруппа абелевой группы $(R^*, \cdot)$ (см. [6]).

В рамках принятых нами обозначений имеет место следующий результат.

Теорема 3. Пусть $\chi_t = \chi \cap R[x_1, \dots, x_t]$ для $t = 1, \dots, k$. Тогда период T линейного регистра сдвига $\langle I, \mathcal{F} \rangle$ удовлетворяет соотношению

$$T = \frac{T_1 T_2 \dots T_k \mid \text{Mult}(F_2) \text{Mult}(F_1) \mid \mid \text{Mult}(F_3) \text{Mult}(\chi_2) \mid \dots \mid \text{Mult}(F_k) \text{Mult}(\chi_{k-1}) \mid}{\mid \text{Mult}(F_1) \mid \dots \mid \text{Mult}(F_k) \mid \mid \text{Mult}(\chi_2) \mid \dots \mid \text{Mult}(\chi_{k-1}) \mid} \quad (22)$$

и верна оценка

$$T \geq \frac{T_1 T_2 \dots T_k}{(T_1, T_2, |R^*|)(T_1 T_2, T_3, |R^*|) \dots (T_1 \dots T_{k-1}, T_k, |R^*|)}. \quad (23)$$

Доказательство. Так как χ — правильный стандартный базис идеала $I = \mathcal{R}_k \chi$, то $F_j(x_j) \in \chi_t$ для любых $t \in \{1, \dots, k\}$ и $j \in \{1, \dots, t\}$, значит,

$$\chi_t \not\subset R[x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_t]$$

для всех $j \in \{1, \dots, t\}$.

Пусть $G_t = \langle \vartheta_1, \dots, \vartheta_t \rangle$ для $t = 1, \dots, k$,

$$H_j = G_{j-1} \cap \langle \vartheta_j \rangle, \quad V_j = \text{Mult}(\chi_{j-1}) \cap \text{Mult}(F_j(x)), \quad j = 2, \dots, k.$$

Поскольку I — реверсивный идеал, период T регистра сдвига $\langle I, \mathcal{F} \rangle$ равен $|G_k|$ (см. [5]). Так как G_{t-1} и $\langle \vartheta_t \rangle$ — конечные подгруппы группы G_t для $t \in \{2, \dots, k\}$, верно равенство

$$|G_t| = \frac{|G_{t-1}| |\langle \vartheta_t \rangle|}{|H_t|}. \quad (24)$$

Тогда

$$|G_t| = \frac{|\langle \vartheta_1 \rangle| \dots |\langle \vartheta_t \rangle|}{|H_2| \dots |H_t|} = \frac{T_1 T_2 \dots T_t}{|H_2| \dots |H_t|}, \quad t = 2, \dots, k. \quad (25)$$

Далее мы покажем, что $H_t = V_t$ для любого $t = 2, \dots, k$. Пусть

$$\vartheta_t^{j_t} = \vartheta_1^{j_1} \dots \vartheta_{t-1}^{j_{t-1}} \in H_t \quad (26)$$

для некоторого набора $(j_1, \dots, j_t) \in \mathbb{N}_0^t$. Это равносильно тому, что в идеале I содержится многочлен $A(\mathbf{x}) = x_t^{j_t} - x_1^{j_1} \dots x_{t-1}^{j_{t-1}}$. Так как χ — стандартный базис идеала I , каждый ненулевой многочлен из I редуцируется к 0 по модулю множества χ . Пусть

$$K_1(x_t) \in NF(x_t^{j_t}, F_t(x_t)), \quad K_2(x_1, \dots, x_{t-1}) \in NF(x_1^{j_1} \dots x_{t-1}^{j_{t-1}}, \chi_{t-1}).$$

Покажем, что $K_1, K_2 \in N(\chi)$. Рассуждениями, аналогичными приведенным в доказательстве предложения 5, можно показать, что $N(\chi) \cap R[x_t] = N(F_t) \ni K_1$. Выполнение условия $K_2 \in N(\chi)$ докажем от противного. Допустим, что для некоторых $G \in \chi$, $b \in R$, $i \in \mathbb{N}_0^k$ и $L \in \mathcal{R}_k$ имеет место редукция $K_2(x_1, \dots, x_{t-1}) \xrightarrow{(G, b, i)} L$. Тогда по определению полиномиальной редукции выполняются условия

$$\text{Cf}(K_2, \mathbf{x}^i \text{Lt}(G)) = b \text{Lc}(G) \neq 0, \quad L = K_2 - b\mathbf{x}^i G.$$

Отсюда и из условия $K_2 \in R[x_1, \dots, x_{t-1}]$ следует, что $\mathbf{x}^i \text{Lt}(G) \in R[x_1, \dots, x_{t-1}]$. Так как $\text{Lt}(G) \in R[x_1, \dots, x_{t-1}]$ и $x_1 < x_2 < \dots < x_k$, то $G \in R[x_1, \dots, x_{t-1}]$. Тогда $G \in \chi_{t-1} = \chi \cap R[x_1, \dots, x_{t-1}]$. Получено противоречие с условием $K_2 \in N(\chi_{t-1})$. Итак, $K_1, K_2 \in N(\chi)$. Тогда согласно предложению 3 многочлен $K_1 - K_2$ является нормальным по модулю множества χ и имеет место следующая последовательность редукций:

$$A(\mathbf{x}) = (x_t^{j_t} - x_1^{j_1} \dots x_{t-1}^{j_{t-1}}) \xrightarrow{\{F_t\}} (K_1 - x_1^{j_1} \dots x_{t-1}^{j_{t-1}}) \xrightarrow{\chi_{t-1}} (K_1 - K_2),$$

то есть $K_1 - K_2 \in NF(A(\mathbf{x}), \chi) = \{0\}$. Итак, $K_1(x_t) = K_2(x_1, \dots, x_{t-1})$. Последнее равенство возможно тогда и только тогда, когда $K_1(x_t) = K_2(x_1, \dots, x_{t-1}) = a \in R$.

Таким образом, $x_t^{j_t} = a + L_1$, $x_1^{j_1} \dots x_{t-1}^{j_{t-1}} = a + L_2$, где $L_1 \in R[x_t]F_t(x_t)$, $L_2 \in R[x_1, \dots, x_{t-1}]\chi_{t-1}$. Отсюда следует, что

$$\vartheta_t^{j_t} = \vartheta_1^{j_1} \dots \vartheta_{t-1}^{j_{t-1}} = a \in \text{Mult}(F_t) \cap \text{Mult}(\chi_{t-1}) = V_t.$$

Пусть теперь $a \in V_t$. Тогда существуют $j_1, \dots, j_t \in \mathbb{N}_0$ такие, что $x_t^{j_t} = a + L_1$, $x_1^{j_1} \dots x_{t-1}^{j_{t-1}} = a + L_2$, где $L_1 \in R[x_t]F_t(x_t)$, $L_2 \in R[x_1, \dots, x_{t-1}]\chi_{t-1}$. Так как $F_t(x_t) \in I$ и $\chi_{t-1} \subset I$, отсюда следует, что

$$a = \vartheta_t^{j_t} = \vartheta_1^{j_1} \dots \vartheta_{t-1}^{j_{t-1}} \in H_t.$$

Таким образом, мы доказали равенства $H_t = V_t$, $t = 2, \dots, k$.

Так как для любого $t \in \{2, \dots, k\}$ группы $\text{Mult}(\chi_{t-1})$ и $\text{Mult}(F_t(x))$ являются конечными подгруппами R^* , имеет место равенство

$$|V_t| = \frac{|\text{Mult}(F_t(x))| |\text{Mult}(\chi_{t-1})|}{|\text{Mult}(F_t(x)) \text{Mult}(\chi_{t-1})|}.$$

Заметим, что $\chi_1 = R[x_1] \cap \chi = \{F_1(x_1)\}$. Тогда из последнего равенства следует, что

$$|V_2| \dots |V_k| = \frac{|\text{Mult}(F_1)| \dots |\text{Mult}(F_k)| |\text{Mult}(\chi_2)| \dots |\text{Mult}(\chi_{k-1})|}{|\text{Mult}(F_2) \text{Mult}(F_1)| |\text{Mult}(F_3) \text{Mult}(\chi_2)| \dots |\text{Mult}(F_k) \text{Mult}(\chi_{k-1})|} \quad (27)$$

Подставляя (27) в (25) при $t = k$, получаем (22).

Докажем теперь нижнюю оценку величины $T = |G_k|$ в (22). Для любого $t = 2, \dots, k$ группа $H_t = V_t$ является подгруппой групп $G_{t-1}, \langle \vartheta_t \rangle$ и R^* , и, следовательно, ее порядок делит $(|G_{t-1}|, T_t, |R^*|)$. Согласно (25) $|G_{t-1}|$ делит произведение $T_1 \dots T_{t-1}$, значит, $|H_t|$ делит $(T_1 \dots T_{t-1}, T_t, |R^*|)$ для любого $t = 2, \dots, k$, что вместе с формулой (25) дает требуемое неравенство для $T = |G_k|$.

Следствие 2. В условиях теоремы 3 пусть $k = 2$. Тогда период T линейного регистра сдвига $\langle I, \mathcal{F} \rangle$ удовлетворяет соотношению

$$T = \frac{T_1 T_2 |\text{Mult}(F_2) \text{Mult}(F_1)|}{|\text{Mult}(F_1)| |\text{Mult}(F_2)|}. \quad (28)$$

Заметим, что в условиях следствия 2 период линейного регистра сдвига $\langle I, \mathcal{F} \rangle$ полностью определяется многочленами $F_1(x_1)$ и $F_2(x_2)$. Это, в частности, означает, что для любого удовлетворяющего условиям следствия 2 правильного регистра сдвига $\langle I, \mathcal{F} \rangle$ существует правильный регистр сдвига $\langle I_1, \Pi \rangle$ того же периода такой, что $L_M(I) \subseteq L_M(I_1)$ и Π есть минимальный параллелепипед, содержащий $\mathcal{F}$.

Следствие 3. Пусть $R = GF(2)$ — поле Галуа из двух элементов. Тогда период T линейного регистра сдвига $\langle I, \mathcal{F} \rangle$ из теоремы 3 удовлетворяет соотношению

$$T = T_1 \dots T_k, \quad (29)$$

и оценка (23) в этом случае является достижимой.

Доказательство. Заметим, что в этом случае $|R^*| = 1$ и подстановка данного значения в неравенство (23) дает требуемый результат.

Следствие 4. Пусть $k = 2$, $R = P = GF(q)$ — поле Галуа из q элементов, многочлены $F_1(x_1)$ и $F_2(x_2)$ неприводимы. Тогда период T линейного регистра сдвига $\langle I, \mathcal{F} \rangle$ удовлетворяет соотношению

$$T = \frac{T_1 T_2}{(T_1, T_2, q - 1)}, \quad (30)$$

(то есть оценка (23) и в этом случае является достижимой).

Доказательство. Из (25) следует, что $T = T_1 T_2 / |H_2|$. В условиях данного следствия $|R^*| = q - 1$, поэтому необходимо показать, что $|H_2| = (T_1, T_2, q - 1)$, где $H_2 = \langle \vartheta_1 \rangle \cap \langle \vartheta_2 \rangle \cap P^*$. Пусть $W_1 = \langle \vartheta_1 \rangle \cap P^*$, $W_2 = \langle \vartheta_2 \rangle \cap P^*$. Покажем, что $|W_i| = (T_i, q - 1)$, $i = 1, 2$. Поскольку W_i — подгруппа $\langle \vartheta_i \rangle$ и P^* , то W_i — циклическая группа и ее порядок делит $(T_i, q - 1)$, $i = 1, 2$. Группа $\langle \vartheta_i \rangle$ имеет подгруппу V_{i1} порядка $(T_i, q - 1)$. Группа P^* тоже имеет подгруппу V_{i2} порядка $(T_i, q - 1)$. Поскольку многочлены $F_1(x_1)$ и $F_2(x_2)$ неприводимы, группы $P[\vartheta_1]^*$ и $P[\vartheta_2]^*$ циклические. Так как циклические группы $\langle \vartheta_i \rangle$ и P^* есть подгруппы группы $P[\vartheta_i]^*$, группы V_{i1} и V_{i2} есть подгруппы порядка $(T_i, q - 1)$ циклической группы $P[\vartheta_i]^*$, а значит, они совпадают, следовательно, $V_{i1} = V_{i2} \subset \langle \vartheta_i \rangle \cap P^* = W_i$. Более того, $V_{i1} = V_{i2} = W_i$.

Итак, $|W_i| = (T_i, q - 1)$, $i = 1, 2$. Заметим, что $H_2 = W_1 \cap W_2$. Циклическая группа W_j , $j = 1, 2$, содержит единственную подгруппу U_j порядка $(T_1, T_2, q - 1)$, которая к тому же является подгруппой циклической группы P^* , значит,

$$U_1 = U_2 \subset H_2.$$

С другой стороны, порядок H_2 делит $(T_1, T_2, q - 1)$, значит, $|H_2| = (T_1, T_2, q - 1)$.

Пример 4. Регистры сдвига $\langle I_1, \mathcal{F}_1 \rangle$ и $\langle I_2, \mathcal{F}_2 \rangle$ из примера 3 имеют периоды 16 и 48, соответственно.

Пусть пара $\langle I, \mathcal{F} \rangle$ образует k -ЛРС периода T . Напомним, что согласно [11], период $T(\mu)$ произвольной k -ЛРП $\mu \in L_M(I)$ определяется как число различных элементов множества $\{x^i \mu : i \in \mathbb{N}_0^k\}$ или $\{x^i \mu[\mathcal{F}] : i \in \mathbb{N}_0^k\}$, причем $T(\mu) \mid T$.

Ниже приведен пример, показывающий, что в отличие от случая $k = 1$, для $k > 1$ период k -линейного регистра сдвига не всегда равен наименьшему общему кратному периодов его выходных последовательностей.

Пример 5. Пусть в условиях следствия 3 $k = 2$, $M = GF(2)$,

$$\mathcal{F} = \{(0, 0), (1, 0), (0, 1)\} \subset \mathbb{N}_0^2$$

— диаграмма Ферре,

$$\chi = \{F_1(x_1) = x_1^2 - 1, F_2(x_1, x_2) = x_1 x_2 - x_1 - x_2 + 1, F_3(x_2) = x_2^2 - 1\}$$

— согласованное с диаграммой Ферре $\mathcal{F}$ множество мономиальных многочленов, $I = \mathcal{R}_2 \chi$. Тогда пара $\langle I, \mathcal{F} \rangle$ образует 2-ЛРС периода 4, в то время как непосредственно легко проверить, что для любой выходной последовательности $\mu \in L_M(I)$ выполняется включение $T(\mu) \in \{1, 2\}$.

Пусть далее $\langle I, \mathcal{F} \rangle$ — правильный призматический полилинейный регистр сдвига, где унитарный идеал $I \triangleleft \mathcal{R}_k$ порожден призматическим базисом

$$\chi = \chi_t \cup \{F_{t+1}(x_{t+1}), \dots, F_k(x_k)\}$$

относительно чисто лексикографического упорядочения $\preccurlyeq$, базис χ имеет основание размерности t и диаграмму Ферре $\mathcal{F}_\chi = \mathcal{F}$. В данном случае формулу (22) для вычисления периода регистра $\langle I, \mathcal{F} \rangle$ можно уточнить следующим образом.

Теорема 4. В введенных выше обозначениях период T линейного регистра сдвига $\langle I, \mathcal{F} \rangle$ удовлетворяет соотношению

$$T = \frac{T_1 T_2 \dots T_k |\text{Mult}(F_2) \text{Mult}(F_1)| |\text{Mult}(F_3) \text{Mult}(\chi_2)| \dots |\text{Mult}(F_t) \text{Mult}(\chi_{t-1})|}{|\text{Mult}(F_1)| \dots |\text{Mult}(F_k)|} \times \frac{|\text{Mult}(F_k) \dots \text{Mult}(F_{t+1}) \text{Mult}(\chi_t)|}{|\text{Mult}(\chi_2)| \dots |\text{Mult}(\chi_t)|}. \quad (31)$$

Доказательство. Так как $\langle I, \mathcal{F} \rangle$ — правильный регистр сдвига, для вычисления его периода T справедлива формула (22). Для каждого $i = t + 1, \dots, k - 1$ докажем равенство

$$\text{Mult}(\chi_i) = \text{Mult}(F_i(x_i)) \dots \text{Mult}(F_{i+1}(x_{i+1})) \text{Mult}(\chi_i). \quad (32)$$

Пусть $a \in \text{Mult}(\chi_i)$. Тогда для некоторого набора $(j_1, \dots, j_i) \in \mathbb{N}_0^i$ верно равенство $x_1^{j_1} \dots x_i^{j_i} - a = A(x)$, где $A \in R[x_1, \dots, x_i] \chi_i \subset I$. Рассмотрим цепочку многочленов $A_i(x), \dots, A_{t+1}(x)$, которая строится следующим образом:

$$\begin{aligned} A_i(x) &= \text{Res}(A(x)/F_i(x_i)), A_{i-1}(x) \\ &= \text{Res}(A_i(x)/F_{i-1}(x_{i-1})), \dots, A_{t+1}(x) \\ &= \text{Res}(A_{t+2}(x)/F_{t+1}(x_{t+1})). \end{aligned}$$

Заметим, что многочлен $A_{t+1}(\mathbf{x})$ имеет вид

$$A_{t+1}(\mathbf{x}) = x_1^{j_1} \dots x_t^{j_t} \text{Res}(x_{t+1}^{j_{t+1}}/F_{t+1}(x_{t+1})) \dots \text{Res}(x_i^{j_i}/F_i(x_i)) - a. \quad (33)$$

Так как для любого $v \in \{t+1, \dots, i\}$ многочлен $F_v(x_v)$ принадлежит идеалу I , то $A_{t+1} \in I \cap R[x_1, \dots, x_i]$. Пусть

$$H \in NF(x_1^{j_1} \dots x_t^{j_t}, \chi_t) \subset R[x_1, \dots, x_t].$$

Тогда, поскольку $x_1 \prec x_2 \prec \dots \prec x_k$, имеет место редукция

$$A_{t+1}(\mathbf{x}) \xrightarrow{\chi_t} L(\mathbf{x}) = H(x_1, \dots, x_t) \text{Res}(x_{t+1}^{j_{t+1}}/F_{t+1}(x_{t+1})) \dots \text{Res}(x_i^{j_i}/F_i(x_i)) - a. \quad (34)$$

Поскольку $\chi_t \subset I \cap R[x_1, \dots, x_t]$, то $L(\mathbf{x}) \in I \cap R[x_1, \dots, x_i]$. Тогда многочлен $L(\mathbf{x})$ либо равен 0, либо редуцируется к 0 по модулю множества χ . Рассуждениями, аналогичными приведенным в доказательстве теоремы 3, можно показать, что многочлен $L(\mathbf{x})$ является нормальным по модулю множества

$$\chi_i = \chi_t \cup \{F_{t+1}(x_{t+1}), \dots, F_i(x_i)\}.$$

Отсюда и из условия $L \in R[x_1, \dots, x_i]$ следует включение $L \in N(\chi)$. Значит, $L(\mathbf{x}) = 0$. Последнее равенство равносильно следующей системе:

$$\begin{aligned} H(x_1, \dots, x_t) &= a_t, \\ \text{Res}(x_{t+1}^{j_{t+1}}/F_{t+1}(x_{t+1})) &= a_{t+1}, \\ &\dots \\ \text{Res}(x_i^{j_i}/F_i(x_i)) &= a_i, \\ a_t \dots a_i &= a \end{aligned} \quad (35)$$

для некоторых $a_t, \dots, a_i \in R$. Отсюда следует, что

$$a_t \in \text{Mult}(\chi_t), \quad a_{t+1} \in \text{Mult}(F_{t+1}), \dots, a_i \in \text{Mult}(F_i)$$

и $a \in \text{Mult}(\chi_t) \text{Mult}(F_{t+1}) \dots \text{Mult}(F_i)$.

Пусть теперь $a = a_t \dots a_i$, где $a_t \in \text{Mult}(\chi_t), a_{t+1} \in \text{Mult}(F_{t+1}), \dots, a_i \in \text{Mult}(F_i)$. Так как $F_{t+1}(x_{t+1}), \dots, F_i(x_i) \in I$, существует набор $(j_1, \dots, j_i) \in \mathbb{N}_0^k$ такой, что $\vartheta_1^{j_1} \dots \vartheta_t^{j_t} = a_t, \vartheta_s^{j_s} = a_s$ для $s = t+1, \dots, i$. Тогда $a = \vartheta_1^{j_1} \dots \vartheta_i^{j_i}$, что равносильно существованию в идеале I многочлена $A(\mathbf{x}) = x_1^{j_1} \dots x_i^{j_i} - a$. Рассмотрим два случая.

Пусть $A = 0$, то есть $(j_1, \dots, j_i) = \mathbf{0}$ и $a = e$. В данном случае включение $a \in \text{Mult}(\chi_i)$ очевидно. Пусть далее $A \neq 0$. Так как $A \in I \cap R[x_1, \dots, x_i]$ и множество χ является стандартным базисом идеала I , многочлен $A(\mathbf{x})$ редуцируется к 0 по модулю множества $\chi \cap R[x_1, \dots, x_i] = \chi_i$, следовательно, $A \in R[x_1, \dots, x_i]\chi_i$ и $a \in \text{Mult}(\chi_i)$.

Итак, для любого $i = t+1, \dots, k-1$ мы показали справедливость равенства (32). Подставив полученное представление $\text{Mult}(\chi_i)$ в (22) и проведя необходимые сокращения, получим (31).

Рассмотрим теперь случай, когда $\langle I, \mathcal{F} \rangle$ — мономиальный полилинейный регистр сдвига, где $\mathcal{F} \subset \mathbb{N}_0^k$ — диаграмма Ферре, а унитарный идеал I порожден согласованным с диаграммой Ферре $\mathcal{F}$ множеством мономиальных многочленов χ (см. (12), (13), (14)). Будем считать, что все зависящие от одной переменной многочлены системы χ реверсивны. Далее, используя построенные в предыдущем параграфе наборы чисел $l_1, \dots, l_k$ и $h_1, \dots, h_k$, получим следующий результат.

Теорема 5. В введенных выше обозначениях период T линейного регистра сдвига $\langle I, \mathcal{F} \rangle$ удовлетворяет соотношению

$$T = \frac{T_1 T_2 \dots T_k}{|\text{Mult}(F_{h_1}^{(1)}(x))| \dots |\text{Mult}(F_{h_k}^{(k)}(x))|} |\text{Mult}(F_{h_1}^{(1)}(x)) \dots \text{Mult}(F_{h_k}^{(k)}(x))|. \quad (36)$$

Доказательство. По построению рассматриваемое множество χ содержит k унитарных многочленов $F_{h_1}^{(1)}(x_1), \dots, F_{h_k}^{(k)}(x_k)$, зависящих от одной переменной и является унитарным стандартным базисом идеала I относительно любого чисто лексикографического упорядочения множества N_0^k (теорема 2). Тогда для периода T регистра сдвига $\langle I, \mathcal{F} \rangle$ справедлива формула (22). Для каждого $t = 2, \dots, k-1$ докажем равенство

$$\text{Mult}(\chi_t) = \text{Mult}(F_{h_1}^{(1)}(x_1)) \text{Mult}(F_{h_2}^{(2)}(x_2)) \dots \text{Mult}(F_{h_t}^{(t)}(x_t)). \quad (37)$$

Пусть $a \in \text{Mult}(\chi_t)$. Тогда для некоторого набора $(j_1, \dots, j_t) \in N_0^t$ верно равенство $x_1^{j_1} \dots x_t^{j_t} = a + A(\mathbf{x})$, где $A \in I \cap R[x_1, \dots, x_t]$. Так как $A \in I$, существуют многочлены $H_{\mathbf{r}} \in \mathcal{R}_k$, $\mathbf{r} \in \mathcal{KF}$ такие, что

$$A(\mathbf{x}) = x_1^{j_1} \dots x_t^{j_t} - a = \sum_{\mathbf{r} \in \mathcal{KF}} F_{\mathbf{r}} H_{\mathbf{r}}. \quad (38)$$

Рассмотрим цепочку многочленов $A_1(\mathbf{x}), \dots, A_k(\mathbf{x})$, которая строится следующим образом:

$$\begin{aligned} A_1(\mathbf{x}) &= A(\mathbf{x}), \\ A_2(\mathbf{x}) &= \text{Res}(A_1(\mathbf{x})/F_{l_2}^{(2)}(x_2)), \\ &\dots \\ A_k(\mathbf{x}) &= \text{Res}(A_{k-1}(\mathbf{x})/F_{l_k}^{(k)}(x_k)). \end{aligned}$$

Так как $A(\mathbf{x}) \in R[x_1, \dots, x_t]$, то $A_i(\mathbf{x}) = A_i(x_1, \dots, x_t) = A_t(x_1, \dots, x_t)$ для любого $i = t, \dots, k$. Пусть

$$B_i = \{\mathbf{r} = (r_1, \dots, r_k) \in \mathcal{KF} : r_i > 0\}, \quad i = 1, \dots, k.$$

Заметим, что для любого $i = 1, \dots, k$ выполняется равенство

$$\mathcal{KF} \setminus B_1 \setminus \dots \setminus B_{i-1} \setminus B_{i+1} \setminus \dots \setminus B_k = h_i \mathbf{1}_i$$

(см. следствие 1). Многочлены $F_{l_i}^{(i)}(x_i)$, $i = 1, \dots, k$, выбраны так, что $F_{l_i}^{(i)}(x_i) | F_{\mathbf{r}}$ для любого $\mathbf{r} \in B_i$. Отсюда и из (38) следует, что

$$\begin{aligned} A_2(\mathbf{x}) &= \text{Res} \left(\sum_{\mathbf{r} \in \mathcal{KF}} F_{\mathbf{r}} H_{\mathbf{r}} / F_{l_2}^{(2)}(x_2) \right) = \sum_{\mathbf{r} \in \mathcal{KF}} \text{Res}(F_{\mathbf{r}} H_{\mathbf{r}} / F_{l_2}^{(2)}(x_2)) \\ &= \sum_{\mathbf{r} \in \mathcal{KF} \setminus B_2} \text{Res}(F_{\mathbf{r}} H_{\mathbf{r}} / F_{l_2}^{(2)}(x_2)), \end{aligned}$$

$$\begin{aligned}
A_3(\mathbf{x}) &= \text{Res} \left(\sum_{\mathbf{r} \in \mathcal{H} \setminus B_2} \text{Res}(F_{\mathbf{r}} H_{\mathbf{r}} / F_{l_2}^{(2)}(x_2)) / F_{l_3}^{(3)}(x_3) \right) \\
&= \sum_{\mathbf{r} \in (\mathcal{H} \setminus B_2) \setminus B_3} \text{Res}(\text{Res}(F_{\mathbf{r}} H_{\mathbf{r}} / F_{l_3}^{(3)}(x_3)) / F_{l_2}^{(2)}(x_2)) \\
&\dots \\
A_k(\mathbf{x}) &= \sum_{\mathbf{r} \in (\dots (\mathcal{H} \setminus B_2) \dots) \setminus B_k} \text{Res}(\dots \text{Res}(F_{\mathbf{r}} H_{\mathbf{r}} / F_{l_k}^{(k)}(x_k)) \dots / F_{l_2}^{(2)}(x_2)) = F_{h_1}^{(1)}(x_1) L(\mathbf{x}),
\end{aligned}$$

где

$$L = \text{Res}(\dots \text{Res}(H_{(h_1, 0, \dots, 0)} / F_{l_k}^{(k)}(x_k)) \dots / F_{l_2}^{(2)}(x_2)).$$

Итак,

$$A_k(\mathbf{x}) = F_{h_1}^{(1)}(x_1) L(\mathbf{x}) = x_1^{j_1} L_2(x_2) \dots L_t(x_t) - a, \quad (39)$$

где

$$L_i(x_i) = \text{Res}(x_i^{j_i} / F_{l_i}^{(i)}(x_i)), \quad i = 2, \dots, t.$$

Приведем левую и правую части равенства (39) по модулю многочлена $F_{h_1}^{(1)}(x_1)$. Получим равенство

$$\text{Res}(x_1^{j_1} / F_{h_1}^{(1)}(x_1)) \text{Res}(x_2^{j_2} / F_{l_2}^{(2)}(x_2)) \dots \text{Res}(x_t^{j_t} / F_{l_t}^{(t)}(x_t)) = a. \quad (40)$$

Заметим, что так как для любого $i = 1, \dots, t$ многочлены $\text{Res}(x_i^{j_i} / F_{l_i}^{(i)}(x_i))$ и $\text{Res}(x_i^{j_i} / F_{h_i}^{(i)}(x_i))$ зависят лишь от одной переменной x_i , то (40) равносильно системе равенств

$$\begin{aligned}
\text{Res}(x_1^{j_1} / F_{h_1}^{(1)}(x_1)) &= a_{11}, \\
\text{Res}(x_2^{j_2} / F_{l_2}^{(2)}(x_2)) &= a_{12}, \\
&\dots \\
\text{Res}(x_t^{j_t} / F_{l_t}^{(t)}(x_t)) &= a_{1t}, \\
a_{11} \dots a_{1t} &= a,
\end{aligned} \quad (41)$$

где $a_{1i} \in R$ для любого $i = 1, \dots, t$. Таким образом, мы показали, что из условия $a \in \text{Mult}(\chi_t)$ следует система равенств (41) для некоторых элементов a_{1i} , $i = 1, \dots, t$, кольца R . Аналогично, можно показать, что из условия $a \in \text{Mult}(\chi_t)$ следует еще

$t - 1$ система равенств вида

$$\begin{aligned}
 \text{Res}(x_1^{j_1} / F_{l_1}^{(1)}(x_1)) &= a_{c1}, \\
 &\dots \\
 \text{Res}(x_{c-1}^{j_{c-1}} / F_{l_{c-1}}^{(c-1)}(x_{c-1})) &= a_{cc-1}, \\
 \text{Res}(x_c^{j_c} / F_{h_c}^{(c)}(x_c)) &= a_{cc}, \\
 \text{Res}(x_{c+1}^{j_{c+1}} / F_{l_{c+1}}^{(c+1)}(x_{c+1})) &= a_{cc+1}, \\
 &\dots \\
 \text{Res}(x_t^{j_t} / F_{l_t}^{(t)}(x_t)) &= a_{ct}, \\
 a_{c1} \dots a_{ct} &= a,
 \end{aligned} \tag{42}$$

где $c = 2, \dots, t$, $a_{ji} \in R$ для любых $j, i = 1, \dots, t$. Заметим, что поскольку $F_{l_i}^{(i)}(x_i) \mid F_{h_i}^{(i)}(x_i)$ для любого $i = 1, \dots, k$, то из условия $x_i^{j_i} \equiv a_{ii} \pmod{F_{h_i}^{(i)}(x_i)}$ следует условие $x_i^{j_i} \equiv a_{ii} \pmod{F_{l_i}^{(i)}(x_i)}$, то есть $a_{ii} = a_{ji} = a_i$ для любых $j, i = 1, \dots, t$. Таким образом, из условия $a \in \text{Mult}(\chi_t)$ следует система равенств

$$\begin{aligned}
 \text{Res}(x_1^{j_1} / F_{h_1}^{(1)}(x_1)) &= a_1, \\
 &\dots \\
 \text{Res}(x_t^{j_t} / F_{h_t}^{(t)}(x_t)) &= a_t, \\
 a_1 \dots a_t &= a.
 \end{aligned} \tag{43}$$

Так как $F_{h_1}^{(1)}(x_1), \dots, F_{h_t}^{(t)}(x_t) \in I$, из (43) получается, что $\vartheta_s^{j_s} = a_s \in \text{Mult}(F_{h_s}^{(s)}(x_s))$ для $s = 1, \dots, t$ и $a = a_1 \dots a_t \in \text{Mult}(F_{h_1}^{(1)}(x_1)) \dots \text{Mult}(F_{h_t}^{(t)}(x_t))$.

Пусть теперь $a = a_1 \dots a_t$, где $a_i \in \text{Mult}(F_{h_i}^{(i)}(x_i))$ для любого $i = 1, \dots, t$. Так как $F_{h_1}^{(1)}(x_1), \dots, F_{h_t}^{(t)}(x_t) \in I$, существует набор $(j_1, \dots, j_t) \in \mathbb{N}_0^t$ такой, что $\vartheta_s^{j_s} = a_s$ для $s = 1, \dots, t$. Тогда $a = \vartheta_1^{j_1} \dots \vartheta_t^{j_t}$, что равносильно существованию в идеале I многочлена $A(\mathbf{x}) = x_1^{j_1} \dots x_t^{j_t} - a$. Так как множество χ является стандартным базисом идеала I , многочлен $A(\mathbf{x})$ редуцируется к 0 по модулю множества χ . Так как $A \in I \cap R[x_1, \dots, x_t]$, рассуждениями, аналогичными приведенным в доказательстве теоремы 3, можно показать, что многочлен $A(\mathbf{x})$ редуцируется к 0 по модулю множества $\chi \cap R[x_1, \dots, x_t] = \chi_t$, следовательно, $A \in \mathcal{R}_k \chi_t$ и $a \in \text{Mult}(\chi_t)$.

Итак,

$$\text{Mult}(\chi_t) = \text{Mult}(F_{h_1}^{(1)}(x_1)) \dots \text{Mult}(F_{h_t}^{(t)}(x_t))$$

для любого $t = 2, \dots, k - 1$. Подставив полученное представление $\text{Mult}(\chi_t)$ в (22) и проведя необходимые сокращения, получим (36).

Результаты данного параграфа могут быть использованы для описания некоторых теоретико-автоматных свойств k -ЛРС. Полилинейный регистр сдвига $\langle I, \mathcal{F} \rangle$ над модулем ${}_R M$ можно рассматривать как неавтономный автомат с внутренним алфавитом $S = M^{|\mathcal{F}|} \setminus \{0\}$, внешним алфавитом $X = \{1, \dots, k\}$ и функцией перехода $h: X \times S \rightarrow S$, заданной следующим образом: $h(x, s) = \Phi_x(s)$, где Φ_x — соответствующий сопровождающий эндоморфизм (см. (5)).

Напомним, что сильно связным называется всякий автомат, граф которого сильно связан. Пусть $R = M = GF(2)$, $I = \mathfrak{R}_2(F_1(x_1), F_2(x_2))$ — идеал в $\mathfrak{R}_2$, порожденный реверсивными многочленами F_1 и F_2 степеней $h_1 > 0$ и $h_2 > 0$, соответственно,

$$\Pi = \{0, 1, \dots, h_1 - 1\} \times \{0, 1, \dots, h_2 - 1\} \subset \mathbb{N}_0^2$$

— параллелепипед. Пользуясь теоремой 1, легко показать, что пара $\langle I, \Pi \rangle$ образует унитарный 2-ЛРС. Ответим на следующий вопрос: может ли регистр сдвига $\langle I, \Pi \rangle$ являться сильно связным автоматом?

Предложение 6. *Регистр сдвига $\langle I, \Pi \rangle$ является сильно связным автоматом тогда и только тогда, когда F_1 и F_2 — примитивные многочлены и $h_1 = 1$ или $h_2 = 1$.*

Доказательство. Пусть $\langle I, \Pi \rangle$ — сильно связный автомат, T — период $\langle I, \Pi \rangle$. Напомним, что период $T(\mu)$ произвольной 2-ЛРП $\mu \in L_R(I)$ определяется как число различных элементов множества $\{x^i \mu[\Pi] : i \in \mathbb{N}_0^2\}$, причем $T(\mu) \mid T$. Так как F_1 и F_2 — реверсивные многочлены, сильная связность автомата $\langle I, \Pi \rangle$ равносильна существованию $\mu \in L_R(I)$ такой, что

$$T(\mu) = |R^{|\Pi|} \setminus \{0\}| = 2^{h_1 h_2} - 1.$$

Значит, $|R^{|\Pi|} \setminus \{0\}| \leq T$. Согласно следствию 3 и предложению 5, период T регистра сдвига $\langle I, \Pi \rangle$ удовлетворяет соотношению

$$T = T(F_1)T(F_2).$$

Тогда имеет место следующая цепочка неравенств

$$2^{h_1 h_2} - 1 \leq T \leq (2^{h_1} - 1)(2^{h_2} - 1) \leq 2^{h_1 h_2} - 1. \quad (44)$$

Отсюда следует, что

$$T = (2^{h_1} - 1)(2^{h_2} - 1) = 2^{h_1 h_2} - 1 = |R^{|\Pi|} \setminus \{0\}|.$$

Второе неравенство в цепочке (44) обращается в равенство тогда и только тогда, когда F_1 и F_2 — примитивные многочлены, а третье тогда и только тогда, когда $h_1 = 1$ или $h_2 = 1$.

Обратное утверждение очевидно.

Для получения других результатов по описанию теоретико-автоматных свойств полилинейных регистров сдвига необходимо более глубоко изучить связь периода k -ЛРС (для начала, правильного k -ЛРС) и периодических свойств его отдельных выходных последовательностей.

Автор выражает глубокую признательность А. А. Нечаеву за помощь в проведении исследований и ценные замечания по оформлению данной работы.

Список литературы

1. Атья М., Макдональд И., *Введение в коммутативную алгебру*. Мир, Москва, 1972.
2. Бухбергер Б., Коллинз Дж., Лоос Р., *Компьютерная алгебра*. Мир, Москва, 1986.
3. Глухов М. М., Елизаров В. П., Нечаев А. А., *Алгебра*, Ч. II. Москва, 1991.
4. Кокс Д., Литл Дж., О'Ши Д., *Идеалы, многообразия и алгоритмы*, Мир, Москва, 2000.
5. Кузьмин А. С., Куракин В. Л., Нечаев А. А., Псевдослучайные и полилинейные последовательности, *Труды по дискретной математике* (1997) бф1, 139–202.
6. Кузьмин А. С., Куракин В. Л., Нечаев А. А., Структурные, аналитические и статистические свойства линейных и полилинейных рекуррент. *Труды по дискретной математике* (2000) 3, 155–194.
7. Лидл Р., Нидеррайтер Г., *Конечные поля*. т. 1, 2. Мир, Москва, 1988.
8. Нечаев А. А., Конечные квазифробениусовы модули, приложения к кодам и линейным рекуррентам. *Фундаментальная и прикладная математика* (1995) 1, № 1, 229–254.
9. Adams W., Loustaunau P., *An introduction to Gröbner bases*. Amer. Math. Soc., Providence, 1994.
10. Becker T., Weispfenning V., *Gröbner bases: a computational approach to commutative algebra*. Springer, Berlin, 1993.
11. Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A., Linear recurring sequences over rings and modules. *J. Math. Sci.* 76 (1995), № 6, 2793–2915.
12. Kurakin V. L., Mikhalev A. V., Nechaev A. A., Polylinear recurring sequences over a bimodule. In: *Proc. 12 Int. Conf. on Formal Power Series Alg. Comb.*, 2000.
13. Mikhailov D. A., Polylinear shift registers and standard bases. In: *Proc. 12 Int. Conf. on Formal Power Series Alg. Comb.*, 2000.
14. Sakata S., Synthesis of two-dimensional linear feedback shift-registers and Gröbner bases. *Lect. Notes Comput. Sci.* (1989) 356, 394–407.
15. Sakata S., A Gröbner basis and a minimal polynomial set of a finite nD array. *Lect. Notes Comput. Sci.* (1991) 508, 280–291.

Статья поступила 11.09.2001.