Math-Net.Ru

Общероссийский математический портал

В. Л. Куракин, В. В. Вязович, Алгоритм построения аннулятора полилинейной рекуррентной последовательности над конечным коммутативным кольцом, *Дискрет. матем.*, 2011, том 23, выпуск 4, 134–157

DOI: <https://doi.org/10.4213/dm1167>

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: 54.198.67.100

26 апреля 2023 г., 17:04:27

Алгоритм построения аннулятора полилинейной рекуррентной последовательности над конечным коммутативным кольцом

© 2011 г. В. Л. Куракин, В. В. Вязович

Предлагается алгоритм, который строит систему образующих аннулятора полилинейной рекуррентной последовательности над конечным коммутативным кольцом с единицей. Трудоемкость алгоритма есть $O(l^3)$, где l — число элементов последовательности, необходимое для однозначного построения аннулятора.

Работа выполнена при поддержке грантом Президента Российской Федерации по поддержке научных школ НШ 4.2008.10.

1. Введение

Пусть R — коммутативное кольцо с единицей, $u = (u(0), u(1), \dots)$ — последовательность и $a(x) = a_m x^m + \dots + a_1 x + a_0 \in R[x]$ — многочлен над кольцом R . Говорят, что многочлен $a(x)$ аннулирует последовательность u , если

$$a_m u(i+m) + a_{m-1} u(i+m-1) + \dots + a_1 u(i+1) + a_0 u(i) = 0, \quad i \geq 0. \quad (1)$$

Множество всех многочленов, аннулирующих последовательность, образует идеал $\text{Ann } u$ в кольце $R[x]$, называемый ее аннулятором.

Если многочлен $a(x)$ унитарный ($a_m = 1$), говорят также, что $a(x)$ порождает последовательность u или является ее характеристическим многочленом, а последовательность u называют линейной рекуррентной последовательностью (ЛРП) порядка m . Вектор $(u(0), \dots, u(m-1)) \in R^m$ называют начальным вектором ЛРП u . Зная характеристический многочлен и начальный вектор, можно вычислить каждый знак $u(i)$ ЛРП u . Характеристический многочлен наименьшей степени называется минимальным многочленом последовательности.

Минимальный многочлен линейной рекуррентной последовательности порядка l может быть найден с помощью алгоритма Берлекэмпа–Мессис с трудоемкостью $O(l^2)$. Алгоритм разработан Берлекэмпом [1] как алгоритм декодирования кодов БЧХ и затем изложен в другой форме Мессис [8] как алгоритм, находящий минимальный многочлен последовательности или ее отрезка длины l над полем.

Алгоритм Берлекэмпа–Мессис исследовался и обобщался различными авторами. Так, в [9] алгоритм Берлекэмпа–Мессис разработан для случая последовательностей над кольцами вычетов $\mathbf{Z}_m$, а в [4, 5, 6] — для последовательностей над произвольным конечным

кольцом R с единицей. В [10]–[16], [18] алгоритм Берлекэмпа–Месси обобщен на случай полилинейных (многомерных) последовательностей над полем, а в [17] — на случай полилинейных последовательностей над кольцами вычетов $\mathbf{Z}_m$. Обзор работ по алгоритму Берлекэмпа–Месси можно найти в [5, 3].

В данной статье приводится алгоритм, который строит систему образующих аннулятора полилинейной рекуррентной последовательности над конечным коммутативным кольцом с единицей. Входом алгоритма являются начальные значения k -линейной рекуррентной последовательности u на некоторой диаграмме Ферре $\mathcal{F} \subset \mathbf{N}_0^k$, а выходом — система образующих аннулятора $\text{Ann } u$ в кольце $R[x]$. Трудоемкость алгоритма составляет $O(l^3)$, где $l = |\mathcal{F}|$ (поэтому мы не называем его алгоритмом Берлекэмпа–Месси, который должен иметь трудоемкость $O(l^2)$).

За основу взят алгоритм из [4, 5] для последовательностей над кольцом R , который обобщен на случай k -последовательностей. Алгоритм по существу представляет собой специальным образом организованное гауссовское исключение, применяемое к сдвигам k -последовательности u . Результатом является система образующих идеала $\text{Ann } u$.

Материал статьи организован следующим образом. В §2 излагаются необходимые сведения о полилинейных рекуррентных последовательностях. В §3 дается описание алгоритма, в §4 приводится его обоснование, а в §5 — подсчет трудоемкости. В §6 приводятся два примера применения алгоритма.

2. Полилинейные последовательности и диаграммы значений

Обозначим через $\mathbf{N}_0$ множество всех целых неотрицательных чисел. Векторы из $\mathbf{N}_0^k$ и их координаты будем обозначать в виде $\mathbf{a} = (a_1, \dots, a_k)$. Нулевой вектор обозначается через $\mathbf{0} = (0, \dots, 0)$.

Всюду далее R — конечное коммутативное кольцо с единицей. Произвольное отображение $u: \mathbf{N}_0^k \rightarrow R$ (см. [7, 2]) называется k -последовательностью над R . Множество всех k -последовательностей над кольцом R будем обозначать $R^{(k)}$. Суммой двух k -последовательностей $u, v \in R^{(k)}$ и произведением элемента $r \in R$ на k -последовательность называются k -последовательности $u + v$, ru со знаками

$$(u + v)(\mathbf{i}) = u(\mathbf{i}) + v(\mathbf{i}), \quad (ru)(\mathbf{i}) = ru(\mathbf{i}), \quad \mathbf{i} \in \mathbf{N}_0^k.$$

Пусть $<$ есть некоторое линейное упорядочение множества $\mathbf{N}_0^k$. Элементы произвольного конечного подмножества $M \subset \mathbf{N}_0^k$ можно расположить в порядке возрастания:

$$M = \{\mathbf{i}_1, \dots, \mathbf{i}_n\}, \quad \mathbf{i}_1 < \dots < \mathbf{i}_n.$$

Вектор

$$u[M] = (u(\mathbf{i}_1), \dots, u(\mathbf{i}_n)) \in R^n$$

будем называть диаграммой значений последовательности u на множестве M . Диаграмму значений, в которой $u(\mathbf{i}_s) = 0$, $1 \leq s \leq n$, будем называть нулевой и обозначать 0 .

В дальнейшем будут рассматриваться диаграммы значений на множествах M , являющихся диаграммами Ферре. Напомним, что диаграммой Ферре называется конечное подмножество $\mathcal{F} \subset \mathbf{N}_0^k$ такое, что

$$\forall \mathbf{i}, \mathbf{j} \in \mathbf{N}_0^k \quad \mathbf{i} + \mathbf{j} \in \mathcal{F} \Rightarrow \mathbf{i} \in \mathcal{F}.$$

Легко видеть, что пересечение диаграмм Ферре также является диаграммой Ферре. Будем считать, что пустое множество является диаграммой Ферре.

Суммой двух диаграмм значений $u_1[\mathcal{F}_1]$ и $u_2[\mathcal{F}_2]$ называется диаграмма значений на множестве $\mathcal{F} = \mathcal{F}_1 \cap \mathcal{F}_2$, определяемая равенствами

$$u[\mathcal{F}] = u_1[\mathcal{F}_1] + u_2[\mathcal{F}_2], \quad u(\mathbf{i}) = u_1(\mathbf{i}) + u_2(\mathbf{i}), \quad \mathbf{i} \in \mathcal{F}.$$

Произведением элемента $r \in R$ на диаграмму значений $u[\mathcal{F}]$ называется диаграмма значений $v[\mathcal{F}] = ru[\mathcal{F}]$ со знаками $v(\mathbf{i}) = ru(\mathbf{i})$, $\mathbf{i} \in \mathcal{F}$.

Опорным элементом диаграммы значений $u[\mathcal{F}]$ называется ее первый ненулевой элемент $u(\mathbf{r})$, $\mathbf{r} \in \mathcal{F}$, относительно упорядочения $<$: $u(\mathbf{r}) \neq 0$, $u(\mathbf{i}) = 0$ при всех $\mathbf{i} \in \mathcal{F}$, $\mathbf{i} < \mathbf{r}$. Вектор $\mathbf{r}$ будем называть индексом опорного элемента, будем также говорить, что опорный элемент находится в точке $\mathbf{r}$. Нулевая диаграмма значений не имеет опорного элемента.

Одной из операций описываемого ниже алгоритма является аннулирование опорного элемента диаграммы значений с помощью опорных элементов множества других диаграмм значений. Опишем эту операцию подробнее.

Пусть $u[\mathcal{F}]$ — диаграмма значений с опорным элементом $u(\mathbf{r})$, и пусть

$$U = \{u_i[\mathcal{F}_i]: i \in I\}$$

— конечное множество диаграмм значений. Обозначим через $U(\mathbf{r})$ множество диаграмм значений из U , у которых опорный элемент находится в точке $\mathbf{r}$. Не ограничивая общности, будем считать, что это первые m диаграмм значений: $U(\mathbf{r}) = \{u_1[\mathcal{F}_1], \dots, u_m[\mathcal{F}_m]\}$. Обозначим через $I_U(\mathbf{r})$ идеал кольца R , порожденный опорными элементами этих m диаграмм значений:

$$I_U(\mathbf{r}) = (u_1(\mathbf{r}), \dots, u_m(\mathbf{r})).$$

Идеал, порожденный пустым множеством, равен 0. Будем говорить, что опорный элемент $u(\mathbf{r})$ диаграммы значений $u[\mathcal{F}]$ можно аннулировать с помощью множества U , или что $u[\mathcal{F}]$ редуцируется множеством U , если $u(\mathbf{r}) \in I_U(\mathbf{r})$. Это означает, что

$$u(\mathbf{r}) = a_1 u_1(\mathbf{r}) + \dots + a_m u_m(\mathbf{r})$$

для некоторых $a_1, \dots, a_m \in R$. В этом случае диаграмма значений

$$v[\hat{\mathcal{F}}] = u[\mathcal{F}] - \sum_{i=1}^m a_i u_i[\mathcal{F}_i], \quad \hat{\mathcal{F}} = \mathcal{F} \cap \bigcap_{i=1}^m \mathcal{F}_i,$$

либо нулевая, либо имеет опорный элемент, индекс которого строго больше, чем у опорного элемента диаграммы значений $u[\mathcal{F}]$.

Введем следующее определение: k -последовательность $u \in R^{(k)}$ называется k -линейной рекуррентной последовательностью (k -ЛРП), если существуют унитарные многочлены $f_1(x), \dots, f_k(x) \in R[x]$ такие, что для любого числа s , $1 \leq s \leq k$, и любых фиксированных $i_0, \dots, i_{s-1}, i_{s+1}, \dots, i_k \geq 0$ последовательность v со знаками $v(i) = u(i_0, \dots, i_{s-1}, i, i_{s+1}, \dots, i_k)$, $i \geq 0$, есть ЛРП с характеристическим многочленом $f_s(x)$. Многочлены $f_1(x_1), \dots, f_k(x_k)$ из кольца многочленов $R[\mathbf{x}] = R[x_1, \dots, x_k]$ от k переменных называются элементарными характеристическими многочленами k -ЛРП u . Теория полилинейных рекуррентных последовательностей над кольцами и модулями развита в [7, 2].

Для вектора $\mathbf{r} = (r_1, \dots, r_k) \in \mathbf{N}_0^k$ обозначим через $\mathbf{x}^{\mathbf{r}}$ моном $\mathbf{x}^{\mathbf{r}} = x_1^{r_1} \dots x_k^{r_k}$ из $R[\mathbf{x}]$. Сдвигом k -последовательности $u \in R^{(k)}$ на вектор $\mathbf{r}$ называется k -последовательность $v = \mathbf{x}^{\mathbf{r}}u \in R^{(k)}$ со знаками

$$v(\mathbf{i}) = (\mathbf{x}^{\mathbf{r}}u)(\mathbf{i}) = u(\mathbf{i} + \mathbf{r}), \quad \mathbf{i} \in \mathbf{N}_0^k.$$

Произведением многочлена

$$f(\mathbf{x}) = \sum_{\mathbf{r} \in \mathbf{N}_0^k} a_{\mathbf{r}} \mathbf{x}^{\mathbf{r}} \in R[\mathbf{x}]$$

на k -последовательность u называется k -последовательность $v = f(\mathbf{x})u \in R^{(k)}$, определяемая равенством

$$v = \sum_{\mathbf{r} \in \mathbf{N}_0^k} a_{\mathbf{r}} \mathbf{x}^{\mathbf{r}} u.$$

Таким образом, v есть линейная комбинация сдвигов k -последовательности u с соответствующими коэффициентами многочлена $f(\mathbf{x})$. Знаки k -последовательности v определяются равенствами

$$v(\mathbf{i}) = (f(\mathbf{x})u)(\mathbf{i}) = \sum_{\mathbf{r} \in \mathbf{N}_0^k} a_{\mathbf{r}} u(\mathbf{i} + \mathbf{r}), \quad \mathbf{i} \in \mathbf{N}_0^k.$$

Если $f(\mathbf{x})u = 0$, то говорят, что многочлен $f(\mathbf{x})$ аннулирует k -последовательность u . Идеал

$$\text{Ann } u = \{f(\mathbf{x}) \in R[\mathbf{x}] : f(\mathbf{x})u = 0\} \triangleleft R[\mathbf{x}]$$

называется аннулятором k -последовательности u . Последовательность u есть k -ЛРП тогда и только тогда, когда $\text{Ann } u$ содержит унитарные многочлены вида $f_1(x_1), \dots, f_k(x_k)$.

Обозначим через $\mathbf{e}_s = (0, \dots, 0, 1, 0, \dots, 0) \in \mathbf{N}_0^k$ вектор, в котором единица находится на s -м месте, $1 \leq s \leq k$. Суммой двух подмножеств $A, B \subset \mathbf{N}_0^k$ назовем множество

$$A + B = \{\mathbf{a} + \mathbf{b} : \mathbf{a} \in A, \mathbf{b} \in B\}.$$

В частности, $\mathbf{a} + B = \{\mathbf{a}\} + B$. Легко показать, что сумма двух диаграмм Ферре есть диаграмма Ферре. Для диаграммы Ферре $\mathcal{F}$ множество

$$\Delta_s \mathcal{F} = (\mathbf{e}_s + \mathcal{F}) \setminus \mathcal{F}$$

назовем (внешней) границей в направлении s , $1 \leq s \leq k$, а множество

$$\Delta \mathcal{F} = \Delta_1 \mathcal{F} \cup \dots \cup \Delta_k \mathcal{F}$$

— (внешней) границей диаграммы Ферре $\mathcal{F}$.

Носителем многочлена

$$F(\mathbf{x}) = \sum_{\mathbf{i} \in \mathbf{N}_0^k} a_{\mathbf{i}} \mathbf{x}^{\mathbf{i}}$$

называется множество

$$\text{sup } F = \{\mathbf{i} \in \mathbf{N}_0^k : a_{\mathbf{i}} \neq 0\}.$$

Многочлен вида

$$F_{\mathbf{c}}(\mathbf{x}) = \mathbf{x}^{\mathbf{c}} - \sum_{\mathbf{i} \in \mathcal{F}} a_{\mathbf{i}} \mathbf{x}^{\mathbf{i}}, \quad \mathbf{c} \in \Delta \mathcal{F}, \quad (2)$$

называется $\mathcal{F}$ -унитарным. Другими словами, многочлен $\mathcal{F}$ -унитарен, если он имеет слагаемое $\mathbf{x}^{\mathbf{c}}$, где $\mathbf{c} \in \Delta \mathcal{F}$, и $\text{supp}(F(\mathbf{x}) - \mathbf{x}^{\mathbf{c}}) \subseteq \mathcal{F}$.

Набор многочленов (2), взятых по одному для каждого вектора $\mathbf{c} \in \Delta \mathcal{F}$, называется полной системой $\mathcal{F}$ -унитарных многочленов. Очевидно, если для некоторой диаграммы Ферре $\mathcal{F}$ идеал $\text{Ann } u$ содержит полную систему $\mathcal{F}$ -унитарных многочленов, то вся k -ЛРП u определяется диаграммой значений $u[\mathcal{F}]$. Такая диаграмма Ферре называется определяющей для k -ЛРП u .

Сдвигом множества $A \subset \mathbf{N}_0^k$ на вектор $\mathbf{i} \in \mathbf{N}_0^k$ назовем множество всех векторов $\mathbf{a} - \mathbf{i}$, $\mathbf{a} \in A$, принадлежащих $\mathbf{N}_0^k$. Этот сдвиг будем обозначать $A - \mathbf{i}$:

$$A - \mathbf{i} = \{\mathbf{a} - \mathbf{i} : \mathbf{a} \in A, \mathbf{a} - \mathbf{i} \in \mathbf{N}_0^k\}.$$

Разность двух подмножеств $A, B \subset \mathbf{N}_0^k$ определим равенством

$$A - B = \bigcap_{\mathbf{b} \in B} (A - \mathbf{b}).$$

Очевидно, если $\mathcal{F}$ — диаграмма Ферре, то $\mathcal{F} - B$ — диаграмма Ферре.

Если для k -последовательности u известна диаграмма значений $u[\mathcal{F}]$, то для сдвига $\mathbf{x}^{\mathbf{i}}u$ известна диаграмма значений $(\mathbf{x}^{\mathbf{i}}u)[\mathcal{F} - \mathbf{i}]$. Определим сдвиг диаграммы значений $u[\mathcal{F}]$ на вектор $\mathbf{i}$ равенством

$$\mathbf{x}^{\mathbf{i}} \cdot u[\mathcal{F}] = (\mathbf{x}^{\mathbf{i}}u)[\mathcal{F} - \mathbf{i}].$$

В более общей ситуации, определим произведение многочлена $f(\mathbf{x})$ на диаграмму значений $u[\mathcal{F}]$ равенством

$$f(\mathbf{x}) \cdot u[\mathcal{F}] = (f(\mathbf{x})u)[\mathcal{F} - \text{supp } f].$$

В этом определении, наряду с тем, что k -последовательность u умножается на многочлен $f(\mathbf{x})$, меняется и множество, на котором рассматривается диаграмма значений полученной в результате последовательности $f(\mathbf{x})u$: исходная диаграмма Ферре $\mathcal{F}$ сдвигается при умножении на каждый моном многочлена и берется пересечение полученных множеств $\mathcal{F} - \mathbf{i}$ для $\mathbf{i} \in \text{supp } f$.

Предложение 1. Пусть u — k -ЛРП с определяющей диаграммой $\mathcal{F}$. Если многочлен $f(\mathbf{x})$ и диаграмма Ферре $\mathcal{G}$ удовлетворяют условиям $f(\mathbf{x}) \cdot u[\mathcal{G}] = 0$, $\text{supp } f + \mathcal{F} \subseteq \mathcal{G}$, то $f(\mathbf{x}) \in \text{Ann } u$.

Доказательство. Из условия предложения следует, что $(f(\mathbf{x})u)[\mathcal{G} - \text{supp } f] = 0$, причем $\mathcal{G} - \text{supp } f \supseteq \mathcal{F}$. Поэтому $(f(\mathbf{x})u)[\mathcal{F}] = 0$. Так как $\mathcal{F}$ — определяющая диаграмма для u , то $\mathcal{F}$ также является определяющей диаграммой для $f(\mathbf{x})u$. Отсюда следует, что $f(\mathbf{x})u = 0$.

Упорядочение $<$ на $\mathbf{N}_0^k$ индуцирует упорядочение на множестве мономов кольца $R[\mathbf{x}]$, так что $\mathbf{x}^{\mathbf{i}} < \mathbf{x}^{\mathbf{j}}$ тогда и только тогда, когда $\mathbf{i} < \mathbf{j}$. Будем считать, что если a, b — ненулевые элементы кольца R , то $a\mathbf{x}^{\mathbf{i}} < b\mathbf{x}^{\mathbf{j}}$ ($a\mathbf{x}^{\mathbf{i}} \leq b\mathbf{x}^{\mathbf{j}}$) тогда и только тогда, когда $\mathbf{i} < \mathbf{j}$ (соответственно $\mathbf{i} \leq \mathbf{j}$). Старший коэффициент и старший член многочлена $f(\mathbf{x})$ относительно упорядочения $<$ будем обозначать $\text{LC}(f)$ и $\text{LT}(f)$ соответственно, а мультистепень многочлена f — через $\text{mdeg } f$. Таким образом,

$$\text{LT}(f) = \text{LC}(f)\mathbf{x}^{\text{mdeg } f}.$$

Упорядочение называется мономиальным, если для любых векторов $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbf{N}_0^n$ выполняется условие $\mathbf{0} < \mathbf{a}$, и из $\mathbf{a} < \mathbf{b}$ следует, что $\mathbf{a} + \mathbf{c} < \mathbf{b} + \mathbf{c}$. В дальнейшем предполагается, что упорядочение $<$ мономиально.

В дальнейшем под редуцированием многочлена $f(\mathbf{x})$ с помощью многочлена $g(\mathbf{x})$ будем понимать вычитание из $f(\mathbf{x})$ многочлена $at(\mathbf{x})g(\mathbf{x})$, где $a \in R$, $t(\mathbf{x}) \in R[\mathbf{x}]$ — моном, и $t(\mathbf{x}) \text{LT}(g) \leq \text{LT}(f)$. Под редуцированием многочлена $f(\mathbf{x})$ с помощью системы многочленов S будем понимать конечное число операций редуцирования многочлена $f(\mathbf{x})$ с помощью многочленов из S .

Ненулевой многочлен $f(\mathbf{x})$ назовем $<$ -унитарным, если $\text{LC}(f) = 1$. Многочлен назовем $(\mathcal{F}, <)$ -унитарным, если он $\mathcal{F}$ -унитарен и $<$ -унитарен. Многочлен вида (2) $(\mathcal{F}, <)$ -унитарен тогда и только тогда, когда $\text{LT}(f) = \mathbf{x}^{\mathbf{c}}$. В общем случае многочлен $f(\mathbf{x})$ является $(\mathcal{F}, <)$ -унитарным тогда и только тогда, когда $\text{LT}(f) = \mathbf{x}^{\mathbf{c}}$, $\mathbf{c} \in \Delta \mathcal{F}$, $\text{supp}(f(\mathbf{x}) - \mathbf{x}^{\mathbf{c}}) \subseteq \mathcal{F}$.

Предложение 2. Пусть $\mathcal{F}$ — диаграмма Ферре и

$$S = \{F_{\mathbf{c}}(\mathbf{x}) : \mathbf{c} \in \Delta \mathcal{F}\}$$

— полная система $(\mathcal{F}, <)$ -унитарных многочленов. Тогда любой многочлен из $R[\mathbf{x}]$ можно редуцировать с помощью этой системы к многочлену, носитель которого лежит в $\mathcal{F}$. Как следствие, если $I = (S)$ — идеал кольца $R[\mathbf{x}]$, порожденный системой S , то

$$\forall g(\mathbf{x}) \in R[\mathbf{x}] \quad \exists h(\mathbf{x}) \in R[\mathbf{x}] : g \equiv h \pmod{I}, \quad \text{supp } h \subseteq \mathcal{F}.$$

Доказательство. Обозначим через $m(g)$ максимальную относительно упорядочения $<$ мультистепень монома многочлена $g(\mathbf{x})$, не принадлежащую $\mathcal{F}$. Предположим, что существует многочлен $g(\mathbf{x}) \in R[\mathbf{x}]$, который нельзя редуцировать к многочлену с носителем в $\mathcal{F}$. Выберем такой многочлен $g(\mathbf{x})$ с наименьшим параметром $m(g)$. Пусть $m(g) = \mathbf{a}$. Тогда $\mathbf{a} \notin \mathcal{F}$, и существует вектор $\mathbf{c} \in \Delta \mathcal{F}$ такой, что $\mathbf{a} = \mathbf{b} + \mathbf{c}$ для некоторого $\mathbf{b} \in \mathbf{N}_0^k$. (Чтобы найти такой вектор $\mathbf{c}$, можно, к примеру, соединить точку $\mathbf{a}$ с началом координат отрезком в пространстве $\mathbf{R}^k$ и найти пересечение этого отрезка с границей диаграммы Ферре $\mathcal{F}$.) Так как многочлен $F_{\mathbf{c}}(\mathbf{x}) \in S$ является $<$ -унитарным, то и многочлен $\mathbf{x}^{\mathbf{b}} F_{\mathbf{c}}(\mathbf{x})$ является $<$ -унитарным, то есть его старший моном равен $\mathbf{x}^{\mathbf{b}+\mathbf{c}} = \mathbf{x}^{\mathbf{a}}$, а все остальные мономы меньше $\mathbf{x}^{\mathbf{a}}$ (так как упорядочение $<$ мономиальное).

Редуцируем многочлен $g(\mathbf{x})$ с помощью многочлена $F_{\mathbf{c}}(\mathbf{x})$, получив многочлен

$$h(\mathbf{x}) = g(\mathbf{x}) - \text{LC}(g)\mathbf{x}^{\mathbf{b}} F_{\mathbf{c}}(\mathbf{x}).$$

Очевидно, h нельзя редуцировать к многочлену с носителем в $\mathcal{F}$. При редуцировании моном мультистепени $m(g)$ сократился, и все мономы многочлена h меньше $\mathbf{a}$ или их мультистепени содержатся в $\mathcal{F}$. Поэтому $h(\mathbf{x})$ — многочлен с параметром $m(h) < \mathbf{a} = m(g)$, получаем противоречие.

3. Описание алгоритма

Элементы $a, b \in R$ называются ассоциированными, если $a = rb$ для некоторого $r \in R^*$, где R^* — множество обратимых элементов кольца R . Отношение ассоциированности является отношением эквивалентности и разбивает кольцо R на попарно не пересекающиеся классы ассоциированных элементов:

$$R = \{0\} \cup R_1 \cup \dots \cup R_N, \quad N \geq 1. \quad (3)$$

Выберем в каждом классе представителя $r_n \in R_n$, $1 \leq n \leq N$. Тогда $R_n = R^* r_n$. Один из классов ассоциированных элементов совпадает с R^* . Будем предполагать, что $R_1 = R^*$ и $r_1 = 1$.

В формулируемом ниже алгоритме рассматривается k -ЛРП u с определяющей диаграммой Ферре $\mathcal{F}$. Введем обозначение

$$\mathcal{F}_+ = \mathcal{F} \cup \Delta \mathcal{F}$$

и упорядочим элементы диаграммы Ферре $\mathcal{F}_+$ в порядке возрастания в соответствии с упорядочением $<$:

$$\mathcal{F}_+ = \mathcal{F} \cup \Delta \mathcal{F} = \{\mathbf{i}_0, \mathbf{i}_1, \dots, \mathbf{i}_{l-1}\}, \quad \mathbf{0} = \mathbf{i}_0 < \mathbf{i}_1 \dots < \mathbf{i}_{l-1}, \quad l = |\mathcal{F}_+|. \quad (4)$$

Обозначим через $\mathcal{G}$ диаграмму Ферре $\mathcal{G} = \mathcal{F} + \mathcal{F}_+$. Геометрически она представляет собой расширение диаграммы Ферре $\mathcal{F}$ примерно в два раза в каждом из k направлений. Тогда алгоритм выполняет l шагов, а входом алгоритма является диаграмма значений $u[\mathcal{G}]$.

Алгоритм заключается в заполнении N таблиц, где N — число классов ненулевых ассоциированных элементов кольца R . На шаге s алгоритма, $0 \leq s < l$, в таблицу с номером n , $1 \leq n \leq N$, вносится одна строка. Эта строка содержит диаграмму Ферре $\mathcal{F}_{sn}$, диаграмму значений $u_{sn}[\mathcal{F}_{sn}]$ и многочлен $f_{sn}(\mathbf{x})$. При этом выполняются следующие условия, которые должны проверяться на каждом шаге алгоритма:

$$\begin{aligned} \mathcal{F}_{sn} &\supseteq (\mathcal{G} - \mathbf{i}_0) \cap (\mathcal{G} - \mathbf{i}_1) \cap \dots \cap (\mathcal{G} - \mathbf{i}_s), \\ u_{sn}[\mathcal{F}_{sn}] &= f_{sn}(\mathbf{x}) \cdot u[\mathcal{G}], \\ \text{LT}(f_{sn}) &= r_n \mathbf{x}^{\mathbf{i}_s}, \quad \text{supp } f_{sn}(\mathbf{x}) \subseteq \mathcal{F}_+. \end{aligned} \quad (5)$$

Последнее условие означает, что мультистепени всех мономов многочлена f_{sn} лежат в $\mathcal{F}_+$ и не превосходят $\mathbf{i}_s$. Из первого условия и определения $\mathcal{G}$ следует, что $\mathcal{F}_{sn} \supseteq \mathcal{F}$. Поэтому, в силу предложения 1, если $u_{sn}[\mathcal{F}_{sn}] = 0$, то $f_{sn}(\mathbf{x}) \in \text{Ann } u$. Поскольку $\mathcal{F}$ — определяющая диаграмма Ферре для k -ЛРП u , то очевидно, что условие $u_{sn}[\mathcal{F}_{sn}] = 0$, ввиду включения $\mathcal{F} \subseteq \mathcal{F}_{sn}$, равносильно условию $u_{sn}[\mathcal{F}] = 0$.

Каждый шаг s алгоритма содержит некоторое конечное число j подшагов, $j = 0, 1, 2, \dots$, в ходе которых вырабатываются диаграмма Ферре $\mathcal{F}_{sn}^{(j)}$, диаграмма значений $u_{sn}^{(j)}[\mathcal{F}_{sn}^{(j)}]$ и многочлен $f_{sn}^{(j)}(\mathbf{x})$. Они удовлетворяют условиям, аналогичным (5). При этом $\mathcal{F}_{sn}, u_{sn}[\mathcal{F}_{sn}]$ и $f_{sn}(\mathbf{x})$ получаются на последнем подшаге j .

Результатом работы алгоритма является система многочленов $f_{sn}(\mathbf{x})$ для тех s и n , для которых $u_{sn}[\mathcal{F}_{sn}] = 0$. Как отмечено выше, такие многочлены $f_{sn}(\mathbf{x})$ принадлежат $\text{Ann } u$. Будет доказано, что на самом деле они порождают идеал $\text{Ann } u$.

Перейдем к описанию алгоритма.

Пусть u — k -ЛРП над кольцом R с определяющей диаграммой Ферре $\mathcal{F}$, для которой существует полная система $(\mathcal{F}, <)$ -унитарных многочленов из $\text{Ann } u$. Входом алгоритма является диаграмма значений $u[\mathcal{G}]$, где $\mathcal{G} = \mathcal{F} + \mathcal{F}_+$ и $\mathcal{F}_+ = \mathcal{F} \cup \Delta \mathcal{F}$.

Требуется построить систему образующих идеала $\text{Ann } u$.

Алгоритм заключается в последовательном выполнении шагов $s = 0, 1, \dots, l - 1$. Алгоритм останавливается после выполнения шага $s = l - 1$. Предварительно кольцо R разбивается на классы ассоциированных элементов (3), выбирается некоторое мономиальное упорядочение $<$, и элементы множества $\mathcal{F}_+$ упорядочиваются согласно (4).

Шаг 0. В строку $s = 0$ каждой таблицы с номером n , $1 \leq n \leq N$, заносим диаграмму Ферре $\mathcal{F}_{0n} = \mathcal{G}$, диаграмму значений $u_{0n}[\mathcal{F}_{0n}] = r_n u[\mathcal{G}]$ и многочлен $f_{0n}(\mathbf{x}) = r_n$. Условия (5) выполняются.

Шаг s ($1 \leq s < l$). Для каждой таблицы n , $1 \leq n \leq N$, выполняются следующие действия. Ниже для определенности считается, что таблицы обрабатываются по порядку. На самом деле, обработку таблиц можно выполнять независимо, в этом смысле алгоритм допускает распараллеливание на N процессоров.

1. Рассмотрим сдвиг $\mathbf{x}^{i_s} \cdot u[\mathcal{G}]$ исходной диаграммы значений $u[\mathcal{G}]$. Положим

$$\mathcal{F}_{sn}^{(0)} = \mathcal{G} - \mathbf{i}_s, \quad u_{sn}^{(0)}[\mathcal{F}_{sn}^{(0)}] = r_n \mathbf{x}^{i_s} \cdot u[\mathcal{G}], \quad f_{sn}^{(0)}(\mathbf{x}) = r_n \mathbf{x}^{i_s}.$$

Условия (5) выполняются.

2. Если $u_{sn}^{(0)}[\mathcal{F}] = 0$ (или, что равносильно, $u_{sn}^{(0)}[\mathcal{F}_{sn}^{(0)}] = 0$), то полагаем

$$\mathcal{F}_{sn} = \mathcal{F}_{sn}^{(0)}, \quad u_{sn}[\mathcal{F}_{sn}] = u_{sn}^{(0)}[\mathcal{F}_{sn}^{(0)}], \quad f_{sn}(\mathbf{x}) = f_{sn}^{(0)}(\mathbf{x}) \quad (6)$$

и переходим к обработке следующей таблицы $n + 1$ при $n < N$ или к следующему шагу $s + 1$ при $n = N$.

Если же $u_{sn}^{(0)}[\mathcal{F}] \neq 0$, то в диаграмме значений $u_{sn}^{(0)}[\mathcal{F}]$ есть опорный элемент $u_{sn}^{(0)}(\mathbf{k}_{sn}^{(0)}) \neq 0$, имеющий некоторый индекс $\mathbf{k}_{sn}^{(0)} \in \mathcal{F}$.

3. Рассмотрим множество

$$U_{s-1} = \{u_{tm}[\mathcal{F}_{tm}]: 0 \leq t < s, 1 \leq m \leq N\}$$

всех диаграмм значений, полученных на предыдущих шагах алгоритма во всех N таблицах. Пусть $I_{s-1}(\mathbf{k}_{sn}^{(0)})$ — идеал кольца R , порожденный теми опорными элементами диаграмм значений $u_{tm}[\mathcal{F}]$, $0 \leq t < s$, $1 \leq m \leq N$, которые имеют индекс $\mathbf{k}_{sn}^{(0)}$. Проверим условие

$$u_{sn}^{(0)}(\mathbf{k}_{sn}^{(0)}) \in I_{s-1}(\mathbf{k}_{sn}^{(0)}). \quad (7)$$

Если оно не выполняется, то опорный элемент диаграммы значений $u_{sn}^{(0)}[\mathcal{F}]$ нельзя аннулировать с помощью множества U_{s-1} . В этом случае выполняем присваивания (6) и переходим к обработке следующей таблицы $n + 1$ при $n < N$ или к следующему шагу $s + 1$ при $n = N$.

4. Если условие (7) выполняется, то опорный элемент диаграммы значений $u_{sn}^{(0)}[\mathcal{F}]$ можно аннулировать с помощью множества U_{s-1} . Пусть

$$U_{s-1}(\mathbf{k}_{sn}^{(0)}) = \{u_{s_i n_i}[\mathcal{F}_{s_i n_i}]: 1 \leq i \leq v\}$$

— множество всех диаграмм значений из U_{s-1} , у которых опорный элемент диаграммы значений $u_{in}[\mathcal{F}]$ имеет индекс $\mathbf{k}_{sn}^{(0)}$. Тогда

$$u_{sn}^{(0)}(\mathbf{k}_{sn}^{(0)}) = \sum_{i=1}^v a_i u_{s_i n_i}(\mathbf{k}_{sn}^{(0)})$$

для некоторых элементов $a_1, \dots, a_v \in R$. Полагаем

$$\begin{aligned} \mathcal{F}_{sn}^{(1)} &= \mathcal{F}_{sn}^{(0)} \cap \mathcal{F}_{s_1 n_1} \cap \dots \cap \mathcal{F}_{s_v n_v}, \\ u_{sn}^{(1)}[\mathcal{F}_{sn}^{(1)}] &= u_{sn}^{(0)}[\mathcal{F}_{sn}^{(0)}] - \sum_{i=1}^v a_i u_{s_i n_i}[\mathcal{F}_{s_i n_i}], \\ f_{sn}^{(1)}(\mathbf{x}) &= f_{sn}^{(0)}(\mathbf{x}) - \sum_{i=1}^v a_i f_{s_i n_i}(\mathbf{x}). \end{aligned} \quad (8)$$

Тогда у диаграммы значений $u_{sn}^{(1)}[\mathcal{F}]$ индекс $\mathbf{k}_{sn}^{(1)}$ опорного элемента больше, чем у диаграммы значений $u_{sn}^{(0)}[\mathcal{F}]$, то есть, $\mathbf{k}_{sn}^{(1)} > \mathbf{k}_{sn}^{(0)}$.

Докажем, что выполняются условия (5). Для диаграмм Ферре $\mathcal{F}_{sn}^{(0)}$ и $\mathcal{F}_{s_i n_i}$ условие (5) выполнено. Так как $s_i < s$, то и для диаграммы Ферре $\mathcal{F}_{sn}^{(1)}$ первое условие в (5) выполнено. В силу определения диаграммы значений $u_{sn}^{(1)}[\mathcal{F}_{sn}^{(1)}]$ и многочлена $f_{sn}^{(1)}(\mathbf{x})$ для них выполнено второе условие в (5). Согласно предыдущим шагам алгоритма, для многочленов $f_{sn}^{(0)}$ и $f_{s_i n_i}$ условие (5) выполнено:

$$\begin{aligned} \text{LT}(f_{sn}^{(0)}) &= r_n \mathbf{x}^{i_s}, & \text{supp } f_{sn}^{(0)} &\subseteq \mathcal{F}_+, \\ \text{LT}(f_{s_i n_i}) &= r_{n_i} \mathbf{x}^{i_{s_i}}, & \text{supp } f_{s_i n_i} &\subseteq \mathcal{F}_+. \end{aligned}$$

Носитель многочлена $f_{sn}^{(1)}$ содержится в объединении носителей этих многочленов, поэтому для многочлена $f_{sn}^{(1)}$ выполняется вторая часть третьего условия в (5). Так как $s_i < s$, то $i_{s_i} < i_s$, и вектор i_s больше, чем любой вектор из носителей многочленов $f_{s_i n_i}$. Отсюда вытекает, что старший член многочлена $f_{sn}^{(1)}$ равен старшему члену многочлена $f_{sn}^{(0)}$, а значит для многочлена $f_{sn}^{(1)}$ выполняется первая часть третьего условия в (5).

5. Для диаграммы значений $u_{sn}^{(1)}[\mathcal{F}_{sn}^{(1)}]$ проделываем те же действия (с очевидными заменами верхних индексов 0 на 1 и 1 на 2), что и для диаграммы значений $u_{sn}^{(0)}[\mathcal{F}_{sn}^{(0)}]$, — они изложены в пп. 2, 3, 4 алгоритма. Получим диаграмму значений $u_{sn}^{(2)}[\mathcal{F}_{sn}^{(2)}]$, для которой индекс $\mathbf{k}_{sn}^{(2)}$ опорного элемента диаграммы значений $u_{sn}^{(2)}[\mathcal{F}]$ больше, чем в диаграмме значений $u_{sn}^{(1)}[\mathcal{F}]$, то есть $\mathbf{k}_{sn}^{(2)} > \mathbf{k}_{sn}^{(1)}$. И так далее, до тех пор, пока при некотором $j = j_{sn}$, $0 \leq j_{sn} \leq |\mathcal{F}|$, получим диаграмму значений $u_{sn}^{(j)}[\mathcal{F}_{sn}^{(j)}]$, для которой диаграмма значений $u_{sn}^{(j)}[\mathcal{F}]$ либо равна 0, либо ее опорный элемент $u_{sn}^{(j)}(\mathbf{k}_{sn}^{(j)})$ нельзя аннулировать с помощью диаграмм значений, полученных на предыдущих шагах алгоритма. Это происходит в случае, когда этот опорный элемент не принадлежит идеалу $I_{s-1}(\mathbf{k}_{sn}^{(j)})$ кольца R , порожденному теми опорными элементами диаграмм значений $u_{tm}[\mathcal{F}]$, $0 \leq t < s$, $1 \leq m \leq N$, которые имеют индекс $\mathbf{k}_{sn}^{(j)}$. В этом случае, как и в пп. 2, 3, мы выполняем присваивания

$$\mathcal{F}_{sn} = \mathcal{F}_{sn}^{(j)}, \quad u_{sn}[\mathcal{F}_{sn}] = u_{sn}^{(j)}[\mathcal{F}_{sn}^{(j)}], \quad f_{sn}(\mathbf{x}) = f_{sn}^{(j)}(\mathbf{x}).$$

При этом выполняются условия (5). Затем переходим к обработке следующей таблицы $n + 1$ при $n < N$ или к следующему шагу $s + 1$ при $n = N$.

После выполнения $(l - 1)$ -го шага алгоритм останавливается.

Результатом работы алгоритма считается система многочленов $f_{sn}(\mathbf{x})$ для тех s и n , для которых $u_{sn}[\mathcal{F}_{sn}] = 0$ (или, что равносильно, $u_{sn}[\mathcal{F}] = 0$), $0 \leq s < l$, $1 \leq n \leq N$.

4. Обоснование алгоритма

Докажем, что многочлены, полученные как результат работы алгоритма, являются системой образующих идеала $\text{Ann } u$ кольца $R[\mathbf{x}]$.

Лемма 1. Пусть $J_{\mathbf{a}}(\mathbf{r})$, $\mathbf{a} \in \mathcal{F}_+ = \mathcal{F} \cup \Delta \mathcal{F}$, $\mathbf{r} \in \mathcal{F}$, — идеал кольца R , состоящий из всех элементов $v(\mathbf{r})$, где

$$\begin{aligned} v &= g(\mathbf{x})u, \quad g(\mathbf{x}) \in R[\mathbf{x}], \quad \text{supp } g \subseteq \mathcal{F}_+, \quad \text{mdeg } g \leq \mathbf{a}, \\ v(\mathbf{r}) &\text{ — опорный элемент для } v[\mathcal{F}]. \end{aligned} \tag{9}$$

Пусть $I_s(\mathbf{r})$ — идеал кольца R , порожденный теми опорными элементами диаграмм значений $u_{tn}[\mathcal{F}]$, $0 \leq t \leq s$, $1 \leq n \leq N$, полученных в ходе алгоритма, которые имеют индекс $\mathbf{r}$:

$$I_s(\mathbf{r}) = (u_{tn}(\mathbf{r}); 0 \leq t \leq s, 1 \leq n \leq N,$$

$$u_{tn}(\mathbf{r}) \text{ — опорный элемент диаграмм значений } u_{tn}[\mathcal{F}]).$$

Тогда

$$I_s(\mathbf{r}) = J_{\mathbf{i}_s}(\mathbf{r}), \quad 0 \leq s < l, \quad \mathbf{r} \in \mathcal{F}.$$

Доказательство. Из определения следует, что множество $J_{\mathbf{a}}(\mathbf{r})$ является идеалом кольца R . Докажем, что $I_s(\mathbf{r}) \subseteq J_{\mathbf{i}_s}(\mathbf{r})$. Пусть $u_{tn}(\mathbf{r})$ — опорный элемент некоторой диаграммы значений $u_{tn}[\mathcal{F}]$, $0 \leq t \leq s$, $1 \leq n \leq N$. Достаточно доказать, что $u_{tn}(\mathbf{r}) \in J_{\mathbf{i}_s}(\mathbf{r})$. Действительно, согласно (5) $u_{tn}[\mathcal{F}_{tn}] = f_{tn}(\mathbf{x}) \cdot u[\mathcal{G}]$, где $\text{supp } f_{tn} \subseteq \mathcal{F}_+$ и $\text{mdeg } f_{tn} \leq \mathbf{i}_t \leq \mathbf{i}_s$, причем $\mathcal{F} \subseteq \mathcal{F}_{tn}$. Тогда $f_{tn}(\mathbf{x})$ — один из многочленов $g(\mathbf{x})$, удовлетворяющих условиям (9) при $\mathbf{a} = \mathbf{i}_s$. Следовательно, $u_{tn}(\mathbf{r}) \in J_{\mathbf{i}_s}(\mathbf{r})$.

Обратное включение докажем индукцией по $s = 0, 1, \dots, l-1$.

Проверим, что $J_{\mathbf{i}_0}(\mathbf{r}) \subseteq I_0(\mathbf{r})$ для любого $\mathbf{r} \in \mathcal{F}$. Заметим, что $\mathbf{i}_0 = \mathbf{0}$, и многочлен $g(\mathbf{x})$, удовлетворяющий условиям (9) при $\mathbf{a} = \mathbf{0}$, есть константа $c \in R$. Поэтому идеал $J_0(\mathbf{r})$ состоит из всех элементов $v(\mathbf{r})$, где

$$v = cu, \quad c \in R, \quad v(\mathbf{r}) \text{ — опорный элемент для } v[\mathcal{F}].$$

Если $c = 0$, то $v(\mathbf{r}) = 0 \in I_0(\mathbf{r})$. Пусть $c \neq 0$. Тогда c принадлежит некоторому классу ассоциированных элементов R_n , $1 \leq n \leq N$. Поэтому $c = dr_n$ для некоторого $d \in R^*$. Согласно шагу 0 алгоритма, в n -й таблице находится диаграмма значений

$$u_{0n}[\mathcal{G}] = r_n u[\mathcal{G}] = d^{-1}cu[\mathcal{G}] = d^{-1}v[\mathcal{G}].$$

Поэтому элемент $d^{-1}v(\mathbf{r})$ принадлежит идеалу $I_0(\mathbf{r})$, а значит и $v(\mathbf{r}) \in I_0(\mathbf{r})$. Отсюда следует, что $J_0(\mathbf{r}) \subseteq I_0(\mathbf{r})$.

Предположим, что $I_t(\mathbf{r}) = J_{\mathbf{i}_t}(\mathbf{r})$ при всех $0 \leq t < s < l$, $\mathbf{r} \in \mathcal{F}$. Нужно доказать, что $J_{\mathbf{i}_s}(\mathbf{r}) \subseteq I_s(\mathbf{r})$ при всех $\mathbf{r} \in \mathcal{F}$.

Пусть $a \in J_{\mathbf{i}_s}(\mathbf{r})$, $a \neq 0$. Тогда существует многочлен $g(\mathbf{x}) \in R[\mathbf{x}]$ такой, что $\text{supp } g \subseteq \mathcal{F}_+$, $\text{mdeg } g \leq \mathbf{i}_s$ и элемент $a = v(\mathbf{r})$ — опорный для диаграммы значений $v[\mathcal{F}]$, где $v = g(\mathbf{x})u$.

Если $\text{mdeg } g \leq \mathbf{i}_t$ для некоторого $t < s$, то $a \in J_{\mathbf{i}_t}(\mathbf{r})$. Тогда по предположению индукции $a \in I_t(\mathbf{r})$. Так как в силу определения $I_t(\mathbf{r}) \subseteq I_{t+1}(\mathbf{r}) \subseteq \dots \subseteq I_s(\mathbf{r})$, то $a \in I_s(\mathbf{r})$ и все доказано.

Иначе многочлен g имеет вид

$$g(\mathbf{x}) = c\mathbf{x}^{\mathbf{i}_s} + g_1(\mathbf{x}), \quad c \in R \setminus 0, \quad \text{supp } g_1 \subseteq \mathcal{F}_+, \quad \text{mdeg } g_1 \leq \mathbf{i}_{s-1}.$$

Пусть $c = dr_n$, где $d \in R^*$, r_n — представитель класса R_n , $1 \leq n \leq N$.

Рассмотрим s -ю строку n -й таблицы, построенной в алгоритме. В ней находится диаграмма значений $u_{sn}[\mathcal{F}_{sn}] = f_{sn}(\mathbf{x}) \cdot u[\mathcal{G}]$, где согласно (5) $\text{LT}(f_{sn}) = r_n\mathbf{x}^{\mathbf{i}_s}$, $\text{supp } f_{sn} \subseteq \mathcal{F}_+$. Как и у многочлена $g(\mathbf{x})$, выделим у многочлена $f_{sn}(\mathbf{x})$ старший член:

$$f_{sn}(\mathbf{x}) = r_n\mathbf{x}^{\mathbf{i}_s} + f_1(\mathbf{x}), \quad \text{supp } f_1 \subseteq \mathcal{F}_+, \quad \text{mdeg } f_1 \leq \mathbf{i}_{s-1}.$$

Согласно алгоритму, диаграмма значений $u_{sn}[\mathcal{F}]$ либо нулевая (тогда и $u_{sn}[\mathcal{F}_{sn}]$ нулевая), либо имеет опорный элемент $b = u_{sn}(\mathbf{i})$, $\mathbf{i} = \mathbf{k}_{sn} \in \mathcal{F}$, который нельзя аннулировать с

помощью множества U_{s-1} всех диаграмм значений, полученных на предыдущих шагах алгоритма во всех N таблицах. Другими словами, $b \notin I_{s-1}(\mathbf{i})$. С другой стороны, $b \in I_s(\mathbf{i})$ по определению идеала $I_s(\mathbf{i})$. Таким образом,

$$b = u_{sn}(\mathbf{i}) \notin I_{s-1}(\mathbf{i}), \quad b \in I_s(\mathbf{i}). \quad (10)$$

Введем обозначение

$$h(\mathbf{x}) = g(\mathbf{x}) - df_{sn}(\mathbf{x}) = g_1(\mathbf{x}) - df_1(\mathbf{x}).$$

Тогда $\text{supp } h \subseteq \mathcal{F}_+$, $\text{mdeg } h \leq \mathbf{i}_{s-1}$. Рассмотрим k -ЛРП $w = h(\mathbf{x})u$. Для нее

$$w[\mathcal{F}] = (h(\mathbf{x})u)[\mathcal{F}] = (g(\mathbf{x})u)[\mathcal{F}] - (df_{sn}(\mathbf{x})u)[\mathcal{F}] = v[\mathcal{F}] - ru_{sn}[\mathcal{F}]. \quad (11)$$

Напомним, что в первой диаграмме значений опорный элемент $a = v(\mathbf{r})$, во второй $db = du_{sn}(\mathbf{i})$. Возможны три случая.

(а) $\mathbf{r} < \mathbf{i}$, включая случай $u_{sn}[\mathcal{F}] = 0$, то есть $\mathbf{i} = \infty$. Тогда диаграмма значений

$$w[\mathcal{F}] = (h(\mathbf{x})u)[\mathcal{F}], \quad \text{supp } h \subseteq \mathcal{F}_+, \quad \text{mdeg } h \leq \mathbf{i}_{s-1},$$

имеет опорный элемент $a = w(\mathbf{r})$. Следовательно, $a \in J_{\mathbf{i}_{s-1}}(\mathbf{r})$. По предположению индукции $a \in I_{s-1}(\mathbf{r})$. Так как $I_{s-1}(\mathbf{r}) \subseteq I_s(\mathbf{r})$, то $a \in I_s(\mathbf{r})$, что и требовалось доказать.

(б) $\mathbf{r} > \mathbf{i}$. Тогда диаграмма значений $w[\mathcal{F}] = (h(\mathbf{x})u)[\mathcal{F}]$ имеет опорный элемент, равный $-db = w(\mathbf{i})$. Следовательно, $-db \in J_{\mathbf{i}_{s-1}}(\mathbf{r})$. В силу предположения индукции $-db \in I_{s-1}(\mathbf{i})$. Поскольку элемент d обратим, то $b \in I_{s-1}(\mathbf{i})$, что противоречит (10). Таким образом, случай (б) невозможен.

(в) $\mathbf{r} = \mathbf{i}$. Тогда диаграмма значений $w[\mathcal{F}] = (h(\mathbf{x})u)[\mathcal{F}]$ имеет опорный элемент $a - db$, либо $a - db = 0$. В любом случае $a - db \in J_{\mathbf{i}_{s-1}}(\mathbf{r})$. По предположению индукции $a - db \in I_{s-1}(\mathbf{r})$. Так как $I_{s-1}(\mathbf{r}) \subseteq I_s(\mathbf{r})$, то $a - db \in I_s(\mathbf{r})$. Ввиду (10) получаем $a \in I_s(\mathbf{r})$, что и требовалось доказать.

Замечание 1. Обозначим через $J'_a(\mathbf{r})$, $\mathbf{a} \in \mathcal{F}_+$, $\mathbf{r} \in \mathcal{F}$, идеал кольца R , состоящий из всех элементов $v(\mathbf{r})$, где $v = g(\mathbf{x})u$, $g(\mathbf{x}) \in R[\mathbf{x}]$, $\text{mdeg } g \leq \mathbf{a}$, $v(\mathbf{r})$ — опорный элемент для $v[\mathcal{F}]$; отличие от (9) состоит в отсутствии условия $\text{supp } g \subseteq \mathcal{F}_+$. Тогда $J'_a(\mathbf{r}) = J_a(\mathbf{r})$.

Действительно, включение $J'_a(\mathbf{r}) \supseteq J_a(\mathbf{r})$ очевидно. Обратно, пусть $v(\mathbf{r}) \in J'_a(\mathbf{r})$ — опорный элемент диаграммы значений $v[\mathcal{F}]$, где $v = g(\mathbf{x})u$, $\text{mdeg } g \leq \mathbf{a}$. По условиям, сформулированным перед алгоритмом, существует полная система $(\mathcal{F}, <)$ -унитарных многочленов из $\text{Ann } u$, обозначим эту систему S . По предложению 2, существует многочлен $h(\mathbf{x}) \in R[\mathbf{x}]$, полученный из $g(\mathbf{x})$ редуцированием многочленами из S , такой, что $\text{supp } h \subseteq \mathcal{F}$. Так как $\text{mdeg } g \leq \mathbf{a}$, то при редуцировании из g вычитаются только многочлены мультистепеней, не превосходящих $\mathbf{a}$. Следовательно, $\text{mdeg } h \leq \mathbf{a}$. Так как $S \subseteq \text{Ann } u$, то $v = g(\mathbf{x})u = h(\mathbf{x})u$. Теперь по определению $v(\mathbf{r}) \in J_a(\mathbf{r})$.

Аналогично, пусть $J''_a(\mathbf{r})$, $\mathbf{a} \in \mathbf{N}_0^k$, $\mathbf{r} \in \mathcal{F}$, — идеал кольца R , состоящий из всех элементов $v(\mathbf{r})$, где $v = g(\mathbf{x})u$, $g(\mathbf{x}) \in R[\mathbf{x}]$, $\text{mdeg } g < \mathbf{a}$, $v(\mathbf{r})$ — опорный элемент для $v[\mathcal{F}]$; здесь отличие в условиях $\text{mdeg } g < \mathbf{a}$, $\mathbf{a} \in \mathbf{N}_0^k$ вместо $\text{mdeg } g \leq \mathbf{a}$, $\mathbf{a} \in \mathcal{F}_+$. Обозначим через $\mathbf{i}_l$ наибольший элемент из $\mathcal{F}_+$ такой, что $\mathbf{i}_l < \mathbf{a}$. Тогда $J''_a(\mathbf{r}) = J_{\mathbf{i}_l}(\mathbf{r})$.

Действительно, в предыдущих рассуждениях следует лишь учесть, что из условий $\text{supp } h \subseteq \mathcal{F}$, $\text{mdeg } h < \mathbf{a}$ следует, что $\text{mdeg } h \leq \mathbf{i}_l$. Как частный случай соотношения $J''_a(\mathbf{r}) = J_{\mathbf{i}_l}(\mathbf{r})$, получаем, что $J''_{\mathbf{i}_s}(\mathbf{r}) = J_{\mathbf{i}_{s-1}}(\mathbf{r})$, $1 \leq s < l$.

В дальнейшем через (S) будем обозначать идеал, порожденный множеством S . Если S — пустое множество, то по определению $(S) = 0$.

Теорема 1. Множество S всех многочленов $f_{sn}(\mathbf{x})$, $0 \leq s < l$, $1 \leq n \leq N$, построенных в алгоритме, таких, что $u_{sn}[\mathcal{F}] = 0$, является системой образующих идеала $\text{Ann } u$.

Доказательство. Согласно (5), $u_{sn}[\mathcal{F}_{sn}] = f_{sn}(\mathbf{x}) \cdot u[\mathcal{G}]$. Так как $\mathcal{G} = \mathcal{F} + \mathcal{F}_+$ и $\text{supp } f_{sn} \subseteq \mathcal{F}_+$, то $\text{supp } f_{sn} + \mathcal{F} \subseteq \mathcal{G}$. При этом $\mathcal{F} \subseteq \mathcal{F}_{sn}$. Поэтому в силу предложения 1, если $u_{sn}[\mathcal{F}] = 0$, то $f_{sn}(\mathbf{x}) \in \text{Ann } u$. Отсюда следует включение $(S) \subseteq \text{Ann } u$.

Докажем обратное включение, то есть что любой многочлен $g(\mathbf{x}) \in \text{Ann } u$ принадлежит (S) . Вначале рассмотрим многочлены, для которых $\text{supp } g \subseteq \mathcal{F}_+ = \mathcal{F} \cup \Delta\mathcal{F}$. Предположим противное. Тогда существует многочлен $g(\mathbf{x}) \in \text{Ann } u$ такой, что $\text{supp } g \subseteq \mathcal{F}_+$ и $g \notin (S)$. Возьмем такой многочлен g наименьшей (относительно упорядочения $<$) мультистепени. Пусть $\text{LT}(g) = c\mathbf{x}^{\mathbf{a}}$, $c \neq 0$, где $\mathbf{a} \in \mathcal{F}_+$ — мультистепень g . Элемент c принадлежит некоторому классу R_n ассоциированных элементов кольца R и $c = dr_n$, где $d \in R^*$. Так как $\mathbf{a} \in \mathcal{F}_+$, то, согласно (4), $\mathbf{a} = \mathbf{i}_s$ для некоторого s , $0 \leq s < l$. Рассмотрим s -ю строку n -й таблицы, построенной в алгоритме. В ней находится диаграмма значений $u_{sn}[\mathcal{F}_{sn}] = f_{sn}(\mathbf{x}) \cdot u[\mathcal{G}]$ и многочлен $f_{sn}(\mathbf{x})$, для которого согласно (5) $\text{LT}(f_{sn}) = r_n\mathbf{x}^{\mathbf{a}}$ и $\text{supp } f_{sn} \subseteq \mathcal{F}_+$. Выделив у многочлена $f_{sn}(\mathbf{x})$ старший член, запишем его в виде

$$f_{sn}(\mathbf{x}) = r_n\mathbf{x}^{\mathbf{a}} + f_1(\mathbf{x}), \quad \text{supp } f_1 \subseteq \mathcal{F}_+, \quad \text{mdeg } f_1 \leq \mathbf{i}_{s-1}.$$

Докажем, что $u_{sn}[\mathcal{F}] = 0$. Предположим противное. Тогда диаграмма значений $u_{sn}[\mathcal{F}]$ имеет опорный элемент $b = u_{sn}(\mathbf{i})$, $\mathbf{i} = \mathbf{k}_{sn} \in \mathcal{F}$, который нельзя аннулировать с помощью множества U_{s-1} всех диаграмм значений, полученных на предыдущих шагах алгоритма во всех N таблицах. Для элемента b выполняются соотношения (10): $b \notin I_{s-1}(\mathbf{i})$, $b \in I_s(\mathbf{i})$. Рассмотрим многочлен

$$h(\mathbf{x}) = g(\mathbf{x}) - df_{sn}(\mathbf{x}) = g_1(\mathbf{x}) - df_1(\mathbf{x}).$$

Тогда $\text{supp } h \subseteq \mathcal{F}_+$, $\text{mdeg } h \leq \mathbf{i}_{s-1}$ и

$$(h(\mathbf{x})u)[\mathcal{F}] = (g(\mathbf{x})u)[\mathcal{F}] - (df_{sn}(\mathbf{x})u)[\mathcal{F}] = 0 - du_{sn}[\mathcal{F}] = -du_{sn}[\mathcal{F}].$$

Последняя диаграмма значений имеет опорный элемент $-du_{sn}(\mathbf{i}) = -db$. По определению идеала $J_{i_{s-1}}(\mathbf{i})$ справедливо включение $-db \in J_{i_{s-1}}(\mathbf{i})$. В силу леммы и обратимости d справедливо включение $b \in I_{s-1}(\mathbf{i})$, что противоречит (10).

Тем самым доказано, что $u_{sn}[\mathcal{F}] = 0$. Тогда и $(h(\mathbf{x})u)[\mathcal{F}] = 0$, а значит, $h(\mathbf{x})$ принадлежит $\text{Ann } u$. Это противоречит тому, что $g(\mathbf{x})$ — многочлен наименьшей мультистепени из $\text{Ann } u$ такой, что $\text{supp } g \subseteq \mathcal{F}_+$. В итоге мы доказали, что любой многочлен $g(\mathbf{x}) \in \text{Ann } u$ такой, что $\text{supp } g \subseteq \mathcal{F}_+$, принадлежит (S) .

Заметим, что согласно условиям, сформулированным перед алгоритмом, k -ЛРП u имеет полную систему $(\mathcal{F}, <)$ -унитарных многочленов из $\text{Ann } u$. Обозначим многочлены из этой системы через $F_{\mathbf{c}}(\mathbf{x})$, как и в (2). Так как носитель $\mathcal{F}$ -унитарного многочлена лежит в $\mathcal{F}_+$, то из доказанного, в частности, следует, что все эти многочлены лежат в (S) .

Пусть теперь $g(\mathbf{x}) \in \text{Ann } u$ — произвольный многочлен. По предложению 2, многочлен g с помощью системы многочленов (2) можно редуцировать к многочлену, носитель которого лежит в $\mathcal{F}$. Следовательно,

$$g(\mathbf{x}) - \sum_{\mathbf{c} \in \Delta\mathcal{F}} F_{\mathbf{c}}(\mathbf{x})a_{\mathbf{c}}(\mathbf{x}) = h(\mathbf{x}), \quad \text{supp } h \subseteq \mathcal{F},$$

для некоторых многочленов $a_{\mathbf{c}}(\mathbf{x}) \in R[\mathbf{x}]$. Так как $F_{\mathbf{c}} \in \text{Ann } u$, то $h \in \text{Ann } u$. Тогда по доказанному $h \in (S)$. А так как $F_{\mathbf{c}} \in (S)$, то и $g \in (S)$.

Замечание 2. Доказательства леммы 1 и теоремы 1 не используют специфики конкретных вычислений, проводимых в алгоритме с диаграммами значений $u_{sn}[\mathcal{F}_{sn}]$ и многочленами f_{sn} . Эти вычисления проводятся в п. 1 алгоритма при присваивании $u_{sn}[\mathcal{F}_{sn}]$ и f_{sn} начальных значений, а также в формулах (8) при основных вычислениях. Лемма 1, замечание 1 и теорема 1 останутся верными, если в п. 1 алгоритма диаграмме значений $u_{sn}[\mathcal{F}_{sn}]$ и многочлену f_{sn} присвоить любые другие начальные значения, важно лишь, чтобы при этом выполнялись условия (5). Определенная свобода есть и в вычислениях, проводимых по формулам (8). При этом необходимо, чтобы сохранялись условия (5), последовательно аннулировались опорные элементы диаграмм значений $u_{sn}^{(j)}[\mathcal{F}_{sn}^{(j)}]$, и переход к следующему шагу алгоритма происходил только тогда, когда опорный элемент $u_{sn}^{(j)}(\mathbf{r})$ нельзя аннулировать опорными элементами из диаграмм значений, полученных на предыдущих шагах алгоритма.

Указанную свободу действий алгоритма можно использовать для того, чтобы уменьшать его трудоемкость, более удачно присваивая начальные значения и организуя вычисления с диаграммами значений $u_{sn}[\mathcal{F}_{sn}]$ и многочленами f_{sn} .

5. Трудоемкость алгоритма

Пусть $d(R)$ — длина кольца R , то есть длина его произвольного композиционного ряда идеалов (в силу теоремы Жордана–Гельдера, все такие ряды имеют одинаковую длину). Тогда каждый идеал I кольца R имеет систему образующих, состоящую не более чем из $d(R)$ элементов. Действительно, чтобы построить такую систему образующих, достаточно выбрать ненулевой элемент $a_1 \in I$, и затем выбирать элементы $a_2, a_3, \dots$ такие, что $a_{n+1} \notin I_n = (a_1, \dots, a_n)$. Тогда цепочка идеалов $I_1 \subseteq I_2 \subseteq \dots$ имеет длину не более $d(R)$ и стабилизируется на идеале I .

Если $0 = I_0 \subseteq I_1 \subseteq \dots \subseteq I_{d(R)} = R$ — композиционный ряд кольца R и p — наименьший простой делитель числа $|R|$, то индекс подгруппы I_{n-1} группы I_n удовлетворяет неравенству $[I_n : I_{n-1}] \geq p$. Следовательно, $|I_n| \geq p^n$, откуда следует, что $|R| \geq p^{d(R)}$, или $d(R) \leq \log_p |R|$. В частности, $d(R) \leq \log_2 |R|$.

Пусть $I = (r_1, \dots, r_n)$ — идеал кольца R , порожденный $n \leq d(R)$ элементами. Чтобы проверить, принадлежит ли элемент $r \in R$ идеалу I , и в случае $r \in I$ представить элемент r в виде $r = a_1 r_1 + \dots + a_n r_n$, где $a_1, \dots, a_n \in R$, достаточно выполнить перебор всех $|R|^n$ сумм $a_1 r_1 + \dots + a_n r_n$. Поскольку вычисление каждой такой суммы и сравнение ее с элементом r занимает $2n$ операций, то данная задача решается не более чем за $|R|^n \cdot 2n \leq |R|^{d(R)} \cdot 2d(R)$ операций. Для конкретного кольца R перебор может быть заменен другими вычислениями в кольце R , при этом трудоемкость уменьшится.

В п. 3 алгоритма выполняется проверка того, что опорный элемент диаграммы значений принадлежит идеалу $I_{s-1}(\mathbf{r})$ кольца R . Чтобы выполнить эту проверку, будем задавать этот идеал с помощью его системы образующих и строить идеалы $I_s(\mathbf{r})$ в процессе алгоритма. На s -м шаге алгоритма, $0 \leq s < l-1$, будем строить идеалы $I_s(\mathbf{r})$ для всех $\mathbf{r} \in \mathcal{F}$. Опишем эти построения.

Напомним, что идеал $I_s(\mathbf{r})$ порождается опорными элементами $u_{tn}(\mathbf{r})$ тех диаграмм значений $u_{tn}[\mathcal{F}]$, $0 \leq t \leq s$, $1 \leq n \leq N$, построенных на предыдущих шагах алгоритма, опорные элементы которых имеют индекс $\mathbf{r}$.

В начале работы алгоритма считаем, что все идеалы нулевые и системы их образующих пустые. После выполнения s -го шага алгоритма, $0 \leq s < l-1$, построены диаграммы значений $u_{sn}[\mathcal{F}]$, $1 \leq n \leq N$. Если $u_{sn}[\mathcal{F}] \neq 0$, то в этой диаграмме значений есть опорный элемент. Его индекс в алгоритме обозначался $\mathbf{r} = \mathbf{k}_{sn}$. Для $1 \leq n \leq N$ опорный элемент

$u_{sn}(\mathbf{k}_{sn})$ должен быть добавлен в систему образующих идеала $I_{s-1}(\mathbf{k}_{sn})$. Мы сделаем это, только если $u_{sn}(\mathbf{k}_{sn}) \notin I_{s-1}(\mathbf{k}_{sn})$, в противном случае добавление элемента к системе образующих не требуется, поскольку идеал от этого не изменится. Как отмечено выше, при этом система образующих идеала будет содержать не более $d(R)$ элементов.

После того, как все опорные элементы $u_{sn}(\mathbf{k}_{sn})$, $1 \leq n \leq N$, добавлены в идеалы $I_{s-1}(\mathbf{k}_{sn})$, эти идеалы становятся равными идеалам $I_s(\mathbf{r})$, $\mathbf{r} \in \mathcal{F}$. Вместе с элементом $u_{sn}(\mathbf{k}_{sn})$, входящим в систему образующих идеала, хранятся числа s, n , показывающие, из какой строки s и из какой таблицы n взят этот элемент. Идеалы $I_s(\mathbf{r})$ затем используются на $(s+1)$ -м шаге алгоритма.

Оценим трудоемкость алгоритма. Под операцией будем понимать любую из четырех арифметических операций в кольце R , операцию сравнения двух элементов кольца R , а также арифметическую операцию или операцию сравнения в кольце целых чисел. Мы не учитываем операции обращения в память, поскольку их число может быть существенно оптимизировано при конкретной реализации алгоритма.

Напомним, что в алгоритме рассматривается k -ЛРП u над кольцом R с определяющей диаграммой Ферре $\mathcal{F}$. Входом алгоритма является диаграмма значений $u[\mathcal{G}]$, где $\mathcal{G} = \mathcal{F} + \mathcal{F}_+$ и $\mathcal{F}_+ = \mathcal{F} \cup \Delta\mathcal{F}$. Введем обозначения

$$l = |\mathcal{F}_+|, \quad L = |\mathcal{G}|.$$

Теорема 2. Трудоемкость алгоритма оценивается сверху величиной $O(Ll^2)$ при $l \rightarrow \infty$. Константа при Ll^2 , без учета операций обращения в память, не превосходит $(4d(R) + 1)N$, где N — число классов ассоциированных ненулевых элементов кольца R , $d(R)$ — длина кольца R . При этом $N < |R|$ и $d(R) \leq \log_2 |R|$.

Доказательство. Вначале нужно представить кольцо R в виде объединения (3) классов попарно ассоциированных элементов. Это заведомо можно сделать за $|R|^2$ операций (составление таблицы Кэли). Трудоемкость данного этапа не зависит от l , то есть равна $O(1)$. В дальнейшем действия алгоритма, имеющие трудоемкость $O(1)$, не учитываются.

На шаге 0 алгоритма выполняется NL операций при вычислении диаграмм значений $u_{0n}[\mathcal{F}_{0n}] = r_n u[\mathcal{G}]$. Затем составляются системы образующих идеалов $I_0(\mathbf{r})$. Для этого в системы образующих этих идеалов добавляются опорные элементы указанных диаграмм значений, всего не более N элементов. Это требует не более $|R|^{d(R)} \cdot 2d(R)N = O(1)$ операций, где $|R|^{d(R)} \cdot 2d(R)$ — оценка трудоемкости проверки принадлежности элемента идеалу.

Рассмотрим шаг s алгоритма, $1 \leq s < l$. Оценим трудоемкость заполнения s -й строки в таблице с номером n , $1 \leq n \leq N$.

В п. 1 производится сдвиг $r_n \mathbf{x}^{i_s} \cdot u[\mathcal{G}]$ диаграммы значений $r_n u[\mathcal{G}]$, которая уже была вычислена на шаге 0 алгоритма. Остальные операции являются обращениями в память и нами не учитываются.

В п. 2 проверяется, является ли диаграмма значений $u_{sn}^{(0)}[\mathcal{F}]$ нулевой, что занимает не более L операций сравнения.

В пп. 3, 4 требуется устанавливать принадлежность элемента $r = u_{sn}^{(0)}(\mathbf{k}_{sn}^{(0)}) \in R$ идеалу $I = I_{s-1}(\mathbf{k}_{sn}^{(0)})$, заданному некоторой системой образующих $I = (u_1, \dots, u_v)$, и в случае $r \in I$ представлять элемент r в виде $r = a_1 u_1 + \dots + a_v u_v$, где $a_1, \dots, a_v \in R$. Это требует не более $|R|^v \cdot 2v \leq |R|^{d(R)} \cdot 2d(R)$ операций.

Далее в п. 4 производятся основные вычисления по формулам (8): не более $2vL \leq 2d(R)L$ операций для вычисления диаграммы значений $u_{sn}^{(1)}[\mathcal{F}_{sn}^{(1)}]$ и не более $2vl \leq 2d(R)l$ операций для вычисления многочленов $f_{sn}^{(1)}$ (напомним, что согласно (5)

носители этих многочленов содержатся в $\mathcal{F}_+$). Следовательно, трудоемкость пп. 3, 4 алгоритма не превосходит $|R|^{d(R)} \cdot 2d(R) + 2d(R)(L + l)$ операций. Первое слагаемое, равное $O(1)$, можно отбросить.

Согласно п. 5 алгоритма, п. 2 выполняется $j_{sn} + 1$ раз, а пп. 3, 4 выполняются j_{sn} раз, при этом $j_{sn} \leq |\mathcal{F}| < l$. Суммируя трудоемкости пп. 1–5, получим, что трудоемкость заполнения s -й строки n -ой таблицы оценивается величиной

$$L(j_{sn} + 1) + 2d(R)(L + l)j_{sn} \leq (4d(R) + 1)Ll.$$

Поскольку таблиц N штук, общая трудоемкость s -го шага алгоритма получается умножением на N . Получаем оценку $(4d(R) + 1)NlL$.

Кроме основных вычислений, изложенных в алгоритме, в конце s -го шага строятся системы образующих идеалов $I_s(\mathbf{r})$, $\mathbf{r} \in \mathcal{F}$. Для этого к системам образующих идеалов $I_{s-1}(\mathbf{r})$ добавляются опорные элементы диаграмм значений $u_{sn}[\mathcal{F}]$, $1 \leq n \leq N$. Как объяснялось для шага 0, это требует не более $|R|^{d(R)} \cdot 2d(R)N = O(1)$ операций.

Складывая трудоемкости всех шагов s , $0 \leq s < l$, получим, что трудоемкость алгоритма (с точностью до $O(Ll)$) не превосходит $(4d(R) + 1)NlL^2$.

Таким образом, трудоемкость алгоритма составляет $O(|\mathcal{F}|^3)$, где $\mathcal{F}$ — определяющая диаграмма Ферре k -ЛРП u . Поэтому по трудоемкости алгоритм нельзя отнести к классу алгоритмов Берлекэмп–Мессе, трудоемкость которых должна составлять $O(|\mathcal{F}|^2)$. Представляется, что трудоемкость можно снизить на порядок с помощью приемов, упоминавшихся выше в замечании 2.

6. Примеры

Рассмотрим примеры применения алгоритма. В первом примере рассматривается 2-ЛРП над полем $\mathbf{Z}_5$. На этом простом примере видно, как заполняются таблицы и как работает «гауссово исключение», постепенно увеличивающее число нулевых элементов в диаграммах значений. Основным является второй пример для 2-ЛРП над кольцом $\mathbf{Z}_4$, на котором демонстрируются все детали алгоритма. Пример над более сложным кольцом R будет аналогичным, лишь увеличится число таблиц и объем вычислений, поэтому мы ограничились примером над кольцом $\mathbf{Z}_4$.

Напомним, что алгоритм Берлекэмп–Мессе для 2-ЛРП над кольцами вычетов разработан Сакатой в [17]. Наш алгоритм, в случае поля или кольца вычетов, существенно отличается от алгоритмов Сакаты. Отметим также, что в [5] приведен пример применения алгоритма Берлекэмп–Мессе к 1-ЛРП над кольцом матриц.

Пример 1. Даны 40 знаков 2-ЛРП u над полем $\mathbf{Z}_5$:

1	2	3	4	3	2	4	2	1	2
3	1	4	0	4	4	3	2	0	2
1	2	3	0	3	3	1	4	0	4
2	4	1	0	1	1	2	3	0	3

Известно, что диаграмма Ферре

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

является определяющей для ЛРП u , причем существует полная система $(\mathcal{F}, <)$ -унитарных многочленов из $\text{Ann } u$, где $<$ — обратное лексикографическое упорядочение. Требуется построить систему образующих идеала $\text{Ann } u$.

Найдем диаграммы Ферре $\mathcal{F}_+ = \mathcal{F} \cup \Delta\mathcal{F}$, $\mathcal{G} = \mathcal{F} + \mathcal{F}_+$. Получаем следующий результат:

Входом алгоритма является диаграмма значений $u[\mathcal{G}]$:

$$u[\mathcal{G}] = \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 3 & 2 & 4 & 2 \\ 3 & 1 & 4 & 0 & 4 & 4 & 3 & \\ 1 & 2 & 3 & 0 & 3 & & & \\ 2 & 4 & 1 & & & & & \end{array}$$

Так как поле содержит один класс ненулевых ассоциированных элементов, то $N = 1$, и согласно алгоритму должна заполняться одна таблица. Каждая строка таблицы должна содержать диаграмму значений $u_{sn}[\mathcal{F}_{sn}]$ и многочлен $f_{sn}(\mathbf{x})$. С учетом того, что $N = n = 1$, будем опускать индекс n и использовать сокращенные обозначения $u_{sn}[\mathcal{F}_{sn}] = u_s$ и $f_{sn}(\mathbf{x}) = f_s$. Помимо u_s и f_s , в строку таблицы будем заносить число s , а также пояснение, какое действие выполняется на данном шаге или подшаге алгоритма.

Переменные в кольце многочленов будем обозначать x и y . Для обратного лексикографического упорядочения, $x < y$. Векторы в диаграмме Ферре $\mathcal{F}_+$ упорядочиваются согласно (4). Изобразим это:

$$\mathcal{F}_+ = \begin{array}{|c|c|c|c|c|} \hline 0 & 1 & 2 & 3 & 4 \\ \hline 5 & 6 & 7 & 8 & \\ \hline 9 & 10 & & & \\ \hline \end{array}$$

Например, $\mathbf{i}_6 = (1, 1)$, $\mathbf{i}_7 = (2, 1)$.

Алгоритм выполняет $|\mathcal{F}_+| = 11$ шагов, s -й шаг начинается со сдвига диаграммы значений $u[\mathcal{G}]$ на вектор $\mathbf{i}_s$, $s = 0, 1, \dots, 11$. Таким образом (см. п. 1 алгоритма),

$$u_s = \mathbf{x}^{\mathbf{i}_s} \cdot u[\mathcal{G}], \quad f_s = \mathbf{x}^{\mathbf{i}_s}.$$

Затем опорный элемент текущей диаграммы значений аннулируется с помощью диаграмм значений, полученных на предыдущих шагах алгоритма. Начнем заполнять таблицу.

s	u_s	f_s	действие
0	$\begin{array}{ccccccc} \textcircled{1} & 2 & 3 & 4 & 3 & 2 & 4 & 2 \\ 3 & 1 & 4 & 0 & 4 & 4 & 3 & \\ 1 & 2 & 3 & 0 & 3 & & & \\ 2 & 4 & 1 & & & & & \end{array}$	1	
1	$\begin{array}{ccccccc} 2 & 3 & 4 & 3 & 2 & 4 & 2 \\ 1 & 4 & 0 & 4 & 4 & 3 & \\ 2 & 3 & 0 & 3 & & & \\ 4 & 1 & & & & & \end{array}$	x	$-2u_0$
	$\begin{array}{ccccccc} 0 & \textcircled{4} & 3 & 0 & 1 & 0 & 4 \\ 0 & 2 & 2 & 4 & 1 & 0 & \\ 0 & 4 & 4 & 3 & & & \\ 0 & 3 & & & & & \end{array}$	$x - 2$	

На шаге $s = 0$ в первую строку таблицы занесены начальная диаграмма значений $u_0 = u[\mathcal{G}]$ и многочлен $f_0 = 1$.

Шаг $s = 1$ начинается со сдвига исходной диаграммы значений на $i_1 = (1, 0)$, то есть на 1 шаг влево. Опорный элемент 2 полученной диаграммы значений можно аннулировать с помощью опорного элемента диаграммы значений u_0 , для этого нужно вычесть $2u_0$. Это указано в таблице в столбце действие. Это действие проводится как с диаграммами значений, так и с соответствующими многочленами. Так как опорный элемент 4 нельзя аннулировать, шаг 1 заканчивается.

Для удобства опорные элементы диаграмм значений, которые нельзя аннулировать, обводятся кружочком. С помощью них будут аннулироваться опорные элементы диаграмм значений, получающихся на следующих шагах алгоритма.

s	u_s	f_s	действие
2	$\begin{array}{cccccc} 3 & 4 & 3 & 2 & 4 & 2 \\ 4 & 0 & 4 & 4 & 3 & \\ 3 & 0 & 3 & & & \\ 1 & & & & & \end{array}$	x^2	$+2u_0$
	$\begin{array}{cccccc} 0 & 3 & 4 & 0 & 0 & 1 \\ 0 & 2 & 2 & 4 & 1 & \\ 0 & 4 & 4 & & & \\ 0 & & & & & \end{array}$	$x + 2$	$+3u_1$
	$\begin{array}{cccccc} 0 & 0 & \textcircled{3} & 0 & 3 & 1 \\ 0 & 3 & 3 & 1 & 4 & \\ 0 & 1 & 1 & & & \\ 0 & & & & & \end{array}$	$x^2 + 3x + 1$	

Началом шага $s = 1$ является сдвиг исходной диаграммы значений на вектор $i_2 = (2, 0)$, то есть на 2 шага влево. Опорный элемент 3 аннулируется с помощью сложения с диаграммой значений $2u_0$. В полученной диаграмме опорный элемент 3 аннулируется с помощью прибавления $3u_1$. Те же действия проводятся с многочленами. Шаг 2 заканчивается, когда опорный элемент очередной диаграммы значений невозможно аннулировать с помощью диаграмм, полученных на предыдущих шагах алгоритма.

s	u_s	f_s	действие
3	$\begin{array}{cccccc} 4 & 3 & 2 & 4 & 2 & \\ 0 & 4 & 4 & 3 & & \\ 0 & 3 & & & & \end{array}$	x^3	$+u_0$
	$\begin{array}{cccccc} 0 & 0 & 0 & \textcircled{3} & 0 & \\ 3 & 0 & 3 & 3 & & \\ 1 & 0 & & & & \end{array}$	$x^3 + 1$	
4	$\begin{array}{cccc} 3 & 2 & 4 & 2 \\ 4 & 4 & 3 & \\ 3 & & & \end{array}$	x^4	$+2u_0$
	$\begin{array}{cccc} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & \\ 0 & & & \end{array}$	$x^4 + 2$	$+u_1$
	$\begin{array}{cccc} 0 & 0 & 3 & 0 \\ 0 & 3 & 3 & \\ 0 & & & \end{array}$	$x^4 + x$	$-u_2$
	$\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \\ 0 & & & \end{array}$	$x^4 - x^2 - 2x - 1$	

Шаги 3 и 4 проводятся аналогично. Результатом третьего шага является диаграмма значений, опорный элемент которой нельзя аннулировать. Результатом четвертого шага является нулевая диаграмма значений. Соответствующий многочлен f_4 войдет в систему образующих идеала $\text{Ann } u$. Как видно из проводимых действий, процедура аннулирования опорных элементов есть не что иное, как специальным образом организованное гауссово исключение. Порядок аннулирования элементов в диаграммах значений определяется выбранным упорядочением $<$.

s	u_s	f_s	действие
5	$\begin{array}{cccccc} 3 & 1 & 4 & 0 & 4 & 4 & 3 \\ 1 & 2 & 3 & 0 & 3 & & \\ 2 & 4 & 1 & & & & \end{array}$	y	$+2u_0$
	$\begin{array}{cccccc} 0 & 0 & 0 & 3 & 0 & 3 & 1 \\ 2 & 4 & 1 & 0 & 1 & & \\ 4 & 3 & 2 & & & & \end{array}$	$y + 2$	$-u_3$
	$\begin{array}{cccccc} 0 & 0 & 0 & 0 & 0 & & \\ \textcircled{4} & 4 & 3 & 2 & & & \\ 3 & 3 & & & & & \end{array}$	$y - x^3 + 1$	

Шаг $s = 5$ начинается со сдвига исходной диаграммы значений на вектор $i_5 = (0, 1)$, то есть, на 1 шаг вверх. Затем происходит аннулирование опорных элементов. Заметим, что на последнем подшаге вычитается диаграмма значений u_3 , меньшая по размерам, чем текущая диаграмма значений. В результате и диаграмма значений, полученная при вычитании, уменьшается по размерам. Определение диаграммы Ферре $\mathcal{G}$ и первое из условий (5) гарантируют, что при всех действиях алгоритма получающиеся диаграммы значений $u_s[\mathcal{F}_s]$ будут содержать диаграмму $u_s[\mathcal{F}]$ (то есть $\mathcal{F} \subseteq \mathcal{F}_s$). Поэтому из равенства $u_s[\mathcal{F}_s] = 0$ следует, что $u_s[\mathcal{F}] = 0$, и значит, $f_s \in \text{Ann } u$.

s	u_s	f_s	действие
6	$\begin{array}{cccccc} 1 & 4 & 0 & 4 & 4 & 3 \\ 2 & 3 & 0 & 3 & & \\ 4 & 1 & & & & \end{array}$	xy	$-u_0$
	$\begin{array}{cccccc} 0 & 2 & 2 & 0 & 1 & 1 \\ 4 & 2 & 1 & 3 & & \\ 3 & 4 & & & & \end{array}$	$xy - 1$	$+2u_1$
	$\begin{array}{cccccc} 0 & 0 & 3 & 0 & 3 & 1 \\ 4 & 1 & 0 & 1 & & \\ 3 & 2 & & & & \end{array}$	$xy + 2x$	$-u_2$
	$\begin{array}{cccccc} 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 3 & 2 & 0 & & \\ 3 & 1 & & & & \end{array}$	$xy - x^2 - x - 1$	$-u_5$
	$\begin{array}{cccccc} 0 & 0 & 0 & 0 & 0 & \\ 0 & \textcircled{4} & 4 & 3 & & \\ 0 & 3 & & & & \end{array}$	$xy - y + x^3 - x^2 - x - 2$	

В начале шага $s = 6$ берется сдвиг диаграммы значений $u[\mathcal{G}]$ на вектор $i_6 = (1, 1)$, то есть на 1 шаг вверх и влево. Этот шаг заканчивается диаграммой значений, в которой опорный элемент не может быть аннулирован. Обводим его кружочком для использования в последующих шагах алгоритма. Отметим, что в последнем действии размер диаграммы значений уменьшился.

s	u_s	f_s	действие
7	$\begin{array}{ccccc} 4 & 0 & 4 & 4 & 3 \\ 3 & 0 & 3 & & \\ 1 & & & & \end{array}$	x^2y	$+u_0$
	$\begin{array}{ccccc} 0 & 2 & 2 & 3 & 1 \\ 1 & 1 & 2 & & \\ 2 & & & & \end{array}$	$x^2y + 1$	$+2u_1$
	$\begin{array}{ccccc} 0 & 0 & 3 & 3 & 3 \\ 1 & 0 & 1 & & \\ 2 & & & & \end{array}$	$x^2y + 2x + 2$	$-u_2$
	$\begin{array}{ccccc} 0 & 0 & 0 & 3 & 0 \\ 1 & 2 & 3 & & \\ 2 & & & & \end{array}$	$x^2y - x^2 - x + 1$	$-u_3$
	$\begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 3 & 2 & 0 & & \\ 1 & & & & \end{array}$	$x^2y - x^3 - x^2 - x$	$+3u_5$
	$\begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 4 & & \\ 0 & & & & \end{array}$	$x^2y + 3y + x^3 - x^2 - x + 3$	$-u_6$
	$\begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & & \\ 0 & & & & \end{array}$	$x^2y - xy - y$	

Шаг $s = 7$ начинается со сдвига диаграммы значений $u[\mathcal{G}]$ на вектор $\mathbf{i}_7 = (2, 1)$, то есть на 1 шаг вверх и на 2 шага влево. Шаг заканчивается нулевой диаграммой значений и, следовательно, многочленом f_7 , который будет включен в систему образующих аннулятора.

s	u_s	f_s	действие
8	$\begin{array}{cccc} 0 & 4 & 4 & 3 \\ 0 & 3 & & \end{array}$	x^3y	$-u_1$
	$\begin{array}{cccc} 0 & 0 & 1 & 3 \\ 0 & 1 & & \end{array}$	$x^3y - x + 2$	$+3u_2$
	$\begin{array}{cccc} 0 & 0 & 0 & 3 \\ 0 & 0 & & \end{array}$	$x^3y + 3x^2 + 3x$	$-u_3$
	$\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 2 & 0 & & \end{array}$	$x^3y - x^3 + 3x^2 + 3x - 1$	$+2u_5$
	$\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & 3 & & \end{array}$	$x^3y + 2y + 2x^3 + 3x^2 + 3x + 1$	$+3u_6$
	$\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & 0 & & \end{array}$	$x^3y + 3xy - y$	
9	$\begin{array}{cccc} 1 & 2 & 3 & 0 & 3 \\ 2 & 4 & 1 & & \end{array}$	y^2	$-u_0$
	$\begin{array}{cccc} 0 & 0 & 0 & 1 & 0 \\ 4 & 3 & 2 & & \end{array}$	$y^2 - 1$	$+3u_3$
	$\begin{array}{cccc} 0 & 0 & 0 & 0 & 0 \\ 3 & 3 & 1 & & \end{array}$	$y^2 + 3x^3 + 2$	$+3u_5$
	$\begin{array}{cccc} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & & \end{array}$	$y^2 + 3y$	

На шагах 8 и 9 также получены многочлены, включаемые в систему образующих аннулятора. Проведем последний шаг алгоритма.

s	u_s	f_s	действие
10	$\begin{array}{cccc} 2 & 3 & 0 & 3 \\ 4 & 1 & & \end{array}$	xy^2	$+3u_0$
	$\begin{array}{cccc} 0 & 4 & 4 & 0 \\ 3 & 4 & & \end{array}$	$xy^2 + 3$	$-u_1$
	$\begin{array}{cccc} 0 & 0 & 1 & 0 \\ 3 & 2 & & \end{array}$	$xy^2 - x$	$+3u_2$
	$\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 3 & 1 & & \end{array}$	$xy^2 + 3x^2 + 3x + 3$	$+3u_5$
	$\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & 3 & & \end{array}$	$xy^2 + 3y - 3x^3 + 3x^2 + 3x + 1$	$+3u_6$
	$\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & 0 & & \end{array}$	$xy^2 + 3xy$	

Результатом алгоритма являются многочлены f_s , полученные на тех шагах s , для которых $u_s[\mathcal{F}] = 0$. В нашем случае это шаги с номерами $s = 4, 7, 8, 9, 10$. По теореме 1

$$\text{Ann } u = (f_4, f_7, f_8, f_9, f_{10}).$$

Остальные многочлены в алгоритме являлись вспомогательными, с их помощью строились многочлены, вошедшие в систему образующих аннулятора.

Заметим, что

$$f_8 = f_7 \cdot (x + 1), \quad f_{10} = f_9 \cdot x.$$

Поэтому

$$\text{Ann } u = (f_4, f_7, f_9) = (x^4 - x^2 - 2x - 1, x^2y - xy - y, y^2 + 3y).$$

Можно проверить, что эти многочлены образуют базис Гребнера.

Пример 2. Даны 24 знака 2-ЛРП u над кольцом $\mathbf{Z}_4$:

$$\begin{array}{|cccccc} \hline 2 & 3 & 3 & 1 & 3 & 1 \\ 3 & 2 & 0 & 0 & 0 & 0 \\ 1 & 0 & 2 & 2 & 2 & 2 \\ 1 & 0 & 2 & 2 & 2 & 2 \\ \hline \end{array}$$

Известно, что диаграмма Ферре

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

является определяющей для 2-ЛРП u , причем существует полная система $(\mathcal{F}, <)$ -унитарных многочленов из $\text{Ann } u$, где $<$ — обратное лексикографическое упорядочение. Требуется построить систему образующих идеала $\text{Ann } u$.

Найдем диаграммы Ферре

$$\mathcal{F}_+ = \mathcal{F} \cup \Delta \mathcal{F}, \quad \mathcal{G} = \mathcal{F} + \mathcal{F}_+.$$

Получим

$$\mathcal{F} = \begin{array}{|c|c|} \hline \square & \square \\ \hline \square & \\ \hline \end{array} \quad \mathcal{F}_+ = \begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & \square & \\ \hline \square & & \\ \hline \end{array} \quad \mathcal{G} = \begin{array}{|c|c|c|c|} \hline \square & \square & \square & \square \\ \hline \square & \square & \square & \\ \hline \square & \square & & \\ \hline \square & & & \\ \hline \end{array}$$

Входом алгоритма является диаграмма значений $u[\mathcal{G}]$:

$$u[\mathcal{G}] = \begin{array}{|c|c|c|c|c|} \hline 2 & 3 & 3 & 1 & \\ \hline 3 & 2 & 0 & & \\ \hline 1 & 0 & & & \\ \hline 1 & & & & \\ \hline \end{array}$$

Разобьем кольцо $\mathbf{Z}_4$ на классы ассоциированных элементов:

$$\mathbf{Z}_4 = \{0\} \cup \{1, 3\} \cup \{2\}.$$

Число классов ненулевых ассоциированных элементов $N = 2$, поэтому в алгоритме будут заполняться две таблицы.

Векторы в диаграмме Ферре $\mathcal{F}_+$ упорядочиваются согласно (4):

$$\mathcal{F}_+ = \begin{array}{|c|c|c|} \hline 0 & 1 & 2 \\ \hline 3 & 4 & \\ \hline 5 & & \\ \hline \end{array}$$

Алгоритм выполняет $|\mathcal{F}_+| = 6$ шагов. Началом s -го шага является сдвиг на вектор $\mathbf{i}_s$ диаграмм значений $u[\mathcal{G}]$ и $2u[\mathcal{G}]$ соответственно в первой и второй таблицах. Затем опорные элементы этих диаграмм значений аннулируются с помощью диаграмм значений, полученных на предыдущих шагах алгоритма в обеих таблицах.

Начнем заполнять таблицы. Слева располагается таблица с номером $n = 1$, справа — с номером $n = 2$.

s	u_{s1}	f_{s1}	действие	s	u_{s2}	f_{s2}	действие
0	$\begin{array}{ c c c c c } \hline \textcircled{2} & 3 & 3 & 1 & \\ \hline 3 & 2 & 0 & & \\ \hline 1 & 0 & & & \\ \hline 1 & & & & \\ \hline \end{array}$	1		0	$\begin{array}{ c c c c c } \hline 0 & \textcircled{2} & 2 & 2 & \\ \hline 2 & 0 & 0 & & \\ \hline 2 & 0 & & & \\ \hline 2 & & & & \\ \hline \end{array}$	2	
1	$\begin{array}{ c c c } \hline \textcircled{3} & 3 & 1 \\ \hline 2 & 0 & \\ \hline 0 & & \\ \hline \end{array}$	x		1	$\begin{array}{ c c c } \hline 2 & 2 & 2 \\ \hline 0 & 0 & \\ \hline 0 & & \\ \hline \end{array}$	$2x$	$+u_{01}$
2	$\begin{array}{ c c } \hline 3 & 1 \\ \hline 0 & \\ \hline \end{array}$ $\begin{array}{ c c } \hline 0 & 2 \\ \hline 2 & \\ \hline \end{array}$ $\begin{array}{ c c } \hline 0 & 0 \\ \hline 0 & \\ \hline \end{array}$	x^2 $x^2 - x$ $x^2 - x + 2$	$-u_{11}$ $+u_{02}$	2	$\begin{array}{ c c c } \hline 0 & \textcircled{1} & 1 \\ \hline 3 & 2 & \\ \hline 1 & & \\ \hline \end{array}$ $\begin{array}{ c c } \hline 2 & 2 \\ \hline 0 & \\ \hline \end{array}$ $\begin{array}{ c c } \hline 0 & 1 \\ \hline 3 & \\ \hline \end{array}$ $\begin{array}{ c c } \hline 0 & 0 \\ \hline 0 & \\ \hline \end{array}$	$2x + 1$ $2x^2$ $2x^2 + 1$ $2x^2 + 2x$	$+u_{01}$ $-u_{12}$

На шаге $s = 0$ в первую таблицу занесены начальная диаграмма значений $u_{01} = u[\mathcal{G}]$ и многочлен $f_{01} = 1$, а во вторую — диаграмма значений $u_{02} = 2u[\mathcal{G}]$ и многочлен $f_{02} = 2$. Кругжками отмечены опорные элементы.

На шаге $s = 1$ исходные диаграммы значений сдвигаются на вектор $\mathbf{i}_1 = (1, 0)$, то есть на 1 шаг влево. В первой таблице опорный элемент 3 нельзя аннулировать, он отмечен кругжком. Во второй таблице опорный элемент 2 можно аннулировать с помощью диаграммы значений u_{01} , полученной на шаге $s = 0$ в первой таблице. В получающейся

диаграмме значений опорный элемент 1 уже нельзя аннулировать, поэтому он отмечен кружком.

Обратим внимание, что опорные элементы 3 и 1, полученные в диаграммах значений на шаге 1 и отмеченные кружком, находятся на тех же местах, что и опорные элементы, равные 2, в диаграммах значений на нулевом шаге алгоритма. Однако, эти элементы не могут быть аннулированы, поскольку они не лежат в идеале, порожденном элементом 2.

Шаг $s = 2$ начинается со сдвига исходной диаграммы значений на вектор $\mathbf{i}_2 = (2, 0)$, то есть на 2 шага влево. Затем опорные элементы дважды аннулируются, в результате чего получается нулевая диаграмма значений. Соответствующие действия проводятся и с многочленами. Во второй таблице действия аналогичны, и также получается нулевая диаграмма. Поэтому многочлены f_{21} и f_{22} войдут в систему образующих идеала $\text{Ann } u$.

s	u_{s1}	f_{s1}	действие
3	$\begin{array}{ccc} 3 & 2 & 0 \\ 1 & 0 & \\ 1 & & \end{array}$	y	$-u_{11}$
	$\begin{array}{ccc} 0 & 3 & 3 \\ 3 & 0 & \\ 1 & & \end{array}$	$y - x$	$+u_{12}$
	$\begin{array}{ccc} 0 & 0 & 0 \\ 2 & 2 & \end{array}$	$y + x + 1$	

s	u_{s2}	f_{s2}	действие
3	$\begin{array}{ccc} 2 & 0 & 0 \\ 2 & 0 & \\ 2 & & \end{array}$	$2y$	$+u_{01}$
	$\begin{array}{ccc} 0 & 3 & 3 \\ 1 & 2 & \\ 3 & & \end{array}$	$2y + 1$	$+u_{12}$
	$\begin{array}{ccc} 0 & 0 & 0 \\ 0 & 0 & \\ 0 & & \end{array}$	$2y + 2x + 2$	

На шаге $s = 3$ берется сдвиг диаграмм значений $u^{[9]}$ и $2u^{[9]}$ на вектор $\mathbf{i}_3 = (0, 1)$, то есть на 1 шаг вверх. После вычислений в первой таблице получаем диаграмму значений, опорный элемент которой нельзя аннулировать, а во второй — нулевую диаграмму значений. Соответствующий многочлен f_{32} войдет в систему образующих идеала $\text{Ann } u$.

s	u_{s1}	f_{s1}	действие
4	$\begin{array}{cc} 2 & 0 \\ 0 & \end{array}$	xy	$+u_{01}$
	$\begin{array}{cc} 0 & 3 \\ 3 & \end{array}$	$xy + 1$	$+u_{12}$
	$\begin{array}{cc} 0 & 0 \\ 2 & \end{array}$	$xy + 2x + 2$	$+u_{31}$
	$\begin{array}{cc} 0 & 0 \\ 0 & \end{array}$	$xy + y - x - 1$	

s	u_{s2}	f_{s2}	действие
4	$\begin{array}{cc} 0 & 0 \\ 0 & \end{array}$	$2xy$	

Началом шага $s = 4$ является сдвиг исходной диаграммы значений на вектор $\mathbf{i}_4 = (1, 1)$, то есть на 1 шаг влево и на 1 шаг вверх. Затем происходит аннулирование опорных элементов до нулевой диаграммы значений. Во второй таблице диаграмма значений сразу нулевая, никаких действий не производится. Многочлены f_{41} и f_{42} войдут в систему образующих идеала $\text{Ann } u$.

s	u_{s1}	f_{s1}	действие
5	$\begin{array}{cc} 1 & 0 \\ 1 & \end{array}$	y^2	$+u_{11}$
	$\begin{array}{cc} 0 & 3 \\ 3 & \end{array}$	$y^2 + x$	$+u_{12}$
	$\begin{array}{cc} 0 & 0 \\ 2 & \end{array}$	$y^2 + 3x + 1$	$+u_{31}$
	$\begin{array}{cc} 0 & 0 \\ 0 & \end{array}$	$y^2 + y + 2$	

s	u_{s2}	f_{s2}	действие
5	$\begin{array}{cc} 2 & 0 \\ 2 & \end{array}$	$2y^2$	$+u_{01}$
	$\begin{array}{cc} 0 & 3 \\ 1 & \end{array}$	$2y^2 + 1$	$+u_{12}$
	$\begin{array}{cc} 0 & 0 \\ 0 & \end{array}$	$2y^2 + 2x + 2$	

На заключительном шаге $s = 5$ берется сдвиг диаграмм значений $u[\mathcal{G}]$ и $2u[\mathcal{G}]$ на вектор $\mathbf{i}_5 = (0, 2)$, то есть на 2 шага вверх. В результате этого шага также получаем нулевые диаграммы значений в обеих основных таблицах, поэтому многочлены f_{51} и f_{52} войдут в систему образующих идеала $\text{Ann } u$.

Как видно из примера, диаграммы значений и многочлены в первой и второй таблицах взаимодействуют друг с другом: к диаграммам из второй таблицы прибавляются диаграммы из первой таблицы, и наоборот. В частности, вычисления в первой и второй таблицах нельзя проводить независимо (полностью распараллелить). Более точно, можно распараллелить вычисления, но не данные: вычисления на каждом s -м шаге в первой и второй таблице можно проводить параллельно, но в вычислениях для каждой таблицы будут использоваться данные из обеих таблиц.

Многочлены во второй таблице, согласно (5), всегда имеют четный старший коэффициент. При этом, как видно из таблиц, другие их коэффициенты могут быть нечетными.

Результатом алгоритма являются многочлены f_{sn} , для которых $u_{sn}[\mathcal{F}] = 0$. В нашем случае такие многочлены получаются в первой таблице на шагах $s = 2, 4, 5$ и во второй таблице на шагах $s = 2, 3, 4, 5$. По теореме 1

$$\begin{aligned}\text{Ann } u &= (f_{21}, f_{41}, f_{51}, f_{22}, f_{32}, f_{42}, f_{52}) \\ &= (x^2 - x + 2, xy + y - x - 1, y^2 + y + 2, \\ &\quad 2x^2 + 2x, 2y + 2x + 2, 2xy, 2y^2 + 2x + 2).\end{aligned}$$

Непосредственно видно, что многочлены f_{22} , f_{42} , f_{52} выражаются через другие многочлены:

$$\begin{aligned}f_{22} &= 2f_{21}, \\ f_{42} &= 2f_{41} + f_{32}, \\ f_{52} &= 2f_{51} + f_{32},\end{aligned}$$

поэтому их можно исключить из системы образующих. В результате

$$\begin{aligned}\text{Ann } u &= (f_{21}, f_{41}, f_{51}, f_{32}) \\ &= (x^2 - x + 2, xy + y - x - 1, y^2 + y + 2, 2y + 2x + 2).\end{aligned}$$

Список литературы

1. Берлекэмп Э., *Алгебраическая теория кодирования*. Мир, Москва, 1971.
2. Кузьмин А. С., Куракин В. Л., Нечаев А. А., Псевдослучайные и полилинейные последовательности. *Труды по дискретной математике* (1997) **1**, 139–202.
3. Куракин В. Л., Алгоритм Берлекэмпа–Мессии над коммутативными артиновыми кольцами главных идеалов. *Фундаментальная и прикладная математика* (1999) **5**, №4, 1061–1101.
4. Куракин В. Л., Алгоритм Берлекэмпа–Мессии над конечными коммутативными кольцами. *Проблемы передачи информации* (1999) **35**, №2, 38–50.
5. Куракин В. Л., Алгоритм Берлекэмпа–Мессии над конечными кольцами, модулями и бимодулями. *Дискретная математика* (1998) **10**, №4, 3–34.
6. V. L. Kurakin, Construction of the annihilator of a linear recurring sequence over finite module with the help of the Berlekamp–Massey algorithm. In: *Proc. FPSAC'00* (Krob D. et al., eds.). Springer, Berlin, 2000, pp. 476–483.

7. Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A., Linear recurring sequences over rings and modules. *J. Math. Sci.* (1995) **76**, 2793–2915.
8. Massey J. L., Shift-register synthesis and BCH decoding. *IEEE Trans. Inform. Theory* (1969) **15**, 122–127.
9. Reeds J. A., Sloane N. J. A., Shift-register synthesis (modulo m). *SIAM J. Comput.* (1985) **14**, 505–513.
10. Sakata S., On determining the independent point set for doubly periodic arrays and encoding two-dimensional cyclic codes and their duals. *IEEE Trans. Inform. Theory* (1981) **27**, 556–565.
11. Sakata S., Finding a minimal set of linear recurring relations capable of generating a given finite two dimensional array. *J. Symbolic Comput.* (1988) **5**, 321–337.
12. Sakata S., Synthesis of two-dimensional linear feedback shift registers and bases. *Lect. Notes Comput. Sci.* (1989) **356**, 394–407.
13. Sakata S., N -dimensional Berlekamp–Massey algorithm for multiple arrays and construction of multivariate polynomials with preassigned zeros. *Lect. Notes Comput. Sci.* (1989) **357**, 356–376.
14. Sakata S., Extension of the Berlekamp–Massey algorithm to N dimensions. *Inform. Comput.* (1990) **84**, 207–239.
15. Sakata S., A Gröbner basis and a minimal polynomial set of a finite nD array. *Lect. Notes Comput. Sci.* (1991) **508**, 280–291.
16. Sakata S., Finding a minimal polynomial vector set of a vector of nD arrays. *Lect. Notes Comput. Sci.* (1991) **539**, 414–425.
17. Sakata S., Two-dimensional shift register synthesis and Gröbner bases for polynomial ideals over an integer residue ring. *Discrete Appl. Math.* (1991) **33**, 191–203.
18. Sakata S., The BM algorithm and the BMS algorithm. In: *Codes, Curves, and Signals. Common Threads in Communications* (Vardy A., ed.). Kluwer, Boston, 1998, pp. 39–52.

Статья поступила 1.02.2010.