Math-Net.Ru

Общероссийский математический портал

Д. А. Михайлов, А. А. Нечаев, Решение системы полиномиальных уравнений над кольцом Галуа–Эйзенштейна с помощью канонической системы образующих полиномиального идеала, *Дискрет. матем.*, 2004, том 16, выпуск 1, 21–51

DOI: <https://doi.org/10.4213/dm141>

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: 3.81.55.215

26 апреля 2023 г., 15:19:41

Решение системы полиномиальных уравнений над кольцом Галуа–Эйзенштейна с помощью канонической системы образующих полиномиального идеала

© 2004 г. Д. А. Михайлов, А. А. Нечаев

Кольцом Галуа–Эйзенштейна или GE-кольцом названо конечное коммутативное цепное кольцо R . Для перечисления всех решений системы полиномиальных уравнений над R сначала рассматривается общий метод покоординатной линеаризации, сводящийся к решению системы полиномиальных уравнений над соответствующим полем вычетов $\bar{R} = GF(q)$ и последующему решению серии систем линейных уравнений над тем же полем. Затем, в произвольном полиномиальном идеале кольца $R[x_1, \dots, x_k]$ строится стандартный базис специального вида, называемый канонической системой образующих (КСО), и вместо исходной системы предлагается решать систему полиномиальных уравнений, в левой части которой стоит КСО идеала, порожденного исходными многочленами. Для получающихся систем уравнений специального вида предлагается модификация метода покоординатной реализации.

Работа поддержана Российским фондом фундаментальных исследований, гранты 02–01–00218 и 02–01–00687, и грантами НШ-2358.2003.9 и НШ-1910.2003.1 Президента РФ для поддержки ведущих научных школ.

1. Введение

В данной работе продолжают начатые в [15, 16] исследования свойств специальных стандартных базисов: канонических систем образующих (КСО) идеалов кольца $R[x_1, \dots, x_k]$ многочленов над коммутативным артиновым цепным кольцом R , и предлагается метод использования свойств КСО для перечисления решений системы полиномиальных уравнений

$$F_i(x_1, \dots, x_k) = 0, \quad i = 1, \dots, d. \quad (1)$$

над таким кольцом в случае, когда оно конечно, то есть является кольцом Галуа–Эйзенштейна (GE-кольцом). Этот метод представляет собой усовершенствованную версию известного метода покоординатной линеаризации, сводящегося к последовательному перечислению координат p -адического разложения каждого решения.

Работа построена следующим образом. В параграфе 2 описан метод покоординатной линеаризации. Он сводится к решению индуцированной системы полиномиальных

уравнений над полем $\bar{R} = R/\text{rad}(R)$ для вычисления нулевых координат решений исходной системы в p -адическом разложении и последовательному решению серии систем линейных уравнений над тем же полем с целью вычисления координат решений с более старшими номерами.

В параграфе 3 излагаются основные известные результаты о строении базисов Гребнера полиномиальных идеалов над полем и их применении для решения систем полиномиальных уравнений.

В параграфе 4 вводится понятие канонической системы образующих (КСО) произвольного полиномиального идеала над коммутативным артиновым цепным кольцом, доказывается существование такой системы и описывается ряд ее свойств. Эти результаты обобщают аналогичные результаты работы [16], в которой были рассмотрены лишь унитарные полиномиальные идеалы.

В параграфе 5 изложена модификация метода покоординатной линеаризации, использующая свойства КСО соответствующего идеала.

2. Метод покоординатной линеаризации

Пусть R — GE-кольцо с единицей e , $\mathfrak{N}$ — его радикал, индекс нильпотентности которого равен $n \in \mathbb{N}$. Тогда (см., например, [14]) решетка идеалов кольца R есть цепь

$$R = \mathfrak{N}^0 \supset \mathfrak{N} \supset \dots \supset \mathfrak{N}^{n-1} \supset \mathfrak{N}^n = 0.$$

Факторкольцо $\bar{R} = R/\mathfrak{N}$ есть поле, называемое полем вычетов кольца R . Если $n = 1$, то $R = \bar{R}$. Далее полагаем $n > 1$.

Зафиксируем $\pi \in \mathfrak{N} \setminus \mathfrak{N}^2$. Тогда для любого $t \in \{0, 1, \dots, n\}$ верно равенство $\mathfrak{N}^t = \pi^t R$. Кольцо R содержит подмножество $\Gamma = \{\alpha \in R : \alpha^q = \alpha\}$ мощности q , называемое π -адическим координатным множеством или координатным множеством Тейхмюллера, и каждый элемент $a \in R$ однозначно представляется в виде

$$a = a^{(0)} + a^{(1)}\pi + \dots + a^{(n-1)}\pi^{n-1},$$

где $a^{(0)}, \dots, a^{(n-1)} \in \Gamma$. Назовем такое представление a его π -адическим разложением, а элемент $a^{(i)} = \gamma_i(a)$, $i \in \{0, 1, \dots, n-1\}$, — i -й координатой элемента a . Для произвольных $j \in \{0, 1, \dots, n-1\}$ и $\mathbf{c} = (c_1, \dots, c_k) \in R^k$ вектор

$$\mathbf{c}^{(j)} = \gamma_j(\mathbf{c}) = (c_1^{(j)}, \dots, c_k^{(j)}) \in \Gamma^k$$

назовем j -м координат-вектором вектора $\mathbf{c}$.

Пусть $\mathcal{R}_k = R[x_1, \dots, x_k]$ — кольцо многочленов от k переменных над кольцом R .

Рассмотрим систему уравнений (1), где $F_1, \dots, F_d \in \mathcal{R}_k$, и укажем алгоритм перечисления всех ее решений $\mathbf{c} = (c_1, \dots, c_k) \in R^k$. Положим $\psi = \{F_1, \dots, F_d\}$ и будем коротко записывать систему (1) в виде

$$\psi(\mathbf{x}) = 0. \quad (2)$$

Для $F_i \in \psi$ и $\mathbf{a} = (a_1, \dots, a_k) \in R^k$, $\mathbf{b} = (b_1, \dots, b_k) \in R^k$ положим

$$F_i(\mathbf{a} + \mathbf{b}\mathbf{x}) = F_i(a_1 + b_1x_1, \dots, a_k + b_kx_k)$$

и будем коротко записывать систему уравнений

$$\begin{aligned} F_1(\mathbf{a} + \mathbf{b}\mathbf{x}) &= 0, \\ &\dots \\ F_d(\mathbf{a} + \mathbf{b}\mathbf{x}) &= 0. \end{aligned}$$

в виде $\psi(\mathbf{a} + \mathbf{b}\mathbf{x}) = 0$.

Суть обсуждаемого метода состоит в том, что множество K решений системы (2) строится путем решения систем сравнений

$$\psi(\mathbf{x}) \equiv 0 \pmod{\pi^j}, \quad (3)$$

последовательно для $j = 1, \dots, n$. Сначала находятся все решения в Γ^k системы сравнений

$$\psi(\mathbf{z}) \equiv 0 \pmod{\pi}. \quad (4)$$

Затем, если уже найдены решения $\mathbf{c}^{[j]} \in \Gamma^k + \pi\Gamma^k + \dots + \pi^{j-1}\Gamma^k$ системы (3), для каждого из них строится множество решений $\mathbf{c}^{[j]} + \pi^j \mathbf{c}^{(j)} \in \Gamma^k + \pi\Gamma^k + \dots + \pi^j\Gamma^k$ системы сравнений

$$\psi(\mathbf{x}) \equiv 0 \pmod{\pi^{j+1}}, \quad (5)$$

при этом, координат-вектор $\mathbf{c}^{(j)} \in \Gamma^k$ находится как решение системы сравнений

$$\psi(\mathbf{c}^{[j]} + \pi^j \mathbf{z}) \equiv 0 \pmod{\pi^{j+1}}. \quad (6)$$

Этот подход реализуется, например, следующим алгоритмом решения системы (2).

Алгоритм 1. Вход: система уравнений (2).

Выход: множество K всех решений в R^k системы (2).

Суть алгоритма состоит в том, что последовательно, по определенным ниже правилам, строятся двумерные массивы (таблицы) $A_0, A_1, \dots, A_{n-1}$, в ячейки которых записываются векторы из Γ^k . Количество столбцов в j -м массиве равно $j + 1$, а количество строк меняется в процессе работы алгоритма. В начальном такте работы все массивы пусты. Алгоритм заканчивает работу, если либо для некоторого $j < n - 1$ массив A_j , после его заполнения, остался пустым (в таком случае система не имеет решений), либо завершено заполнение массива A_{n-1} (в таком случае K есть, по сути, множество строк массива A_{n-1}).

Этап I. Построение решений над полем вычетов. Найдем все решения в Γ^k системы сравнений (4) (о том, как решать эту систему, а также другие системы, встречающиеся далее в алгоритме, мы подробно поговорим позднее). Пусть $C^{(0)} \subset \Gamma^k$ — множество решений системы (4).

Если $C^{(0)} = \emptyset$, то полагаем $K = \emptyset$ и работа алгоритма 1 закончена.

В противном случае, перенумеровав каким-либо образом все получившиеся решения, запишем их в массив (столбец) A_0 . Если $n = 1$, то полагаем $K = C^{(0)}$ и завершаем работу алгоритма. Если $n > 1$, то обозначаем через b_0 число строк в массиве A_0 и переходим к второму этапу.

Этап II. Подъем решений. Этот этап состоит из $n - 1$ шагов. На j -м шаге, $j \in \{1, \dots, n - 1\}$, строится массив A_j . Каждая строка этого массива состоит из $j + 1$ элементов множества Γ^k . Строки массива формируются путем последовательной обработки строк уже построенного массива A_{j-1} . Пусть $b_j(v)$ — число строк массива A_j , полученных после обработки первых v строк массива A_{j-1} , и b_j — общее число строк массива A_j ($b_j = b_j(b_{j-1})$).

Допустим, что для некоторого $v \in \{1, \dots, b_{j-1}\}$ уже обработаны строки массива A_{j-1} с номерами $1, \dots, v - 1$, в результате чего сформировано $b_j(v - 1)$ строк массива A_j . Тогда обработка v -й строки массива A_{j-1} сводится к следующему. Если $A_{j-1}(v, 1) = c^{(0)}$, $A_{j-1}(v, 2) = c^{(1)}, \dots, A_{j-1}(v, j) = c^{(j-1)}$, то решается система сравнений (6). Пусть $C^{(j)}(v) \subset \Gamma^k$ — множество ее решений, и l — его мощность. Полагаем $b_j(v) = b_j(v - 1) + l$, и если $l > 0$, то произвольным образом нумеруем элементы множества $C^{(j)}(v)$:

$$C^{(j)}(v) = \{c_1^{(j)}, \dots, c_l^{(j)}\}.$$

Далее, для каждого $s \in \{1, \dots, l\}$ полагаем

$$A_j(b_j(v - 1) + s, 1) = A_{j-1}(v, 1) = c^{(0)},$$

...

$$A_j(b_j(v - 1) + s, j) = A_{j-1}(v, j) = c^{(j-1)},$$

$$A_j(b_j + s, j + 1) = c_s^{(j)}.$$

Если $v = b_{j-1}$, то процедура формирования массива A_j закончена. В противном случае, мы аналогичным образом обрабатываем $(v + 1)$ -ю строку массива A_{j-1} .

Если $b_j = 0$, то есть массив A_j пуст, то алгоритм завершает работу, в противном случае переходим к построению массива A_{j+1} . Заметим, что массив A_{j-1} в дальнейшем уже не нужен и может быть удален из памяти. Таким образом, в каждый момент работы алгоритма в памяти достаточно хранить лишь все неиспользованные строки последнего построенного массива и все строки очередного строящегося массива.

По завершении формирования массива A_{n-1} положим

$$K = \{A_{n-1}(i, 1) + \pi A_{n-1}(i, 2) + \dots + \pi^{n-1} A_{n-1}(i, n), \quad i = 1, \dots, b_{n-1}\} \subset R^k.$$

Предложение 1. Множество K есть множество всех решений системы (2).

Доказательство. Пусть $c = c^{(0)} + \pi c^{(1)} + \dots + \pi^{n-1} c^{(n-1)} \in K$, то есть $c^{(s)} = A_{n-1}(i, s + 1)$, $s \in \{0, 1, \dots, n - 1\}$, для некоторого $i \in \{1, \dots, b_{n-1}\}$. Тогда c — решение системы (2), поскольку в алгоритме 1 координатный вектор $c^{(n-1)}$ был выбран как решение системы $\psi(c^{(0)} + \dots + \pi^{n-2} c^{(n-2)} + \pi^{n-1} x) = 0$, и значит, $\psi(c) = 0$.

Пусть теперь вектор $c = c^{(0)} + \pi c^{(1)} + \dots + \pi^{n-1} c^{(n-1)} \in R^k$ является решением системы (2). Покажем, что $c \in K$. Заметим, что $\psi(c^{(0)}) \equiv \psi(c) \equiv 0 \pmod{\pi}$. Значит, $c^{(0)} \in C^{(0)}$ и массив A_0 содержит строку $c^{(0)}$. Пусть $j \in \{1, \dots, n - 1\}$ и уже доказано, что массив A_{j-1} содержит строку $(c^{(0)}, c^{(1)}, \dots, c^{(j-1)})$. Покажем, что массив A_j содержит строку $(c^{(0)}, c^{(1)}, \dots, c^{(j)})$. Действительно, так как

$$\psi(c^{(0)} + \pi c^{(1)} + \dots + \pi^{j-1} c^{(j-1)} + \pi^j c^{(j)}) \equiv \psi(c) \equiv 0 \pmod{\pi^{j+1}},$$

вектор $c^{(j)}$ есть решение системы сравнений (6). Значит, строка $(c^{(0)}, c^{(1)}, \dots, c^{(j)})$ включается в массив A_j на некотором этапе его построения. Отсюда индукцией по $j \in \{1, \dots, n - 1\}$ получаем, что строка $(c^{(0)}, c^{(1)}, \dots, c^{(n-1)})$ принадлежит массиву A_{n-1} .

Ясно, что число строк в массиве A_0 удовлетворяет неравенству $|A_0| \leq q^k = |\Gamma^k|$ и для каждого $j \in \{1, \dots, n-1\}$ имеет место неравенство $|A_j| \leq |\Gamma^k| |A_{j-1}|$. Поэтому количество всех строк массивов $A_0, \dots, A_{n-1}$, то есть общее число шагов алгоритма, оценивается сверху величиной

$$q^k + q^{2k} + \dots + q^{(n-1)k} = \frac{q^{nk} - q^k}{q^k - 1}.$$

Таким образом, алгоритм 1 сводит решение системы (1) к решению системы (4) и некоторого количества систем сравнений вида (6), где $\mathbf{z} \in \Gamma^k$, $\psi = \{F_1, \dots, F_d\} \subset \mathcal{R}_k$, $j \in \{1, \dots, n-1\}$ и $\mathbf{c}^{[j]} \in R^k$ — решение системы (3). Остановимся подробнее на решении систем уравнений вида (4) и (6).

Система (4) равносильна системе полиномиальных уравнений

$$\psi^{(0)}(\mathbf{z}) = 0 \quad (7)$$

над полем $(\Gamma, \oplus, \cdot) = GF(q)$ с операцией $\oplus$, определяемой для $a, b \in \Gamma$ равенством

$$a \oplus b = \gamma_0(a + b),$$

где $\psi^{(0)} = \{F_1^{(0)}, \dots, F_d^{(0)}\}$, $F_i^{(0)}(\mathbf{z}) \in \Gamma[\mathbf{z}]$, $F_i^{(0)}(\mathbf{z}) \equiv F_i(\mathbf{z}) \pmod{\pi}$, $i = 1, \dots, d$. Для решения системы (7) можно использовать все известные методы решений систем полиномиальных уравнений над полями Галуа, в том числе и методы, использующие свойства базиса Гребнера.

Решение системы сравнений (6) в Γ^k сводится к решению системы линейных уравнений над полем Γ следующим образом. Пусть $D_i F(\mathbf{x})$ — частная производная многочлена $F(\mathbf{x}) \in \mathcal{R}_k$ по переменной x_i и $\text{grad } F(\mathbf{x}) = (D_1 F(\mathbf{x}), \dots, D_k F(\mathbf{x}))$. Тогда (см., например, [12]) для любых $\mathbf{c} \in R^k$ и $j \in \{1, \dots, n-1\}$ имеет место разложение Тейлора

$$F(\mathbf{c} + \pi^j \mathbf{z}) \equiv F(\mathbf{c}) + \pi^j \text{grad } F(\mathbf{c}) \cdot \mathbf{z}^\downarrow \pmod{\pi^{2j}}, \quad (8)$$

где

$$\text{grad } F(\mathbf{c}) \cdot \mathbf{z}^\downarrow = \sum_{i \in \{1, \dots, k\}} D_i F(\mathbf{c}) z_i.$$

Пользуясь этим разложением, систему сравнений (6) можно записать в виде

$$F_i(\mathbf{c}^{[j]}) + \pi^j \text{grad } F_i(\mathbf{c}^{[j]}) \cdot \mathbf{z}^\downarrow \equiv 0 \pmod{\pi^{j+1}}, \quad i = 1, \dots, d.$$

Так как $\mathbf{c}^{[j]}$ — решение системы сравнений (3), то

$$F_i(\mathbf{c}^{[j]}) \equiv \pi^j \gamma_j(F_i(\mathbf{c}^{[j]})) \pmod{\pi^{j+1}},$$

где $\gamma_j(F_i(\mathbf{c}^{[j]}))$ — j -я координата π -адического разложения элемента $F_i(\mathbf{c}^{[j]})$. Теперь нетрудно увидеть, что система сравнений (6) равносильна системе сравнений

$$\text{grad } F_i(\mathbf{c}^{[j]}) \cdot \mathbf{z}^\downarrow \equiv -\gamma_j(F_i(\mathbf{c}^{[j]})) \pmod{\pi}, \quad i = 1, \dots, d.$$

которая при обозначениях

$$D\psi(\mathbf{x}) = (D_s F_i(\mathbf{x}))_{d \times k}, \quad \psi^\downarrow(\mathbf{x}) = (F_1(\mathbf{x}), \dots, F_d(\mathbf{x}))^T \quad (9)$$

равносильна системе

$$D\psi(\mathbf{c}^{[j]}) \cdot \mathbf{z}^\downarrow \equiv -\gamma_j(\psi^\downarrow(\mathbf{c}^{[j]})) \pmod{\pi}.$$

Наконец, очевидно, что в матрице из левой части последней системы значимыми являются лишь нулевые разряды π -адических разложений ее элементов. Поэтому, вводя дополнительно к (9) обозначения

$$D\psi^{(0)}(\mathbf{z}) = (D_s F_i^{(0)}(\mathbf{z}))_{d \times k}, \quad (10)$$

получаем, что система сравнений (6) над Γ^k равносильна системе линейных уравнений

$$D\psi^{(0)}(\mathbf{c}^{(0)}) \cdot \mathbf{z}^\downarrow = \Gamma - \gamma_j(\psi^\downarrow(\mathbf{c}^{[j]})) \quad (11)$$

над полем Γ . Здесь равенство $=\Gamma$ означает, что все операции в левой и правой его частях выполняются в поле $(\Gamma, \oplus, \cdot)$. Напомним, что матрицу $D\psi(\mathbf{x})$ (матрицу $D\psi^{(0)}(\mathbf{z})$) принято называть якобианом системы функций ψ (системы функций $\psi^{(0)}$).

Суммируя проведенные рассуждения мы получаем следующие результаты.

Теорема 1. Для любого $j \in \{1, \dots, n-1\}$ и любого решения $\mathbf{c}^{[j]} \in \Gamma^k + \pi\Gamma^k + \dots + \pi^{j-1}\Gamma^k$ системы (3) справедливы следующие утверждения.

- (a) Система (6) равносильна системе линейных уравнений (11).
- (b) Если система (6) совместна, она имеет в точности $q^{k-\text{rank}(D\psi^{(0)}(\mathbf{c}^{(0)}))}$ решений.
- (c) Система (1) имеет единственное решение в точности если система полиномиальных уравнений (4) над полем Γ имеет единственное решение $\mathbf{c}^{(0)} \in \Gamma^k$ и якобиан $D\psi^{(0)}(\mathbf{c}^{(0)})_{d \times k}$ имеет ранг k .

Полученные результаты позволяют оценить количество систем линейных уравнений вида (11), которое потребуется решить в процессе выполнения алгоритма 1. Пусть $C^{(0)} = \{\mathbf{c}_1^{(0)}, \dots, \mathbf{c}_N^{(0)}\}$ — множество всех решений в Γ^k системы (4). Положим $r_i = \text{rank}(D\psi^{(0)}(\mathbf{c}_i^{(0)}))$, $k_i = k - r_i$ для $i \in \{1, \dots, N\}$. Тогда из теоремы 1 следует, что для каждого фиксированного вектора $\mathbf{c}_i^{(0)} \in C^{(0)}$, если a_{ij} — число строк массива A_j , начинающихся с $\mathbf{c}_i^{(0)}$, то для каждого $j \in \{1, \dots, n-1\}$ имеет место неравенство $a_{ij} \leq a_{i,j-1}q^{k_i}$. Отсюда получаем следующее утверждение.

Предложение 2. Количество систем линейных уравнений вида (11), которое потребуется решить в процессе выполнения алгоритма 1, оценивается сверху величиной

$$\sum_{i \in \{1, \dots, N\}} \frac{q^{nk_i} - 1}{q^{k_i} - 1}.$$

Пример 1. Решим над $R = \mathbf{Z}_4$ систему уравнений

$$\begin{aligned} F_1(x_1, x_2) &= 2x_1x_2 + 2x_2 + x_1^3 + x_1^2 = 0, \\ F_2(x_1, x_2) &= x_2^2 + x_1^2x_2 + x_1^2 = 0, \\ F_3(x_1, x_2) &= x_2^2 + x_1x_2 + x_1^2 = 0, \\ F_4(x_1, x_2) &= x_1x_2^2 + x_2^2 = 0, \\ F_5(x_1, x_2) &= x_2^3 + x_1^2 = 0, \\ F_6(x_1, x_2) &= 2x_2 + 2x_1 = 0. \end{aligned} \quad (12)$$

Положим $\psi = \{F_1, \dots, F_6\}$. Тогда система (12) может быть записана в виде $\psi(x) \equiv 0 \pmod{4}$. Следуя алгоритму 1, для описания всех ее решений сначала строим множество C_0 всех возможных решений над $\Gamma = \mathbf{Z}_2$ системы уравнений $\psi^{(0)}(x) \equiv 0 \pmod{2}$, то есть системы

$$\begin{aligned} x_1^3 + x_1^2 &\equiv 0 \pmod{2}, \\ x_2^2 + x_1^2 x_2 + x_1^2 &\equiv 0 \pmod{2}, \\ x_2^2 + x_1 x_2 + x_1^2 &\equiv 0 \pmod{2}, \\ x_1 x_2^2 + x_2^2 &\equiv 0 \pmod{2}, \\ x_2^3 + x_1^2 &\equiv 0 \pmod{2}. \end{aligned} \quad (13)$$

Очевидно, последняя система равносильна системе

$$\begin{aligned} x_2 \oplus x_1 x_2 \oplus x_1 &= 0, \\ x_1 x_2 \oplus x_2 &= 0, \\ x_2 \oplus x_1 &= 0, \end{aligned} \quad (14)$$

которая имеет единственное решение $\mathbf{c}^{(0)} = (0, 0)$. Таким образом $C_0 = \{\mathbf{c}^{(0)}\}$. Для подъема этого решения до решений исходной системы над $\mathbf{Z}_4$ составляется система линейных уравнений (11), которая в нашем случае имеет вид

$$D\psi^{(0)}((0, 0))\mathbf{x}^\downarrow =_\Gamma -\psi^\downarrow((0, 0))^{(1)},$$

где $D\psi^{(0)}((0, 0)) = 0_{3 \times 2}$, $-\psi^\downarrow((0, 0))^{(1)} = 0^\downarrow$. Очевидно, что решением данной системы является любой вектор $\mathbf{c}^{(1)} = (c_1^{(1)}, c_2^{(1)}) \in \mathbf{Z}_2^2$. Таким образом, исходная система имеет 4 решения $(0, 0)$, $(0, 2)$, $(2, 0)$, $(2, 2)$.

3. Базис Гребнера полиномиального идеала над полем

Коротко стандартный базис идеала I в кольце многочленов $\mathcal{R}_k = R[x_1, \dots, x_k]$ над кольцом R можно охарактеризовать как систему его образующих χ и некоторый алгоритм редуцирования (обобщенного деления с остатком) произвольного многочлена $H(\mathbf{x}) \in \mathcal{R}_k$ по модулю множества χ , который позволяет за конечное число шагов проверять включение $H \in I$. История изучения стандартных базисов полиномиальных идеалов начинается с известной теоремы Гильберта о базисе [48]. Однако доказательство Гильберта не давало алгоритма нахождения базиса идеала. Видимо, первый конструктивный результат, построение базиса полиномиального идеала в кольце $\mathbf{Z}[x]$, принадлежит Л. Кронекеру [55].

Современный этап истории изучения стандартных базисов начинается с работ А. И. Ширшова [20] (1962), Х. Хиронаки [49] (1964) и Б. Бухбергера [32] (1965), в которых опубликованы приблизительно, одни и те же идеи, результаты и алгоритмы, соответственно для левых алгебр, формальных степенных рядов и коммутативных многочленов. Построенный в последней работе базис полиномиального идеала был назван базисом Гребнера, а алгоритм его построения по произвольной конечной системе образующих идеала стали называть алгоритмом Бухбергера. В настоящее время имеет место тенденция называть базисом Гребнера любой стандартный базис идеала (не обязательно даже полиномиального [27, 58]), то есть, фактически, отождествлять понятия стандартный базис и базис Гребнера. Мы будем называть базисом Гребнера лишь стандартный

базис кольца многочленов над полем, используя в остальных случаях более нейтральный термин стандартный базис.

Изложим кратко некоторые основные результаты о базисах Гребнера, необходимые в дальнейшем.

Пусть $\preccurlyeq$ — произвольное мономиальное (допустимое) упорядочение на множестве N_0^k , то есть линейное упорядочение такое, что $0 \preccurlyeq i$ для каждого $i \in N_0^k$ и для любых $u, s, t \in N_0^k$ условие $s \preccurlyeq t$ влечет $s + u \preccurlyeq t + u$. Важными примерами мономиальных упорядочений на N_0^k являются лексикографическое упорядочение и градуированное лексикографическое упорядочение, которые задаются следующим образом: для произвольных $i = (i_1, \dots, i_k), j = (j_1, \dots, j_k) \in N_0^k$ 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;
- 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.

Заметим, что для любого мономиального упорядочения верна импликация

$$\forall i, j \in N_0^k \quad (i \leq j \text{ (покоординатно)}) \implies (i \preccurlyeq j). \quad (15)$$

Отношение линейного порядка $\preccurlyeq$, заданное на N_0^k , распространим естественным образом на мономы из кольца $\mathcal{R}_k = R[x]$, полагая $ax^i \preccurlyeq bx^j$, если $a = 0$ или $b \neq 0$ и $i \preccurlyeq j$.

Для $A \in \mathcal{R}_k$ и $i = (i_1, \dots, i_k) \in N_0^k$ через $\text{Cf}(A, x^i)$ обозначим коэффициент многочлена $A(x)$ при терме (произведении степеней независимых переменных) $x^i = x_1^{i_1} \dots x_k^{i_k}$. Конечное множество

$$\mathfrak{S}(A) = \text{supp}(A) = \{i \in N_0^k : \text{Cf}(A, x^i) \neq 0\}$$

назовем носителем многочлена A . Относительно выбранного упорядочения $\preccurlyeq$ множество $\mathfrak{S}(A)$ имеет максимальный элемент, который называется мультистепенью многочлена A и обозначается $\text{mdg}(A)$. Определим старший моном $\text{Hm}(A)$, старший коэффициент $\text{Hc}(A)$ и старший член (терм) $\text{Ht}(A)$ многочлена A соответственно равенствами

$$\text{Ht}(A) = x^{\text{mdg}(A)}, \quad \text{Hc}(A) = \text{Cf}(A, \text{Ht}(A)), \quad \text{Hm}(A) = \text{Hc}(A) \text{Ht}(A).$$

Многочлен $A \in \mathcal{R}_k$, удовлетворяющий условию $\text{Hc}(A) = e$, назовем унитарным.

Пусть теперь $R = P$ — поле и $\mathcal{P}_k = P[x_1, \dots, x_k]$ — кольцо многочленов над P . Напомним в этой ситуации основные определения, связанные с понятием полиномиальной редукции (обобщенного деления с остатком). Будем говорить, что многочлен $A \in \mathcal{P}_k$ редуцируется к многочлену $H \in \mathcal{P}_k$ с помощью многочлена $G \in \mathcal{P}_k$, элемента $b \in P$ и вектора $i \in N_0^k$ и писать

$$A \rightarrow_{(G, b, i)} H,$$

если $\text{Cf}(A, x^i \text{Ht}(G)) = b \text{Hc}(G) \neq 0$ и $H = A - bx^i G$.

Пусть $\chi = \{G_1(x), \dots, G_l(x)\}$ — некоторое непустое подмножество $\mathcal{P}_k$. Будем говорить, что многочлен $A \in \mathcal{P}_k$ редуцируется к многочлену $H \in \mathcal{P}_k$ по модулю множества

χ и писать $A \rightarrow_\chi H$, если для некоторого $d \in \mathbb{N}$ существуют индексы $s_j \in \{1, \dots, l\}$, $H_j \in \mathcal{P}_k$, элементы $b_j \in P$ и векторы $i_j \in \mathbb{N}_0^k$, $j \in \{1, \dots, d\}$, такие, что

$$A \rightarrow_{(G_{s_1}, b_1, i_1)} H_1 \rightarrow_{(G_{s_2}, b_2, i_2)} H_2 \rightarrow_{(G_{s_3}, b_3, i_3)} \dots \rightarrow_{(G_{s_d}, b_d, i_d)} H_d = H.$$

Назовем многочлен A нормальным по модулю множества χ , если не существует такого многочлена H , что $A \rightarrow_\chi H$. Через $N(\chi)$ обозначим множество всех нормальных многочленов по модулю χ . Заметим, что $0 \in N(\chi)$ для любого множества χ . Многочлен H называется нормальной формой многочлена A по модулю χ , если $H \in N(\chi)$ и либо $A = H$, либо A редуцируется к H по модулю множества χ . Пусть $NF(A, \chi)$ — множество всех нормальных форм многочлена A по модулю χ . Отметим, что для любого $A \in \chi$ множество $NF(A, \chi)$ содержит 0.

Для любого многочлена $A \in \mathcal{P}_k$ множество $NF(A, \chi)$ не пусто. Более того, при фиксированном упорядочении $\preccurlyeq$ и фиксированной нумерации элементов множества χ существует конечный алгоритм $\rightarrow_\chi$ редуцирования любого многочлена $A \in (\mathcal{P}_k \setminus N(\chi))$ по модулю множества χ , при котором $A \rightarrow_\chi H$, где $H \in N(\chi)$. Отсюда, в частности, следует, что с помощью алгоритма редуцирования любой многочлен $A \in \mathcal{P}_k$ может быть представлен в виде

$$A(\mathbf{x}) = Q_1(\mathbf{x})G_1(\mathbf{x}) + \dots + Q_l(\mathbf{x})G_l(\mathbf{x}) + H(\mathbf{x}), \quad (16)$$

где $H \in NF(A, \chi)$.

Конечное множество $\chi \subset \mathcal{P}_k$ унитарных многочленов назовем редуцированной системой Гребнера (относительно мономиального упорядочения $\preccurlyeq$), если каждый многочлен $G \in \chi$ является нормальным по модулю множества $\chi \setminus \{G\}$ и идеал $I = \mathcal{P}_k \chi$ удовлетворяет условию

$$\forall A \in I \quad NF(A, \chi) = \{0\}. \quad (17)$$

Такая система многочленов называется также редуцированным базисом Гребнера идеала I . Отметим, что условие (17) эквивалентно условию

$$\forall A \in \mathcal{P}_k \quad |NF(A, \chi)| = 1. \quad (18)$$

Любой ненулевой идеал $I \triangleleft \mathcal{P}_k$ содержит единственный (при заданном упорядочении $\preccurlyeq$) редуцированный базис Гребнера (см., например, [2, 10, 33]).

В дополнение к приведенному общему комбинаторно-алгебраическому описанию свойств базиса Гребнера нам понадобится также его линейно-алгебраическая характеристика, связанная с диаграммами Ферре.

Напомним, что диаграммой Ферре называется конечное множество $\mathcal{F} \subset \mathbb{N}_0^k$ такое, что

$$\forall i \in \mathcal{F}, j \in \mathbb{N}_0^k \quad (j \leq i) \implies (j \in \mathcal{F}) \quad (19)$$

(см., например, [19]). Мы будем называть такое множество конечной диаграммой Ферре, а произвольное (не обязательно конечное) множество $\mathcal{F} \subset \mathbb{N}_0^k$, удовлетворяющее условию (19), — (обобщенной) диаграммой Ферре.

Обозначим s -ю строку единичной $k \times k$ матрицы над $\mathbb{Z}$ через 1_s . Пусть $\bar{\mathcal{F}} = \mathbb{N}_0^k \setminus \mathcal{F}$. Назовем множество

$$\mathcal{H}\mathcal{F} = \{i \in \bar{\mathcal{F}} : \forall s \in \{1, \dots, k\} \quad (i_s > 0) \implies (i - 1_s \in \mathcal{F})\} \quad (20)$$

Рис. 1. Примеры конечных диаграмм Ферре в случае $k = 2$

множеством (внешних) углов диаграммы Ферре $\mathcal{F}$. Нетрудно увидеть, что $\mathcal{KF}$ можно охарактеризовать также как множество минимальных элементов частично упорядоченного множества $(\mathcal{F}, \leq)$. Любая диаграмма Ферре $\mathcal{F}$ однозначно определяется своим множеством углов $\mathcal{KF}$

$$\mathcal{F} = \mathbf{N}_0^k \setminus \bigcup_{\mathbf{i} \in \mathcal{KF}} (\mathbf{i} + \mathbf{N}_0^k). \quad (21)$$

Для любого $\mathbf{i} \in \mathcal{KF}$ любой многочлен $G_{\mathbf{i}}(\mathbf{x})$ вида

$$G_{\mathbf{i}} = \mathbf{x}^{\mathbf{i}} - \sum_{\mathbf{j} \in \mathcal{F}} g_{\mathbf{i}, \mathbf{j}} \mathbf{x}^{\mathbf{j}}$$

назовем $\mathcal{F}$ -унитарным многочленом. Произвольное множество χ $\mathcal{F}$ -унитарных многочленов вида $\chi = \{G_{\mathbf{i}} : \mathbf{i} \in \mathcal{KF}\}$ назовем характеристическим множеством $\mathcal{F}$ -унитарных многочленов.

Важный крайний случай диаграммы Ферре: $\mathcal{F} = \emptyset$ — пустое множество. Для него $\mathcal{KF} = \{(0, 0)\}$ и единственное характеристическое множество $\mathcal{F}$ -унитарных многочленов $\chi = \{e\}$.

Напомним, что для произвольного кольца R идеал $I \triangleleft \mathcal{P}_k$ называется унитарным, если он содержит некоторую систему унитарных многочленов $F_1(x_1), \dots, F_k(x_k)$ с коэффициентами из R (систему элементарных унитарных многочленов). Если R — коммутативное артиново кольцо с единицей, то это условие эквивалентно тому, что R -модуль $\mathcal{P}_k/I$ конечно порожден [57].

Произвольному собственному идеалу $I \triangleleft \mathcal{P}_k$ соответствует факторкольцо $S = \mathcal{P}_k/I$ — кольцо операторов идеала I , которое можно представить в виде $S = P[\omega_1, \dots, \omega_k]$, где $\omega_s = x_s + I$, $s = 1, \dots, k$. Кольцо S есть P -алгебра, базис которой можно выбрать из элементов $\omega^{\mathbf{i}} = \omega_1^{i_1} \dots \omega_k^{i_k}$, $\mathbf{i} \in \mathbf{N}_0^k$, причем, если I — унитарный идеал, то этот базис конечен. Доказательства следующих двух результатов почти не отличаются от доказательств теоремы 2.2 и предложения 2.4 из [13].

Теорема 2. Пусть $I \triangleleft \mathcal{P}_k$, $\preccurlyeq$ — мономиальное отношение на $\mathbf{N}_0^k$. Тогда I имеет единственный редуцированный базис Гребнера χ относительно $\preccurlyeq$. Множество

$$\mathcal{K} = \{\text{mdg}(G) : G \in \chi\}$$

является множеством углов $\mathcal{K} = \mathcal{KF}$ диаграммы Ферре

$$\mathcal{F} = \mathcal{F}_{\chi} = \mathbf{N}_0^k \setminus \bigcup_{\mathbf{i} \in \mathcal{K}} (\mathbf{i} + \mathbf{N}_0^k).$$

В случае, когда I — собственный унитарный идеал, кольцо $S = \mathbb{P}_k/I$ операторов идеала I есть P -алгебра размерности $|\mathcal{F}_\chi|$ с базисом $\mathcal{B} = \{\omega^i: i \in \mathcal{F}\}$.

В обозначениях теоремы 2 назовем диаграмму Ферре $\mathcal{F}_\chi = \mathcal{F}(I, \preceq)$ опорной диаграммой Ферре базиса χ и идеала I . Заметим, что χ есть характеристическое множество $\mathcal{F}_\chi$ -унитарных многочленов и произвольный многочлен $H \in \mathbb{P}_k$ является нормальным по модулю множества χ , в точности если $\mathcal{S}(H) \subseteq \mathcal{F}_\chi$.

Предложение 3. Если I, J — идеалы кольца $\mathbb{P}_k$ и $I \subseteq J$, то при фиксированном мономиальном упорядочении $\preceq$ справедливо включение $\mathcal{F}(J, \preceq) \subseteq \mathcal{F}(I, \preceq)$ и равенство $I = J$ эквивалентно равенству $\mathcal{F}(J, \preceq) = \mathcal{F}(I, \preceq)$.

В настоящее время имеется большое количество алгебраических методов решения систем полиномиальных уравнений вида (1) над полем (см., например, [3, 4, 6, 10, 54, 60, 5]), к которым следует добавить методы, основанные на вычислении базисов Гребнера [10, 31, 34, 39, 45, 50, 60, 61, 70], сводящие исходную систему к равносильной и более просто разрешимой системе уравнений с редуцированным базисом Гребнера в левой части. Эти методы основаны на следующем результате.

Лемма 1. Пусть R — коммутативное кольцо, $\chi = \{G_1, \dots, G_l\} \subset \mathbb{R}_k$ — некоторая система образующих идеала $I = \mathbb{R}_k(F_1, \dots, F_d)$. Тогда система (1) равносильна системе

$$G_i(x_1, \dots, x_k) = 0, \quad i = 1, \dots, l. \quad (22)$$

Доказательство. Если строка $(a_1, \dots, a_k) \in R^k$ есть решение системы (1), то она — решение системы (22). Действительно, произвольный многочлен $G \in \chi$ представляется в виде

$$G = \sum_{i=1}^d H_i F_i, \quad H_i \in \mathbb{R}_k, \quad i = 1, \dots, d,$$

поэтому

$$G(a_1, \dots, a_k) = \sum_{i=1}^d H_i(a_1, \dots, a_k) F_i(a_1, \dots, a_k) = 0.$$

Пример 2. Рассмотрим систему уравнений

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 - 1 &= 0, \\ x_1^2 + x_3^2 - x_2 &= 0, \\ x_3 - x_1 &= 0 \end{aligned} \quad (23)$$

над полем $\mathbb{C}$. Пусть $I \triangleleft \mathbb{C}[x_1, x_2, x_3]$ — идеал, порожденный многочленами из левой части системы (23), и $\preceq$ — лексикографическое упорядочение на $\mathbb{N}_0^3$, при котором $x_3 < x_2 < x_1$. Редуцированный базис Гребнера χ идеала I по отношению к этому упорядочению есть

$$\chi = \{G_1 = x_1 - x_3, G_2 = -x_2 + 2x_3^2, G_3 = x_3^4 + (1/2)x_3^2 - (1/4)\}.$$

Согласно лемме 1 система уравнений (23) равносильна системе

$$\begin{aligned} x_1 - x_3 &= 0, \\ -x_2 + 2x_3^2 &= 0, \\ x_3^4 + (1/2)x_3^2 - (1/4) &= 0. \end{aligned} \quad (24)$$

Эта система легко решается методом последовательного исключения переменных. Последнее уравнение ($G_3 = 0$) зависит только от x_3 , и его 4 решения легко вычисляются как решения биквадратного уравнения:

$$x_3 = \pm \frac{1}{2} \sqrt{\pm \sqrt{5} - 1}.$$

Подставляя каждое из этих значений в систему уравнений $G_2 = 0$, $G_1 = 0$, мы однозначно определяем x_2 и x_1 . Таким образом вычисляются все 4 решения системы (23).

Пример 2 иллюстрирует свойство системы Гребнера последовательно исключать переменные при решении систем уравнений, суть которого проясняет следующая теорема.

Теорема 3 ([10]). Пусть $\preccurlyeq$ — лексикографическое упорядочение на $\mathbb{N}_0^k$, при котором $x_k < x_{k-1} < \dots < x_1$, и ψ — соответствующий $\preccurlyeq$ базис Гребнера идеала $I \triangleleft \mathbb{P}_k$. Тогда для каждого $r \in \{1, \dots, k\}$ множество $\psi \cap P[x_r, \dots, x_k]$ есть базис Гребнера идеала $I \cap P[x_r, \dots, x_k]$.

Этот результат лежит в основе теории исключения, показывающей, в частности, что редуцированный базис Гребнера в случае указанного лексикографического упорядочения позволяет последовательно определять (исключать) переменные $x_k, \dots, x_1$. Более того, использование базиса Гребнера — наилучший (а не какой-то случайный) способ произвести указанную цепочку исключений. Подробнее об этом, а также об использовании других допустимых упорядочений см. [10] и цитируемую там литературу.

Оценка трудоемкости алгоритмов построения базиса Гребнера в общем случае — открытый вопрос. Нет удовлетворительных оценок даже для количества и степеней многочленов, входящих в редуцированный базис Гребнера идеала, заданного некоторой своей системой образующих. С некоторыми результатами по данной тематике можно ознакомиться в [2, 10, 38, 61, 63, 71]. Отметим последние результаты [40, 41, 42], где задача построения базиса Гребнера полиномиального идеала над полем сведена к трансформированию некоторых разреженных матриц. Это позволило программно реализовать алгоритмы построения базисов Гребнера, которые работают, по меньшей мере, в 100 раз быстрее любых известных реализованных версий алгоритма Бухбергера. Этот подход позволяет также надеяться на получение теоретических оценок трудоемкости построения базисов Гребнера, более точных, чем имеющиеся оценки трудоемкости алгоритма Бухбергера.

4. Каноническая система образующих идеала из $\mathcal{R}_k$

Алгоритм Бухбергера построения базисов Гребнера обобщался в двух направлениях: на многочлены с коэффициентами из коммутативного кольца, отличного от поля, и на некоммутативные и неассоциативные полиномиальные кольца.

Результаты последнего направления слабо связаны с данной работой и в связи с ними мы ограничимся лишь перечислением основных первоисточников [20, 64, 1, 7, 8, 17, 68, 24, 11, 9, 18, 62, 47, 43, 21].

Базисы Гребнера в коммутативных кольцах многочленов над кольцами, отличными от полей, изучались в [70, 72, 35, 51, 66, 26, 13, 15, 36, 65]. В [70, 72, 35] алгоритм Бухбергера обобщался на $\mathbb{Z}[x_1, \dots, x_k]$. В [51] полиномы рассматривались над евклидовыми кольцами, в [66] — над областями главных идеалов (ОГИ). Более точно, алгоритм, предложенный в [66], строит слабый базис Гребнера. Это базис идеала I , относительно которого каждый многочлен идеала I (и только такой многочлен) может быть редуцирован к 0.

Пусть далее R — коммутативное артиново цепное кольцо. В [15] для произвольного идеала кольца $R[x]$ был построен стандартный базис специального вида, названный канонической системой образующих (КСО). В [65] приведен алгоритм построения стандартного базиса (базиса Гребнера) произвольного идеала I в кольце многочленов $\mathcal{R}_k = R[x_1, \dots, x_k]$. Этот базис, названный минимальным сильным базисом Гребнера, несократим с точки зрения предложенного алгоритма проверки включения $H \in I$. В общем случае для такого базиса получены лишь некоторые характеристики. Наиболее полный вид и свойства минимального сильного базиса Гребнера описаны только при $k = 1$. В связи с этим необходимо отметить, что для $k = 1$ данный базис совпадает с КСО из [15] (см. также [57]). К сожалению, работа [65] не содержит ссылок на эти результаты. В [36] для случая, когда R — кольцо Галуа, также построен стандартный базис (базис Гребнера) полиномиального идеала из $\mathcal{R}_k$.

Результаты [15] обобщены в [13] на случай унитарного идеала кольца многочленов $R[x_1, \dots, x_k]$, то есть идеала, содержащего некоторую систему из k унитарных многочленов $F_1(x_1), \dots, F_k(x_k)$. В параграфе 3 данной работы результаты [15, 13] обобщены на случай произвольного идеала кольца многочленов $R[x_1, \dots, x_k]$.

При $k \geq 1$ КСО из [13] обладают рядом преимуществ по сравнению с базисами Гребнера из [36, 65]. В [57, 15, 13] показано, что КСО унитарного идеала из $\mathcal{R}_k$ позволяет не только проверять включение $H \in I$ для многочлена $H(x) \in \mathcal{R}_k$, но также вычислять мощность факторкольца $\mathcal{R}_k/I$, строить систему образующих семейства линейных рекуррент с характеристическим идеалом I , вычислять период идеала I и т. д. Некоторыми такими хорошими свойствами обладает и классический базис Гребнера полиномиального идеала над полем [2, 10, 30, 33, 34, 53]. Отметим, что предложенный в [65] минимальный сильный базис Гребнера в случае $k > 1$ описан недостаточно глубоко для того, чтобы с его помощью можно было решать аналогичные задачи без применения алгоритмов перебора.

В этом параграфе результаты работ [15] (для произвольных идеалов из $R[x]$) и [13] (для унитарных идеалов из $\mathcal{R}_k$) обобщаются на произвольные идеалы из $\mathcal{R}_k$, $k \geq 1$. Для таких идеалов доказывается существование стандартного базиса, который совпадает с КСО в указанных выше частных случаях и также называется канонической системой образующих.

Мы сохраняем обозначения параграфа 2, отказываясь лишь от условия конечности кольца R : e — единица кольца R ; $\mathfrak{N}$ — его единственный максимальный идеал (радикал), индекс нильпотентности которого равен $n \in \mathbb{N}$; $\bar{R} = R/\mathfrak{N}$ — поле вычетов. Если $n = 1$, то $R = \bar{R}$. Если $n > 1$, то решетка идеалов кольца R есть цепь

$$R = \mathfrak{N}^0 \supset \mathfrak{N}^1 \supset \dots \supset \mathfrak{N}^{n-1} \supset \mathfrak{N}^n = 0,$$

Зафиксируем $\pi \in \mathfrak{N} \setminus \mathfrak{N}^2$. Тогда для любого $t \in \{0, 1, \dots, n\}$ верно равенство $\mathfrak{N}^t = \pi^t R$.

Для элемента $\alpha \in R$, многочлена $F(x) \in \mathcal{R}_k$ и множества $S \subseteq {}^s\mathcal{R}_k$ обозначим через $\bar{\alpha}$, $\bar{F}$, $\bar{S}$ их образы при соответствующих естественных эпиморфизмах $R \rightarrow \bar{R}$ и $\mathcal{R}_k \rightarrow \bar{\mathcal{R}}[x]$ и определим норму соответственно равенствами [15]

$$\begin{aligned} \|\alpha\| &= \max\{t \in \{0, 1, \dots, n\} : \alpha \in \mathfrak{N}^t\}, \\ \|F\| &= \max\{t \in \{0, 1, \dots, n\} : F \in \pi^t \mathcal{R}_k\}, \\ \|S\| &= \max\{t \in \{0, 1, \dots, n\} : S \subseteq \pi^t \mathcal{R}_k\}. \end{aligned}$$

Результаты [15] о построении КСО для идеала из $R[x]$ основаны на хорошо известной теореме Крулля [56]: для любого многочлена $F(x) \in R[x]$ такого, что $\bar{F} \neq 0$, существуют унитарный многочлен $G(x) \in R[x]$ и обратимый многочлен $U(x) \in R[x]$ такие,

что $G = UF$. Эту теорему можно сформулировать также и в следующем виде: для любого идеала $I \triangleleft R[x]$ такого, что $\bar{I} \neq \bar{0}$, существует унитарный многочлен $G(x) \in I$ такой, что $\bar{I} = \bar{R}[x]\bar{G}$. Ниже приводится обобщение этого результата для кольца многочленов от $k > 1$ переменных. Далее предполагается, что на N_0^k зафиксировано мономиальное упорядочение $\preccurlyeq$ и все редукции и базисы Гребнера строятся относительно $\preccurlyeq$. Мы будем использовать для обозначения идеала, порожденного данным подмножеством $\chi = \{G_1, \dots, G_l\} \subset \mathcal{R}_k$, выражение $\mathcal{R}_k \chi = \mathcal{R}_k \{G_1, \dots, G_l\}$.

Теорема 4. Пусть $I \triangleleft \mathcal{R}_k$, $\bar{I} \neq \bar{0}$ и $\Psi \subset I$ — система многочленов такая, что $|\Psi| = |\bar{\Psi}|$ и $\bar{\Psi}$ — редуцированный базис Гребнера идеала $\bar{I} \triangleleft \bar{\mathcal{R}}_k$ с опорной диаграммой Ферре $\mathcal{F}_{\bar{\Psi}} = \mathcal{F}$. Тогда идеал I содержит характеристическое множество $\chi \subset I$ $\mathcal{F}$ -унитарных многочленов такое, что

$$\bar{\chi} = \bar{\Psi}. \quad (25)$$

Доказательство этой теоремы дословно повторяет доказательство теоремы 3.1 из [13], сформулированной для случая, когда I — унитарный идеал.

Пусть $\mathcal{F} \subset N_0^k$ — диаграмма Ферре. Будем говорить, что (при заданном мономиальном упорядочении) множество $\chi \subset \mathcal{R}_k$ $\mathcal{F}$ -унитарных многочленов есть система Крулля (круллева система) с опорной диаграммой Ферре $\mathcal{F}$, если множество $\bar{\chi}$ является редуцированной системой Гребнера с опорной диаграммой Ферре $\mathcal{F}_{\bar{\chi}} = \mathcal{F}$. Используя данное понятие, теорему 4 можно сформулировать следующим образом: при заданном мономиальном упорядочении для любого идеала $I \triangleleft \mathcal{R}_k$ нормы 0 существуют диаграмма Ферре $\mathcal{F} \subset N_0^k$ и круллева система многочленов $\chi \subset I$ с опорной диаграммой $\mathcal{F}$ такие, что $\bar{I} = \bar{\mathcal{R}}_k \bar{\chi}$. Назовем эту систему главной частью канонической системы образующих (КСО) идеала I (относительно упорядочения $\preccurlyeq$). Заметим, что такая система определяется идеалом I , вообще говоря, неоднозначно. Отметим также, что если R — не поле, то есть $n > 1$, то круллева система многочленов χ , в отличие от редуцированной системы Гребнера $\bar{\chi}$, не обязательно состоит из унитарных многочленов.

Пример 3. Пусть $R = \mathbb{Z}_4$ и $\preccurlyeq$ — градуированное лексикографическое упорядочение на $\mathcal{R}_2$ такое, что

$$e < x_2 < x_1 < x_2^2 < x_1 x_2 < x_1^2 < \dots$$

Тогда система χ , состоящая из многочленов

$$G_1(\mathbf{x}) = x_1^3, \quad G_2(\mathbf{x}) = x_1 x_2 + 2, \quad G_3(\mathbf{x}) = x_2^2 + 2x_1^2,$$

есть круллева система с опорной диаграммой $\mathcal{F} = \{(0, 0), (0, 1), (0, 2), (1, 0)\}$, соответствующая редуцированной системе Гребнера $\bar{\chi} = \{x_1^3, x_1 x_2, x_2^2\} \subset \bar{\mathcal{R}}_2$. Последняя состоит из унитарных многочленов, однако, $G_3(\mathbf{x})$ — не унитарный многочлен.

Для построения канонической системы образующих мы определим редукцию (обобщенное полиномиальное деление) в $\mathcal{R}_k$ нестандартным способом. Для этого, наряду с понятиями старшей степени, старшего монома и старшего члена многочлена, введем ряд дополнительных понятий. Для произвольного многочлена $A \in \mathcal{R}_k$ назовем ведущей (мульти)степенью и обозначим через $\text{ldg}(A)$ максимальный относительно $\preccurlyeq$ элемент $\mathbf{i} \in \mathbb{S}(A)$, удовлетворяющий условию $\|\text{Cf}(A, \mathbf{x}^{\mathbf{i}})\| = \|A\|$. Если R — поле, то параметры $\text{ldg}(A)$ и $\text{mdg}(A)$ совпадают. В общем же случае они связаны следующим образом. Ненулевой многочлен A можно представить в виде $A = \pi^{\|A\|} A_1$, где $A_1 \in \mathcal{R}_k$, $A_1 \neq \bar{0}$. Тогда $\text{ldg}(A) = \text{mdg}(A_1) \preccurlyeq \text{mdg}(A)$. Из описания круллевой системы многочленов вытекает следующее утверждение.

Предложение 4. Пусть $\mathcal{F} \subset \mathbb{N}_0^k$ — диаграмма Ферре, χ — круллева система $\mathcal{F}$ -унитарных многочленов. Тогда справедливо равенство $\{\text{ldg}(G) : G \in \chi\} = \mathcal{KF}$.

Определим ведущий терм, ведущий коэффициент и ведущий моном многочлена $A \in \mathcal{R}_k$ соответственно равенствами

$$\text{Lt}(A) = \mathbf{x}^{\text{ldg}(A)}, \quad \text{Lc}(A) = \text{Cf}(A, \mathbf{x}^{\text{ldg}(A)}), \quad \text{Lm}(A) = \text{Lc}(A) \text{Lt}(A).$$

По определению считаем $\text{Lt}(0) = 0$, $\text{Lc}(0) = 0$. Отметим, что многочлен A является унитарным, если $\text{ldg}(A) = \text{mdg}(A)$ и $\text{Lc}(A) = e$.

Заметим, что в случае, когда $R = P$ — поле, введенные здесь функции от A совпадают с теми, которые были введены выше в параграфе 3:

$$\text{Lt}(A) = \text{Ht}(A), \quad \text{Lc}(A) = \text{Hc}(A), \quad \text{Lm}(A) = \text{Hm}(A).$$

Определение 1. Будем говорить, что многочлен A редуцируется к многочлену $H \in \mathcal{R}_k$ с помощью многочлена $G \in \mathcal{R}_k$, элемента $b \in R$ и вектора $\mathbf{i} \in \mathbb{N}_0^k$ и писать $A \rightarrow_{(G, b, \mathbf{i})} H$, если $\text{Cf}(A, \mathbf{x}^{\mathbf{i}} \text{Lt}(G)) = b \text{Lc}(G) \neq 0$ и $H = A - b \mathbf{x}^{\mathbf{i}} G$. Если при этом $\mathbf{x}^{\mathbf{i}} \text{Lt}(G) = \mathbf{x}^{\mathbf{j}}$, то будем говорить также, что $a_j \mathbf{x}^{\mathbf{j}}$ многочлена A редуцируется ведущим мономом $\text{Lm}(G)$ многочлена G .

Несложно доказать следующее утверждение.

Предложение 5. Если $A \rightarrow_{(G, b, \mathbf{i})} H$, то $\|H\| \geq \|A\|$.

Определение 2. Пусть χ — некоторое непустое подмножество $\mathcal{R}_k$. Будем говорить, что многочлен $A \in \mathcal{R}_k$ редуцируется к многочлену $H \in \mathcal{R}_k$ по модулю множества χ и писать $A \rightarrow_\chi H$, если для некоторого $d \in \mathbb{N}$ существуют многочлены $G_j \in \chi$, $H_j \in \mathcal{R}_k$, элементы $b_j \in R$ и векторы $\mathbf{i}_j \in \mathbb{N}_0^k$, $j = 1, \dots, d$, такие, что

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

Назовем многочлен A нормальным по модулю множества χ , если не существует такого многочлена H , что $A \rightarrow_\chi H$, то есть если многочлен A не содержит такого ненулевого монома, который редуцируется ведущим мономом какого-либо многочлена из множества χ .

Через $N(\chi)$ обозначим множество всех нормальных многочленов по модулю χ . Многочлен H назовем нормальной формой многочлена A по модулю χ , если $H \in N(\chi)$ и либо $A = H$, либо A редуцируется к H по модулю множества χ . Пусть $NF(A, \chi)$ — множество всех нормальных форм многочлена A по модулю χ . Отметим, что $0 \in N(\chi)$ для любого $\chi \subset \mathcal{R}_k$ и $0 \in NF(A, \chi)$ для любого $A \in \chi$.

Теорема 5. Пусть $\chi = \{G_1, \dots, G_t\} \subset \mathcal{R}_k$ — круллева система многочленов с опорной диаграммой Ферре $\mathcal{F} \subset \mathbb{N}_0^k$. Тогда существует алгоритм $\rightarrow_\chi$ редуцирования многочленов $A \in \mathcal{R}_k \setminus N(\chi)$ по модулю множества χ , при котором $A \rightarrow_\chi H$, где $H \in N(\chi)$.

Доказательство этой теоремы дословно повторяет доказательство теоремы 4.1 из [13], сформулированной для случая, когда опорная диаграмма Ферре системы χ конечна.

Отметим, что в общем случае последнюю теорему нельзя дополнить утверждением о единственности нормальной формы. Соответственно неверно и утверждение о том, что идеалу $I = \mathcal{R}_k \chi$ принадлежат лишь многочлены с нулевой нормальной формой. Так, в примере 3 $H(\mathbf{x}) = 2x_2$ — ненулевой многочлен в нормальной форме, принадлежащий идеалу I , $H = 2G_1 + x_2G_2 - x_1G_3$.

Пример 4 ([13]). Пусть $R = \mathbb{Z}_4$ и упорядочение $\preccurlyeq$ выбрано так же, как и в примере 3. Тогда $\chi = \{G_1(\mathbf{x}) = x_1^2 - 2, G_2(\mathbf{x}) = x_1x_2 - 2, G_3(\mathbf{x}) = x_2^2\}$ есть круллева система многочленов с опорной диаграммой $\mathcal{F} = \{(0, 0), (0, 1), (1, 0)\}$. Многочлен $A = x_1^2x_2$ имеет две различные нормальные относительно χ формы $2x_2 = A - x_2G_1$ и $2x_1 = A - x_1G_2$.

Условия, при которых в теореме 5 нормальная форма многочлена A единственна, легко формулируются в терминах кольца операторов $S = \mathcal{R}_k/I$ идеала $I = \mathcal{R}_k\chi$, которое мы можем рассматривать как R -модуль и представить как расширение факторкольца $\tilde{R} = R/I \cap R$:

$$S = \tilde{R}[\vartheta_1, \dots, \vartheta_k], \quad \vartheta_s = x_s + I, \quad s = 1, \dots, k. \quad (26)$$

Теорема 6 ([13]). Пусть $\chi \subset \mathcal{R}_k$ — круллева система с опорной диаграммой Ферре $\mathcal{F} \neq \emptyset$. Тогда R -модуль ${}_RS$ имеет несократимую систему образующих

$$\mathcal{A} = \{\vartheta^{\mathbf{i}} : \mathbf{i} \in \mathcal{F}\}. \quad (27)$$

Для того, чтобы любой многочлен $A \in \mathcal{R}_k$ имел единственную нормальную форму по модулю χ , достаточно, чтобы система $\mathcal{A}$ была линейно независимой, то есть чтобы модуль ${}_RS$ был свободным.

Нашим основным результатом является следующая теорема. В [13] этот результат был сформулирован и доказан лишь для унитарных идеалов.

Теорема 7. Пусть $I \triangleleft \mathcal{R}_k$, $\preccurlyeq$ — мономимальное упорядочение на $\mathbb{N}_0^k$. Тогда для некоторого $t \in \{0, 1, \dots, n-1\}$ существуют цепочка

$$\mathcal{F}_t \subset \mathcal{F}_{t-1} \subset \dots \subset \mathcal{F}_0 \subset \mathbb{N}_0^k \quad (28)$$

строго упорядоченных по включению диаграмм Ферре и набор

$$\|I\| = a_0 < a_1 < \dots < a_t < a_{t+1} = n \quad (29)$$

целых чисел, удовлетворяющие следующим условиям:

(C1) для любых $F \in \mathcal{R}_k$ и $s \in \{0, 1, \dots, t\}$

$$(F \in I, \mathfrak{S}(F) \subseteq \mathcal{F}_s) \implies (\|F\| \geq a_{s+1});$$

(C2) для каждого $s \in \{0, 1, \dots, t\}$ существует круллева система $\chi_s \subset \mathcal{R}_k$ $\mathcal{F}_s$ -унитарных многочленов такая, что $\pi^{a_s} \chi_s \subset I$.

При условии (C1) любая система многочленов

$$\chi_0, \chi_1, \dots, \chi_t, \quad (30)$$

удовлетворяющая условию (C2), обладает также следующими свойствами.

(C3) Если $F \in I$ и $\|F\| = a \geq a_s$ для некоторого $s \in \{0, 1, \dots, t\}$, то

$$F \in \mathcal{R}_k\{\pi^a \chi_s \cup \pi^{a_{s+1}} \chi_{s+1} \cup \dots \cup \pi^{a_t} \chi_t\},$$

в частности,

$$I = \mathcal{R}_k\{\pi^{a_0} \chi_0 \cup \pi^{a_1} \chi_1 \cup \dots \cup \pi^{a_t} \chi_t\}.$$

(C4) Если $s \in \{0, 1, \dots, t\}$ и $a_s \leq a < a_{s+1}$, то

$$I \cap \pi^a \mathcal{R}_k = \mathcal{R}_k \{ \pi^a \chi_s \cup \pi^{a_{s+1}} \chi_{s+1} \cup \dots \cup \pi^{a_t} \chi_t \}, \quad (31)$$

$$(I : \pi^a) = \mathcal{R}_k \{ \chi_s \cup \pi^{a_{s+1}-a} \chi_{s+1} \cup \dots \cup \pi^{a_t-a} \chi_t \cup \{ \pi^{n-a} \} \}. \quad (32)$$

(C5) Если $H(\mathbf{x}) = H_0(\mathbf{x}) \in \mathcal{R}_k$ и $H_1(\mathbf{x}), \dots, H_{t+1}(\mathbf{x})$ — многочлены, построенные рекурсивно по правилу: $H_{s+1} \in NF(H_s, \chi_s)$, $s = 0, 1, \dots, t$, то включение $H \in I$ эквивалентно системе условий

$$\|H_s(x)\| \geq a_s, \quad s = 0, 1, \dots, t+1. \quad (33)$$

(C6) Множество

$$\chi = \pi^{a_0} \chi_0 \cup \pi^{a_1} \chi_1 \cup \dots \cup \pi^{a_t} \chi_t$$

является стандартным базисом идеала I относительно упорядочения $\preccurlyeq$, то есть для любого многочлена $F \in \mathcal{R}_k$ условия $F \in I$ и $F \rightarrow_\chi 0$ равносильны.

(C7) Идеал I является унитарным тогда и только тогда, когда $a_0 = 0$ и диаграмма $\mathcal{F}_0$ конечна (то есть все диаграммы $\mathcal{F}_s$ конечны). Если I — унитарный идеал, R — конечное кольцо, $\bar{R} = GF(q)$ и $|\mathcal{F}_s| = m_s$ для $s = 0, 1, \dots, t$, то $S = \mathcal{R}_k/I$ — конечное кольцо и

$$|S| = q^{(m_0-m_1)a_1+\dots+(m_{t-1}-m_t)a_t+m_t n}. \quad (34)$$

В условиях теоремы 7 система образующих

$$\chi = \pi^{a_0} \chi_0 \cup \pi^{a_1} \chi_1 \cup \dots \cup \pi^{a_t} \chi_t \quad (35)$$

идеала I называется канонической системой образующих (КСО) идеала I (относительно допустимого упорядочения $\preccurlyeq$).

Доказательство. Сначала рассмотрим случай $\|I\| = a_0 = 0$. Построим цепочки (28) и (29), удовлетворяющие условиям (C1), (C2). Пусть $\chi_0 = \{G_1^{(0)}, \dots, G_{t_0}^{(0)}\}$ — главная часть КСО идеала I — крулева система с опорной диаграммой $\mathcal{F}_0$ такая, что $\bar{\chi}_0$ — редуцированный базис Гребнера идеала $\bar{I}$. Обозначим через $\mathcal{N}_0$ множество всех нормальных форм по модулю χ_0 всех многочленов из идеала I . Заметим, что $\|\mathcal{N}_0\| = a_1 > 0$, так как нормальная форма любого многочлена из $\bar{I}$ по модулю $\bar{\chi}_0$ равна 0. Если $a_1 = n$, то $I = \mathcal{R}_k \chi_0$ и условия (C1), (C2) выполняются при $t = 0$.

Пусть $a_1 < n$. Рассмотрим идеал I_1 , порожденный в $\mathcal{R}_k$ множеством $\mathcal{N}_0 \cup \pi^{a_1} \chi_0$. Очевидно, $I_1 \subseteq I \cap \pi^{a_1} \mathcal{R}_k$, и по построению идеал I_1 содержит любой многочлен $F \in I \cap \pi^{a_1} \mathcal{R}_k$, поскольку редуцирование многочлена F по модулю системы χ_0 дает соотношение

$$F = Q_1 G_1^{(0)} + \dots + Q_{t_0} G_{t_0}^{(0)} + H, \quad Q_1, \dots, Q_{t_0} \in \pi^{a_1} \mathcal{R}_k, \quad H \in \mathcal{N}_0.$$

Следовательно,

$$I_1 = I \cap \pi^{a_1} \mathcal{R}_k. \quad (36)$$

Таким образом, диаграмма $\mathcal{F}_0$ и система параметров $a_0 < a_1$ удовлетворяют условиям (C1), (C2) при $s = 0$. Допустим, что мы уже построили набор строго убывающих диаграмм Ферре

$$\mathcal{F}_0 \supset \mathcal{F}_1 \supset \dots \supset \mathcal{F}_i \quad (37)$$

и набор строго возрастающих целых чисел

$$0 = a_0 < a_1 < \dots < a_i < a_{i+1} \leq n, \quad (38)$$

а также соответствующий набор круллевых систем

$$\chi_0, \chi_1, \dots, \chi_i, \quad (39)$$

такие, что условия (C1), (C2) выполняются для $s \in \{0, 1, \dots, i\}$ и

$$a_{i+1} = \|\{A \in I : \mathfrak{S}(A) \subseteq \mathcal{F}_i\}\|. \quad (40)$$

Если в (40) $a_{i+1} = n$, то $i = i$ и нужный набор параметров и круллевых систем построен.

Пусть $a_{i+1} < n$. Очевидно, достаточно показать, что в этом случае к каждой из цепочек (37)–(39) можно добавить еще по одному звену с сохранением свойств (C1), (C2) и свойства, соответствующего (40). Для произвольного многочлена $A \in \mathcal{R}_k$ построим цепочку нормальных форм

$$H_0 \in NF(A, \chi_0), \quad H_s \in NF(H_{s-1}, \chi_s), \quad s = 1, \dots, i. \quad (41)$$

Нормальную форму H_s назовем s -й нормальной формой многочлена A относительно набора круллевых систем (39). Заметим, что так как для $s \in \{0, 1, \dots, i\}$ выполняются включения $\mathfrak{S}(H_s) \subseteq \mathcal{F}_s$ и справедливы свойства (C1), (C2), то для любого $A \in I$ выполняются соотношения $H_s \in I$, $\|H_s\| \geq a_{s+1}$, $s = 0, 1, \dots, i$. Обозначим через $\mathcal{N}_s$ множество всех s -х нормальных форм H_s всех многочленов A из идеала I . Очевидно, что $\|\mathcal{N}_i\| = a_{i+1}$. Рассмотрим идеал I_{i+1} , порожденный в $\mathcal{R}_k$ множеством $\mathcal{N}_i \cup \pi^{a_{i+1}}(\chi_0 \cup \dots \cup \chi_i)$. Очевидно, $I_{i+1} \subseteq I \cap \pi^{a_{i+1}}\mathcal{R}_k$, и по построению идеал I_{i+1} содержит любой многочлен $F \in I \cap \pi^{a_{i+1}}\mathcal{R}_k$. Следовательно,

$$I_{i+1} = I \cap \pi^{a_{i+1}}\mathcal{R}_k. \quad (42)$$

Рассмотрим идеал $J_{i+1} = (I_{i+1} : \pi^{a_{i+1}})$. Очевидно, это идеал нормы 0, содержащий системы (39), поэтому ввиду предложения 3 главная часть χ_{i+1} КСО идеала J_{i+1} есть круллева система с опорной диаграммой $\mathcal{F}_{i+1} \subseteq \mathcal{F}_i$, удовлетворяющая условию $\pi^{a_{i+1}}\chi_{i+1} \subset I$. В случае $J_{i+1} = \mathcal{R}_k$, верно равенство $\mathcal{F}_{i+1} = \emptyset$ и $\mathcal{F}_{i+1} \subset \mathcal{F}_i$ — строгое включение. Пусть далее $J_{i+1} \neq \mathcal{R}_k$. Тогда, при сделанных предположениях, можно утверждать, что множество $\mathcal{N}_{i+1}$ содержит многочлен $H = \pi^{a_{i+1}}B$ для некоторого многочлена $B \in \mathcal{R}_k$ такого, что $B \neq \bar{0}$ и $\mathfrak{S}(B) \subseteq \mathcal{F}_i$. По предложению 3 это означает, что $\mathcal{F}_{i+1} \neq \mathcal{F}_i$, то есть $\mathcal{F}_{i+1} \subset \mathcal{F}_i$ — строгое включение. Таким образом, мы имеем строго убывающую цепочку диаграмм Ферре

$$\mathcal{F}_0 \supset \mathcal{F}_1 \supset \dots \supset \mathcal{F}_{i+1}, \quad (43)$$

являющихся опорными, соответственно, для круллевых систем из набора

$$\chi_0, \chi_1, \dots, \chi_{i+1}, \quad (44)$$

удовлетворяющих условию (C2) для $s = 0, 1, \dots, i + 1$. Для каждого многочлена $A \in \mathcal{R}_k$ к цепочке нормальных форм (41) можно добавить многочлен $H_{i+1} \in NF(H_i, \chi_{i+1})$. При этом множество $\mathcal{N}_{i+1}$ всех $(i + 1)$ -х нормальных форм всех многочленов $A \in I$ имеет норму, большую, чем a_{i+1} , то есть параметр

$$a_{i+2} = \|\{A \in I : \mathfrak{S}(A) \subseteq \mathcal{F}_{i+1}\}\| \quad (45)$$

удовлетворяет соотношениям $a_{i+1} < a_{i+2} \leq n$. Действительно, если $A \in I$ и $\mathfrak{S}(A) \subseteq \mathcal{F}_{i+1}$, то $\mathfrak{S}(A) \subseteq \mathcal{F}_i$ и потому $\|A\| \geq a_{i+1}$, то есть $A \in I_{i+1}$. Более того, $A = \pi^{a_{i+1}} B$, где $B \in J_{i+1}$, $\mathfrak{S}(B) = \mathfrak{S}(A) \subseteq \mathcal{F}_{i+1}$. Следовательно, $\|B\| \geq 1$ (ввиду выбора системы χ_{i+1}) и $\|A\| \geq a_{i+1} + 1$. Таким образом, мы доказали возможность удлинения цепочек (37)–(39) при условии $a_{i+1} < n$ и тем самым – существование набора параметров (28), (29) удовлетворяющих условиям (C1), (C2) теоремы.

Рассмотрим теперь общий случай $\|I\| = a_0 \geq 0$. Идеал $I' = (I : \pi^{a_0})$ имеет норму 0. Следовательно, по доказанному выше, для некоторого $t' \in \{0, 1, \dots, n - 1\}$ существуют цепочка $\mathcal{F}_{t'} \subset \mathcal{F}_{t'-1} \subset \dots \subset \mathcal{F}_0$ строго упорядоченных по включению диаграмм Ферре и набор $0 = a'_0 < a'_1 < \dots < a'_{t'} < a'_{t'+1} = n$ целых чисел, удовлетворяющие условиям

(C'1) для любых $F' \in \mathcal{R}_k$ и $s \in \{0, 1, \dots, t'\}$

$$(F' \in I', \mathfrak{S}(F') \subseteq \mathcal{F}_s) \implies (\|F'\| \geq a'_{s+1});$$

(C'2) для каждого $s \in \{0, 1, \dots, t'\}$ существует крулева система $\chi_s \subset \mathcal{R}_k$ $\mathcal{F}_s$ -унитарных многочленов такая, что $\pi^{a_s} \chi_s \subset I'$.

Положим

$$t = \max\{s \in \{0, 1, \dots, t'\} : a'_s + a < n\}, \quad a_s = a_0 + a'_s, \quad s = 0, 1, \dots, t.$$

Докажем, что при введенных обозначениях рассматриваемый идеал I удовлетворяет условиям (C1), (C2).

Пусть $F \in I$ и $\mathfrak{S}(F) \subseteq \mathcal{F}_s$ для некоторого $s \in \{0, 1, \dots, t\}$. Заметим, что $F = \pi^{a_0} F'$, где $F' \in I'$, причем F' можно выбрать так, что $\mathfrak{S}(F') = \mathfrak{S}(F) \subseteq \mathcal{F}_s$. Тогда из (C'1) следует, что $\|F'\| \geq a'_{s+1}$. Значит, $\|F\| \geq a_0 + a'_{s+1} = a_{s+1}$, то есть верно (C1).

Условие (C2) очевидно следует из (C'2) и включения $\pi^{a_0} I' \subseteq I$.

Докажем теперь, что любая система многочленов (30), удовлетворяющая условиям (C1), (C2), обладает также свойствами (C3)–(C7).

Докажем свойство (C3). Используем индукцию по параметру $b = n - a \geq 0$. Если $b = 0$, то $F = 0$ и утверждение очевидно. Пусть $l > 0$ и утверждение верно для всех $b < l$, докажем его для случая $b = l$. Многочлен F можно представить в виде $F = \pi^a G$, $G \in \mathcal{R}_k$. Редуцируя многочлен G по модулю системы

$$\chi_s = \{G_1^{(s)}, \dots, G_{r_s}^{(s)}\}, \quad (46)$$

получаем равенство

$$G = \sum_{i \in \{1, \dots, r_s\}} Q_i G_i^{(s)} + H, \quad \mathfrak{S}(H) \subseteq \mathcal{F}_s. \quad (47)$$

Умножая обе части этого равенства на π^a и пользуясь включением $\pi^a \chi_s \subset I$, получаем, что $\pi^a H = F_1 \in I$, откуда, ввиду свойства (C1), следует неравенство $\|F_1\| \geq a_{s+1}$. Таким образом, $n - \|F_1\| < l$, и по предположению индукции справедливо включение

$$\pi^a H = F_1 \in \mathcal{R}_k \{\pi^{a_{s+1}} \chi_{s+1} \cup \dots \cup \pi^{a_l} \chi_l\}.$$

Отсюда и из (47) следует нужное включение для F .

Докажем свойство (C4). Равенство (31) есть переформулировка свойства (C3). Докажем (32). Если многочлен $G \in \mathcal{R}_k$ принадлежит идеалу из правой части (32), то $\pi^a G$ принадлежит, очевидно, идеалу из правой части (31). Следовательно, $\pi^a G \in I$ и $G \in (I : \pi^a)$. Наоборот, если $G \in (I : \pi^a)$, то $\pi^a G \in I \cap \pi^a \mathcal{R}_k$, то есть $\pi^a G$ принадлежит идеалу, стоящему в правой части равенства (31). Отсюда легко увидеть, что G принадлежит правой части (32).

Докажем свойство (C5). При обозначениях (46) для подходящих многочленов $Q_i^{(s)} \in \mathcal{R}_k$ последовательные редукции из условия дают соотношения

$$H_0 = \sum_{i \in \{1, \dots, r_0\}} Q_i^{(0)} G_i^{(0)} + H_1, \quad \mathfrak{S}(H_1) \subseteq \mathcal{F}_0; \quad (48)$$

$$H_s = \sum_{i \in \{1, \dots, r_s\}} Q_i^{(s)} G_i^{(s)} + H_{s+1}, \quad \mathfrak{S}(H_{s+1}) \subseteq \mathcal{F}_s, \quad s = 1, \dots, t. \quad (49)$$

При этом, если выполняются условия (33), то $H_{t+1} = 0$ и для подходящих многочленов $K_i^{(s)} \in \mathcal{R}_k$ выполняются равенства $Q_i^{(s)} = \pi^{a_s} K_i^{(s)}$. Поэтому, ввиду (C3),

$$H = \sum_{s \in \{0, 1, \dots, t\}} \sum_{i \in \{1, \dots, r_s\}} K_i^{(s)} (\pi^{a_s} G_i^{(s)}) \in I.$$

Наоборот, если $H \in I$, то из (48) и (C3) следует, что $H_1 \in I$, а из (48) и (C1) следует, что $\|H_1\| \geq a_1$. Далее, аналогично рассуждая, из (49) и (C3), (C1) последовательно для $s = 1, \dots, t$ получаем, что в (49) выполняются соотношения

$$\|Q_i^{(s)}\| \geq a_s, \quad Q_i^{(s)} G_i^{(s)} \in I, \quad H_{s+1} \in I, \quad \|H_{s+1}\| \geq a_{s+1}.$$

Свойство (C6) очевидным образом следует из (C5).

Наконец, докажем свойство (C7). Как уже отмечалось, унитарность идеала I равносильна конечной порожденности R -модуля $S = \mathcal{R}_k/I$. Если a_0 положительно, то ${}_R M$ не имеет конечной системы образующих, поскольку фактором этого модуля является R -модуль $S/\pi^{a_0} S \cong (R/\pi^{a_0} R)[x]$, не имеющий конечной системы образующих. Если $a_0 = 0$, то $I \subset J = \mathcal{R}_k \chi_0 + \pi \mathcal{R}_k$ и $\mathcal{R}_k/J \cong \bar{R}[x_1, \dots, x_k]/\bar{R}[x_1, \dots, x_k]\bar{\chi}_0$ есть фактормодуль модуля ${}_R S$. При этом, если $\mathcal{F}_0$ — бесконечная диаграмма Ферре, то, очевидно, R -модуль $\mathcal{R}_k/J$ не имеет конечной системы образующих. Если $a_0 = 0$ и диаграмма Ферре $\mathcal{F}_0$ конечна, то конечная порожденность модуля ${}_R S$ очевидна. Оставшаяся часть утверждения данного пункта доказана в [13].

Пример 5. Построим КСО χ идеала $I = \mathcal{R}_2\{F_1, \dots, F_6\}$, порожденного многочленами из левой части системы (12). Пусть $\prec$ — лексикографическое упорядочение множества $\mathbb{N}_0^2$, при котором $x_1 < x_2$. В обозначениях из доказательства последней теоремы очевидно, что $a_0 = 0$ и

$$\begin{aligned} \bar{I} &= \bar{\mathcal{R}}_2\{\bar{F}_1 = x_1^3 \oplus x_1^2, \bar{F}_2 = x_2^2 \oplus x_1^2 x_2 \oplus x_1^2, \\ &\quad \bar{F}_3 = x_2^2 \oplus x_1 x_2 \oplus x_1^2, \bar{F}_4 = x_1 x_2^2 \oplus x_2^2, \bar{F}_5 = x_2^3 \oplus x_1^2\}. \end{aligned}$$

Применяя алгоритм Бухбергера, получаем, что редуцированным базисом Гребнера идеала $\bar{I}$ является множество

$$\bar{\chi}_0 = \{\bar{F}_1 = x_1^3 \oplus x_1^2, \bar{F}_3 = x_2^2 \oplus x_1 x_2 \oplus x_1^2, x_1^2 x_2 \oplus x_1 x_2\}.$$

Заметим, что $x_1^2 x_2 + x_1 x_2 = \overline{F_2 + 3F_3}$. Последний факт нетрудно проверить, пользуясь непосредственно определением редуцированного базиса Гребнера. Теперь ясно, что главная часть КСО идеала I есть

$$\chi_0 = \{F_1, F_3, F_2 + 3F_3 = x_1^2 x_2 + 3x_1 x_2\}.$$

Далее, несложным перебором получаем, что $I_1 = 2J_1$, где

$$J_1 = \mathcal{R}_2\{F_1, F_2, F_3, F_4, F_5, x_2 + x_1, 2\},$$

значит,

$$\bar{J}_1 = \bar{\mathcal{R}}_2\{\bar{F}_1, \bar{F}_2, \bar{F}_3, \bar{F}_4, \bar{F}_5, x_2 \oplus x_1\}.$$

Редуцированным базисом Гребнера идеала $\bar{J}_1$ является множество $\bar{\chi}_1 = \{x_1^2, x_2 \oplus x_1\}$. Замечая, что $x_1^2 = F_3 + x_2(x_2 + x_1) \in I_1$, получаем, что главная часть КСО идеала I_1 есть $\chi_1 = \{x_1^2, x_2 + x_1\}$.

Таким образом, КСО идеала I есть

$$\chi = \{F_1, F_3, x_1^2 x_2 + 3x_1 x_2\} \cup 2\{x_1^2, 2x_2 + x_1\}.$$

Следует заметить, что построенная в теореме 7 КСО идеала I , вообще говоря, не является его редуцированным базисом Гребнера, поскольку она может содержать заведомо лишние для порождения идеала многочлены. Эта избыточность возникает в случае, если (в обозначениях теоремы) $t > 0$ и для некоторого $s < t$ существует внешний угол $\mathbf{i} \in \mathcal{H}\mathcal{F}_s$, принадлежащий также $\mathcal{H}\mathcal{F}_{s+1}$. В таком случае существуют многочлены $G \in \chi_s$, $H \in \chi_{s+1}$ такие, что $\text{ldg}(G) = \text{ldg}(H) = \mathbf{i}$, и по построению $\bar{G} = \bar{H}$. Отсюда следует, что в системе образующих $\pi^{a_0} \chi_0 \cup \pi^{a_1} \chi_1 \cup \dots \cup \pi^{a_t} \chi_t$ идеала I многочлен $\pi^{a_{s+1}} H$ лишний.

Пример 6. Пусть $R = \mathbf{Z}_4$, $I \triangleleft \mathcal{R}_2$ — идеал с системой образующих

$$\psi = \{x_1^2, x_2^2, x_1 x_2, 2x_2\}$$

и $\preccurlyeq$ — градуированное лексикографическое упорядочение, при котором $x_2 \prec x_1$. Нетрудно увидеть, что главная часть КСО этого идеала есть круллева система $\chi_0 = \{x_1^2, x_2^2, x_1 x_2\}$ с опорной диаграммой $\mathcal{F}_0 = \{(0, 0), (0, 1), (1, 0)\}$ и идеал $I_1 = I \cap 2\mathcal{R}_2$ порождается многочленами $2x_1^2, 2x_2$. Следовательно, главная часть КСО идеала $J_1 = (I_1 : 2)$ есть круллева система $\chi_1 = \{x_1^2, x_2\}$ с опорной диаграммой $\mathcal{F}_2 = \{(0, 0), (1, 0)\}$. Нетрудно видеть, что получившиеся диаграммы Ферре имеют общий внешний угол $(2, 0)$ и $2x_1^2$ — лишний многочлен в КСО $\chi_0 \cup 2\chi_1$ идеала I .

Отметим, однако, что именно эта допускаемая избыточность КСО позволяет сформулировать результаты (C3)–(C7) теоремы 7.

Результаты теорем 5, 7 делают интересным для изучения следующее понятие.

Определение 3. Круллеву систему многочленов $\chi \subset \mathcal{R}_k$ назовем системой Гребнера, если она есть КСО идеала $\mathcal{R}_k \chi$.

Заметим, что определение 3 обобщает данное в параграфе 3 определение системы Гребнера. По аналогии с предложением 4.15 из [13] несложно доказать следующее утверждение.

Предложение 6. Для собственного идеала $I \triangleleft \mathbb{R}_k$, имеющего КСО χ вида (35), в которой $a_0 = 0$, следующие условия эквивалентны:

- (а) $t = 0$, то есть χ_0 есть система Гребнера, порождающая I ;
 (б) для каждого многочлена $A \in I$ выполняется равенство

$$NF(A, \chi_0) = \{0\};$$

- (с) факторкольцо $S = \mathbb{R}_k/I$ есть свободный R -модуль с базисом

$$\mathcal{A}_0 = \{\vartheta^i : i \in \mathbb{F}_0\}, \quad (50)$$

определяемым из (26);

- (д) факторкольцо $S = \mathbb{R}_k/I$ есть свободный R -модуль.

5. Решение систем полиномиальных уравнений над кольцом Галуа–Эйзенштейна с помощью КСО

Здесь предлагается модификация изложенной в параграфе 2 методики решения системы полиномиальных уравнений (1) над ГЕ-кольцом R , использующая свойства канонической системы образующих χ идеала $I = \mathbb{R}_k\{F_1, \dots, F_d\} \triangleleft \mathbb{R}_k$.

Пусть $\preccurlyeq$ — некоторое допустимое упорядочение множества N_0^k и χ — КСО идеала I относительно упорядочения $\preccurlyeq$ вида (35). Согласно лемме 1 система (1) равносильна системе полиномиальных уравнений над R

$$\chi(\mathbf{x}) = 0. \quad (51)$$

Предлагается метод решения системы (51), представляющийся в случае $t > 0$ более эффективным, чем общий метод покоординатной линеаризации.

Заметим сразу, что достаточно рассмотреть случай $a_0 = 0$, так как иначе задача легко сводится к решению системы $\tilde{\chi}(\mathbf{x}) = 0$ над кольцом $\tilde{R} = R/\pi^{n-a_0}R$, где

$$\tilde{\chi} = \tilde{\chi}_0 \cup \pi^{a_1-a_0} \tilde{\chi}_1 \dots \cup \pi^{a_t-a_0} \tilde{\chi}_t.$$

Для упрощения обозначений вместо χ удобно рассмотреть избыточную систему функций

$$\psi = \psi_0 \cup \pi \psi_1 \cup \dots \cup \pi^{n-1} \psi_{n-1},$$

где $\psi_j = \chi_i$, если $a_i \leq j < a_{i+1}$. Очевидно, система уравнений (51) равносильна системе уравнений $\psi(\mathbf{x}) = 0$, то есть системе

$$\begin{aligned} \psi_0(\mathbf{x}) &= 0, \\ \pi \psi_1(\mathbf{x}) &= 0, \\ &\dots \\ \pi^{n-1} \psi_{n-1}(\mathbf{x}) &= 0. \end{aligned} \quad (52)$$

Структурированность системы ψ позволяет при условии $t > 0$ предложить следующие упрощения при решении соответствующих систем уравнений (4) и (6). Далее наряду с обозначениями, введенными в этом параграфе, используются также обозначения параграфа 2.

Теорема 8. Вектор $\mathbf{c} \in R^k$ есть решение системы уравнений (52) тогда и только тогда, когда

(а) нулевой координат-вектор $\mathbf{c}^{(0)} \in \Gamma^k$ есть решение системы уравнений

$$\psi_{n-1}(\mathbf{z}) \equiv 0 \pmod{\pi}, \quad (53)$$

(б) для каждого $j \in \{1, \dots, n-1\}$ координат-вектор $\mathbf{c}^{(j)} \in \Gamma^k$ есть решение системы

$$\psi_{n-j-1}(\mathbf{c}^{[j]} + \pi^j \mathbf{z}) \equiv 0 \pmod{\pi^{j+1}}. \quad (54)$$

Доказательство. Заметим, что

$$\mathbf{c} \equiv \mathbf{c}^{[j+1]} \equiv \mathbf{c}^{[j]} + \pi^j \mathbf{c}^{(j)} \pmod{\pi^{j+1}}, \quad j = 1, \dots, n-1,$$

поэтому с учетом равенства $\mathbf{c}^{(0)} = \mathbf{c}^{[1]}$ совокупность условий (а), (б) равносильна условию

$$\pi^{n-j-1} \psi_{n-j-1}(\mathbf{c}) = 0, \quad j = 0, 1, \dots, n-1,$$

которое, очевидно, равносильно условию $\psi(\mathbf{c}) = 0$.

Заметим также, что, как показано в параграфе 2 (см. (11)), система уравнений (54) равносильна следующей системе линейных уравнений над полем Γ :

$$D\psi_{n-j-1}^{(0)}(\mathbf{c}^{(0)}) \cdot \mathbf{z}^\downarrow =_{\Gamma} -\gamma_j(\psi_{n-j-1}^\downarrow(\mathbf{c}^{[j]})) \quad (55)$$

Предлагается следующая модификация алгоритма 1.

Алгоритм 2. Вход: система уравнений (51).

Выход: множество K всех решений в R^k системы (51).

Суть алгоритма состоит в том, что последовательно по определенным ниже правилам строятся двумерные массивы (таблицы) $A_0, A_1, \dots, A_{n-1}$, в ячейки которых записываются векторы из Γ^k . Количество столбцов в j -м массиве равно $j+1$, а количество строк меняется в процессе работы алгоритма. В начальном такте работы все массивы пусты. Алгоритм заканчивает работу, если либо для некоторого $j < n-1$ массив A_j после его заполнения остался пустым (в таком случае система не имеет решений), либо завершено заполнение массива A_{n-1} (в таком случае K есть, по сути, множество строк массива A_{n-1}).

Этап I. Построение решений над полем вычетов. Найдем все решения в Γ^k системы сравнений $\psi_{n-1}(\mathbf{x}) \equiv 0 \pmod{\pi}$. Пусть $C^{(0)} \subset \Gamma^k$ — множество решений данной системы.

Если $C^{(0)} = \emptyset$, то полагаем $K = \emptyset$ и работа алгоритма 2 закончена.

В противном случае, перенумеровав каким-либо образом все получившиеся решения, поместим их в массив A_0 . Если $n = 1$, то полагаем $K = C^{(0)}$ и завершаем работу алгоритма. Если $n > 1$, то обозначаем через b_0 число строк в массиве A_0 и переходим к второму этапу.

Этап II. Подъем решений. Этап состоит из $n - 1$ шагов. На j -м шаге, $j \in \{1, \dots, n - 1\}$, строится массив A_j , строки которого формируются путем последовательной обработки строк уже построенного массива A_{j-1} . Пусть $b_j(v)$ — число строк массива A_j , полученных после обработки первых v строк массива A_{j-1} , и b_j — общее число строк массива A_j ($b_j = b_j(b_{j-1})$).

Допустим, что для некоторого $v \in \{1, \dots, b_{j-1}\}$ уже обработаны строки массива A_{j-1} с номерами $1, \dots, v - 1$, в результате чего сформировано $b_j(v - 1)$ строк массива A_j . Тогда обработка v -й строки массива A_{j-1} сводится к следующему. Если $A_{j-1}(v, 1) = \mathbf{c}^{(0)}$, $A_{j-1}(v, 2) = \mathbf{c}^{(1)}, \dots, A_{j-1}(v, j) = \mathbf{c}^{(j-1)}$, то решается система сравнений (54), которая, как уже отмечалось выше, эквивалентна системе линейных уравнений (55) над Γ . Пусть $C^{(j)}(v) \subset \Gamma^k$ — множество ее решений и l — его мощность. Полагаем $b_j(v) = b_j(v - 1) + l$ и если $l > 0$, то произвольно нумеруем элементы множества $C^{(j)}(v) = \{\mathbf{c}_1^{(j)}, \dots, \mathbf{c}_l^{(j)}\}$ и для каждого $s \in \{1, \dots, l\}$ полагаем

$$A_j(b_j(v - 1) + s, 1) = A_{j-1}(v, 1) = \mathbf{c}^{(0)},$$

...

$$A_j(b_j(v - 1) + s, j) = A_{j-1}(v, j) = \mathbf{c}^{(j-1)},$$

$$A_j(b_j(v - 1) + s, j + 1) = \mathbf{c}_s^{(j)}.$$

Если $v = b_{j-1}$, то процедура формирования массива A_j закончена. В противном случае, мы аналогичным образом обрабатываем $(v + 1)$ -ю строку массива A_{j-1} .

Если $b_j = 0$, то есть массив A_j пуст, то алгоритм завершает работу, в противном случае переходим к построению массива A_{j+1} . Заметим, что массив A_{j-1} в дальнейшем уже не нужен и может быть удален из памяти. Таким образом, в каждый момент работы алгоритма в памяти достаточно хранить лишь все неиспользованные строки последнего построенного массива и все строки очередного строящегося массива.

По завершении формирования массива A_{n-1} положим

$$K = \{A_{n-1}(i, 1) + \pi A_{n-1}(i, 2) + \dots + \pi^{n-1} A_{n-1}(i, n) : i = 1, \dots, b_{n-1}\} \subset R^k.$$

Используя теорему 8 и рассуждения из доказательства предложения 1, легко показать, что K есть множество всех решений системы (51).

Заметим, что алгоритм 2 отличается от примененного к системе (52) алгоритма 1 лишь тем, что здесь для построения j -х координат решений системы (51) решается не система $\chi(\mathbf{c}^{[j]} + \pi^j \mathbf{z}) \equiv 0 \pmod{\pi^{j+1}}$, как положено по алгоритму 1, а лишь ее подсистема. Поэтому, если для заданной системы уравнений (52) удастся просто построить КСО идеала, порожденного многочленами из ее левой части, и эта КСО состоит из $t > 0$ компонент, то для решения исходной системы, вместо алгоритма 1, может оказаться более эффективным решение эквивалентной системы (52) по алгоритму 2.

Пример 7. Решим с помощью предложенного выше метода систему уравнений из примера 1 над $R = \mathbb{Z}_4$.

Для этого воспользуемся построенной в примере 5 КСО идеала I , порожденного многочленами из левой части системы (12):

$$\chi = \{F_1, F_3, x_1^2 x_2 + 3x_1 x_2\} \cup \{2x_1^2, 2x_2 + 2x_1\}.$$

Согласно лемме 1 исходная система уравнений равносильна следующей системе:

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

Следуя алгоритму 2, для описания множества $C^{(0)}$ всех возможных нулевых координат решений исходной системы достаточно решить систему уравнений

$$\begin{aligned} z_1^2 &= 0, \\ z_2 \oplus z_1 &= 0, \end{aligned} \quad (56)$$

где $z_1, z_2 \in \Gamma = \bar{\mathbf{Z}}_4 = GF(2)$. Отметим, что система (56) состоит из меньшего, чем система (13), числа уравнений (два вместо пяти), которые к тому же проще. Очевидно, система (56) имеет единственное решение $(0, 0)$, то есть для любого решения с исходной системы $c^{(0)} = (0, 0)$. Для описания всех возможных поднятий найденного решения согласно алгоритму 2 составим систему линейных уравнений (55), которая в нашем случае имеет вид

$$D\chi_0^{(0)}((0, 0))z^\downarrow = \Gamma - \gamma_1(\chi_0^\downarrow((0, 0))).$$

Легко заметить, что $D\chi_0^{(0)}((0, 0)) = 0_{3 \times 2}$, $-\chi_0^\downarrow((0, 0))^{(1)} = 0^\downarrow$. Очевидно, любой вектор $c^{(1)} = (c_1^{(1)}, c_2^{(1)}) \in \mathbf{Z}_2^2$ является решением данной системы. Значит, исходная система имеет 4 решения $(0, 0)$, $(0, 2)$, $(2, 0)$, $(2, 2)$.

Таким образом, по сравнению с общим методом покоординатной линеаризации, использование для решения системы (12) предложенной в данном параграфе модификации может привести к решению более простых систем уравнений над полем Γ . Более того, использование КСО может также приводить к меньшему по сравнению с алгоритмом 1 исходному множеству $C^{(0)}$ возможных значений нулевых координат.

Пример 8. Пусть над $R = \mathbf{Z}_9$ задана система уравнений

$$\begin{aligned} x^2 - 1 &= 0, \\ x^2 - 1 + 3(x - 1) &= 0. \end{aligned} \quad (57)$$

Положим

$$\psi = \{x^2 - 1, x^2 - 1 + 3(x - 1)\}, \quad I = R[x]\psi.$$

Если для решения системы (57) применить алгоритм 1, то для определения множества $C^{(0)}$ потребуется решить систему $\psi(x) \equiv 0 \pmod{3}$, то есть $x^2 \ominus 1 = 0$ над $\Gamma = \mathbf{Z}_3$. Последнее уравнение имеет два решения 1, 2. Очевидно, КСО идеала I есть множество $\chi = \chi_0 \cup 3\chi_1$, где $\chi_0 = \{x^2 - 1\}$, $\chi_1 = \{x - 1\}$. Если решать систему (57) по алгоритму 2, то $C^{(0)}$ определяется как множество решений в $\mathbf{Z}_3$ уравнения $\chi_1(x) \equiv 0 \pmod{3}$, то есть $x \ominus 1 = 0$. Данное уравнение имеет единственное решение 1. Таким образом, алгоритм 1 определил на первом этапе одно лишнее значение нулевой координаты, равное 2, которое отсеется в процессе его подъема. Использование же КСО и алгоритма 2 позволяет произвести указанный отсев на более раннем этапе.

Рис. 2. Матрица $D\psi^{(0)}(\mathbf{c}^{(0)})$

Отметим, что основные рассматриваемые в алгоритме 2 системы уравнений (53) и (55) отличаются от аналогичных систем (4) и (11) из алгоритма 1 тем, что их левые части соответствуют системам Гребнера, в то время как в алгоритме 1 они произвольны. Это позволяет говорить о снижении сложности решения систем из алгоритма 2 в случае, если в качестве допустимого упорядочения $\preccurlyeq$ на $\mathbf{N}_0^k$, которое использовалось при построении КСО χ , было выбрано лексикографическое упорядочение. Поясним специфику решения систем (4) и (11) в случае, если в левой части данных систем стоит круллева система $\mathcal{F}$ -унитарных многочленов $\psi = \{G_1, \dots, G_l\} \subset \mathcal{R}_k$ с опорной диаграммой Ферре $\mathcal{F} \subset \mathbf{N}_0^k$, соответствующая лексикографическому упорядочению $\preccurlyeq$. Всюду далее будем считать, что это упорядочение индуцировано следующим упорядочением переменных: $x_k < x_{k-1} < \dots < x_1$, то есть совпадает с упорядочением из теоремы 3.

Как было отмечено в параграфе 2, процесс решения системы (4) сводится к решению над полем Γ системы уравнений с редуцированным базисом Гребнера $\psi^{(0)}$ в левой части. Такая система может быть эффективно решена путем последовательного исключения переменных с использованием теоремы 3.

Охарактеризуем упрощения в решении соответствующей системы (11) с круллевой системой многочленов ψ в левой части. Без ограничения общности можно считать, что многочлены $G_1, \dots, G_l$ системы ψ упорядочены так, что

$$\text{ldg}(G_l) < \text{ldg}(G_{l-1}) < \dots < \text{ldg}(G_2) < \text{ldg}(G_1).$$

Так как множество $\psi^{(0)}$ является редуцированной системой Гребнера над полем Γ , для любых $G \in \psi$, $\mathbf{i} \in \mathfrak{S}(G^{(0)}) \setminus \{\text{ldg}(G)\}$ верны соотношения $\text{ldg}(G) = \text{mdg}(G^{(0)})$ и $\mathbf{i} < \text{ldg}(G)$. Последнее означает, что если $\text{ldg}(G) = (0, \dots, 0, j_s, \dots, j_k)$, $j_s \neq 0$, то $\mathfrak{S}(G^{(0)}) \subset \{0\}^{s-1} \times \mathbf{N}_0^{k-s+1}$, то есть $G^{(0)} \in \tilde{R}[x_s, \dots, x_k]$. Положим

$$t_s = |(\psi^{(0)} \cap \Gamma[x_s, \dots, x_k]) \setminus \Gamma[x_{s+1}, \dots, x_k]|, \quad s = 1, \dots, k-1.$$

Тогда при нашем выборе отношения $\preccurlyeq$ и упорядочения многочленов из множества ψ матрица $D\psi^{(0)}(\mathbf{c}^{(0)})$ соответствующей системы линейных уравнений (11) имеет блочно ступенчатый вид, изображенный на рис. 2.

Наличие значительного количества нулей в матрице $D\psi^{(0)}(\mathbf{c}^{(0)})$ облегчает решение соответствующей системы (11).

Очевидно, что самостоятельный интерес представляет изучение условий, при которых система (11) имеет единственное решение. Здесь мы рассмотрим первый естественный случай, когда $l = k$. В этом случае критерием определенности системы является условие $|D\psi^{(0)}(\mathbf{c}^{(0)})| \neq 0$. В связи с этим представляет интерес для изучения следующее понятие.

Напомним, что параллелепипедом называется диаграмма Ферре следующего вида:

$$\Pi(m_1, \dots, m_k) = \{0, 1, \dots, m_1 - 1\} \times \dots \times \{0, 1, \dots, m_k - 1\}, \quad m_1, \dots, m_k \in \mathbb{N}.$$

Определение 4. Редуцированная система Гребнера $\psi^{(0)} \subset \Gamma[x_1, \dots, x_k]$ называется треугольной системой Гребнера, если

$$\mathcal{F}_{\psi^{(0)}} = \Pi(m_1, \dots, m_k).$$

Замечание 1. Из определения 4 и задания упорядочения $\preccurlyeq$ следует, что треугольная система Гребнера $\psi^{(0)} \subset \Gamma[x_1, \dots, x_k]$ имеет вид

$$\psi^{(0)} = \{G_1^{(0)}(x_1, \dots, x_k), \dots, G_{k-1}^{(0)}(x_{k-1}, x_k), G_k^{(0)}(x_k)\},$$

где $\text{Lm}(G_s) \in \Gamma[x_s]$ для каждого $s \in \{1, \dots, k\}$.

Последний результат очевидно вытекает из следующей леммы.

Лемма 2. Пусть $\mathcal{F} \subset \mathbb{N}_0^k$ — конечная диаграмма Ферре. Тогда множество $\mathcal{H}\mathcal{F}$ 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 $\mathbf{s} = (s_1, \dots, s_k) \in \mathcal{F}$ таков, что координата s_i есть максимум i -х координат всех векторов из $\mathcal{F}$. Так как $\mathbf{u}_i = (0, \dots, 0, s_i, 0, \dots, 0) \leq \mathbf{s} \in \mathcal{F}$, то $\mathbf{v}_i = (0, \dots, 0, s_i + 1, 0, \dots, 0) \in \Delta\mathcal{F}$. Положим $h_i = s_i + 1$. Тогда согласно (20) вектор $\mathbf{v}_i = h_i \mathbf{1}_i$ принадлежит $\mathcal{H}\mathcal{F}$.

Предложение 7. Пусть $\psi^{(0)} \subset \Gamma[x_1, \dots, x_k]$ — система Гребнера. Тогда эквивалентны следующие утверждения:

- (а) $\psi^{(0)}$ — треугольная система Гребнера;
- (б) $|\psi^{(0)}| = k$ и $I = \Gamma[x_1, \dots, x_k]\psi^{(0)}$ — унитарный идеал.

Доказательство. Импликация (а) $\Rightarrow$ (б) очевидна.

Докажем, что (б) $\Rightarrow$ (а). По определению унитарный идеал I содержит k унитарных элементарных многочленов $F_1(x_1), \dots, F_k(x_k)$. Так как $\psi^{(0)}$ — базис Гребнера идеала I , для каждого $i \in \{1, \dots, k\}$ существует $G_i \in \psi^{(0)}$ такой, что

$$\text{mdg}(G_i) \leq \text{mdg}(F_i) = (0, \dots, 0, h_i, 0, \dots, 0),$$

то есть $\text{mdg}(G_i) = (0, \dots, 0, m_i, 0, \dots, 0) = \mathbf{s}_i$ для некоторого $m_i \in \mathbb{N}$. Так как $|\psi^{(0)}| = k$, отсюда и из теоремы 2 следует, что

$$\mathcal{H}\mathcal{F}_{\psi^{(0)}} = \{\mathbf{s}_1, \dots, \mathbf{s}_k\} = \mathcal{H}\Pi(m_1, \dots, m_k).$$

Значит,

$$\mathcal{F}_{\psi^{(0)}} = \Pi(m_1, \dots, m_k).$$

Определение 5. Круллеву систему многочленов $\psi \subset \mathcal{R}_k$ назовем треугольной, если

$$\mathcal{F}_\psi = \Pi(m_1, \dots, m_k).$$

Очевидно, что последнее условие равносильно тому, что $\psi^{(0)}$ является треугольной системой Гребнера.

Предложение 8. Пусть $j \in \{1, \dots, n-1\}$ и в левой части системы уравнений (11) стоит треугольная круллева система многочленов $\psi \subset \mathcal{R}_k$, вектор $\mathbf{c}^{[j]} \in R^k$ является решением системы (3). Тогда следующие два утверждения эквивалентны:

(а) существует и единственно решение системы уравнений (11);

(b) $D_i G_i^{(0)}(\mathbf{c}^{(0)}) \neq 0$ для любого $i = 1, \dots, k$.

Доказательство. Легко заметить, что в условиях предложения квадратная $k \times k$ матрица $D\psi^{(0)}(\mathbf{c}^{(0)})$ является верхнетреугольной с элементами $D_1 G_1^{(0)}(\mathbf{c}^{(0)})$, $D_2 G_2^{(0)}(\mathbf{c}^{(0)})$, $\dots$, $D_k G_k^{(0)}(\mathbf{c}^{(0)})$ на главной диагонали. Теперь очевидно, что условие $|D\psi^{(0)}(\mathbf{c}^{(0)})| \neq 0$, равносильное (а), эквивалентно условию (b).

Список литературы

1. Бокуть Л. А., Фонг Ю., Ке В.-Ф., Колесников П.С., Базисы Гребнера и Гребнера–Ширшова в алгебре и конформные алгебры. *Фундаментальная и прикладная математика* (2000) 6, №3, 669–706.
2. Бухбергер Б., Коллинз Дж., Лоос Р., *Компьютерная алгебра*. Мир, Москва, 1986.
3. Бухштаб А. А., *Теория чисел*. Просвещение, Москва, 1966.
4. Виноградов И. М. *Основы теории чисел*. Физматлит, Москва, 1965.
5. Ван дер Варден Б. Л., *Алгебра*. Наука, Москва, 1976.
6. Глухов М. М., Елизаров В. П., Нечаев А. А., *Алгебра*. ч. I, Гелиос, Москва, 2003; ч. II, Гелиос, Москва, 2003.
7. Золотых А. А., Михалев А. А., Стандартные базисы двусторонних идеалов свободных ассоциативных алгебр над кольцами многочленов. *Труды пятых матем. чтений МГСУ*. Москва, 1997, 100–104.
8. Золотых А. А., Михалев А. А., Алгоритмы построения стандартных базисов Гребнера–Ширшова идеалов свободных алгебр над коммутативными кольцами. *Программирование* (1998), №6, 10–11.
9. Ийуду Н. К., Симплификационные свойства слабо редуцируемых алгебр. *Фундаментальная и прикладная математика* (1996) 2, №1, 133–146.
10. Кокс Д., Литтл Дж., О’Ши Д., *Идеалы, многообразия и алгоритмы: введение в вычислительные аспекты алгебраической геометрии и коммутативной алгебры*. Мир, Москва, 2000.
11. Латышев В. Н., *Комбинаторная теория колец, стандартные базисы*. Изд-во МГУ, Москва, 1988.
12. Ленг С., *Алгебра*. Мир, Москва, 1968.
13. Михайлов Д. А., Нечаев А. А., Каноническая система образующих унитарного полиномиального идеала над коммутативным артиновым цепным кольцом. *Дискретная математика* (2001) 13, №4, 3–42.

14. Нечаев А. А., О строении конечных колец. *Матем. заметки* (1971) **10**, №6, 679–688.
15. Нечаев А. А., Линейные рекуррентные последовательности над коммутативными кольцами. *Дискретная математика* (1991) **3**, № 4, 107–121.
16. Нечаев А. А., Михайлов Д. А., Использование КСО для решения систем уравнений над кольцами. *XXXII Межведомств. научно-техн. конф. "Проблемы обеспечения эффективности и устойчивости функционирования сложных технических систем"*. СВИ РВ, Серпухов, 2003, т. 2, 49–52.
17. Панкратьев Е. В., О некоторых подходах к построению теорий дифференциальных базисов Гребнера. В кн.: *Математические методы и приложения*. Изд-во МГСУ, Москва, 2002, с. 132–135.
18. Поинтковский Д. И., Базисы Гребнера и когерентность мономиальной ассоциативной алгебры. *Фундаментальная и прикладная математика* (1996) **2**, №2, 501–509.
19. Сачков В. Н., *Введение в комбинаторные методы дискретной математики*. Наука, Москва, 1982.
20. Ширшов А. И., Некоторые алгоритмические проблемы для алгебр Ли. *Сиб. матем. журнал* (1962) **3**, 292–296.
21. Apel J., Lassner W., An extension of Buchberger's algorithm and calculations in enveloping fields of Lie algebras. *J. Symbolic Comput.* (1988) **6**, 361–370.
22. Apel J., A Gröbner approach to involutive bases. *J. Symbolic Comput.* (1996) **11**, 1–16.
23. Apel J., Computational ideal theory in finitely generated extension rings. *Theor. Computer Sci.* (2000) **244**, 1–33.
24. Astrelin A. V., Pankratiev E. V., Groebner bases and involutive bases. *Abstracts IMACS ACA 2000*, St. Petersburg, 66–67.
25. Bachmair L., Ganzinger H., Buchberger's algorithm: A constraint-based completion procedure. *Lect. Notes Comput. Sci.* (1994) **845**, 285–301.
26. Bachmair L., Tiwari A., D-bases for polynomial ideals over commutative noetherian rings. *Lect. Notes Comp. Sci.* (1997) **230**, 5–20.
27. Ballantyne A. M., Lancford D. S., New decision algorithms for finitely presented commutative semi-groups. *Comput. Math. Appl.* (1981) **7**, 159–165.
28. Bayer D., Stillman M., A criterion for detecting m -regularity. *Invent. Math.* (1987) **87**, 1–11.
29. Blinkov Yu. A., Zharkov A. Yu., Involution approach to investigating polynomial systems. *Math. Comp. Simul.* (1996) **42**, 323–332.
30. Becker T., Weispfenning V., *Gröbner bases: a computational approach to commutative algebra*. Springer, Berlin, 1993.
31. Boege W., Gebauer R., Kredel H., Some examples for solving systems of algebraic equations by calculating Groebner bases. *J. Symbolic Comput.* (1986) **5**, 83–98.
32. Buchberger B., *An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal*. Univ. Innsbruck, Ph. D. Thesis, 1965.
33. Buchberger B., A note on the complexity of constructing Groebner bases. *Lect. Notes Comput. Sci.* (1983) **162**, 137–145.
34. Buchberger B., Groebner bases: An algorithmic method in polynomial ideal theory. In: *Recent Trends in Multidimensional System Theory*. Reidel, Dordrecht, 1985, pp. 184–232.
35. Buchberger B., A critical-pair completion algorithm for finitely generated ideals in rings. *Lect. Notes Comp. Sci.* (1984) **171**, 137–161.

36. Byrne E., Fitzpatrick P., Gröbner bases over Galois rings with an application to decoding alternant codes. *J. Symbolic Comput.* (2001) **31**, 565–584.
37. Collart S., Kalkbrener M., Mall D., Converting Bases with the Gröbner walk. *J. Symbolic Comput.* (1997) **24**, 465–469.
38. Dubé T. W., The structure of polynomial ideals and Gröbner bases. *SIAM J. Comput.* (1990) **19**, 750–775.
39. Faugère J. C., Gianni P., Lazard D., Mora T., Efficient change of ordering for Gröbner bases of zero-dimensional ideals. *J. Symbolic Comp.* (1993) **16**, 329–344.
40. Faugère J. C., A new efficient algorithm for computing Gröbner bases *f4*. *J. Pure and Appl. Algebra* (1999) **139**, 61–88.
41. Faugère J. C., *A new efficient algorithm for computing Gröbner bases without reduction to zero f5*. In: *ISSAC 2002*. ACM Press, Paris, 2002.
42. Faugère J. C., Ars J., An algebraic cryptanalysis of nonlinear filter generators using Gröbner bases. INRIA, rapport №4739, 2003.
43. Galligo A., Some algorithmic questions on ideals of differential operators. *Lect. Notes Comput. Sci.* (1985) **204**, 413–421.
44. Gebauer R., Möller H. M., On an installation of Buchberger's algorithm. In: *Computational Aspects of Commutative Algebra*. Academic Press, New York, 1988, pp. 141–152.
45. Gianni P., Mora T., Algebraic solution of systems of polynomial equations using Groebner bases. *Lect. Notes Comput. Sci.* (1989) **356**.
46. Giovini A., Mora T., Niesi G., Robbiano L., Taverso C., "One sugar cube, please," or selection strategies in the Buchberger's algorithm. In: *ISSAC 1991*. ACM Press, New York, 1991, pp. 49–54.
47. Hartley D., Tuckey P., Gröbner bases in Clifford and Grassman algebras. *J. Symbolic Comp.* (1995) **18**, 197–205.
48. Hilbert D., Über die Theorie der algebraischen Formen. *Math. Ann.* (1890) **36**, 473–534.
49. Hironaka H., Resolution of singularities of an algebraic variety over a field of characteristic zero. I, II. *Ann. Math.* (1964) **79**, 109–326.
50. Kalkbrener M., Solving systems of algebraic equations by using Gröbner bases. *Lect. Notes Comput. Sci.* (1987), **378**.
51. Kandri-Rody A., Kapur D., Computing a Gröbner basis of a polynomial ideal over a Euclidean domain. *J. Symbolic Comput.* (1988) **6**, 37–57.
52. Kandri-Rody A., Weispfenning V., Non-commutative Gröbner bases in algebras of solvable type. *J. Symbolic Comput.* (1990) **9**, 1–26.
53. Koblitz N., *Algebraic aspects of cryptography*. Springer, Berlin, 1997.
54. Kobayashi H., Moritsugu S., Hogan R. W., Solving systems of algebraic equations. *Lect. Notes Comput. Sci.* (1989) **358**.
55. Kronecker L., *Vorlesungen über Zahlentheorie*. Bd. I. Teubner, Leipzig, 1901.
56. Krull W., Algebraische Theorie der Ringe. II. *Math. Ann.* (1923) **91**, 1–46.
57. Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A., Linear recurring sequences over rings and modules. *J. Math. Sci.* (1995) **76**, №6, 2793–2915.
58. Landau S., Polynomial time algorithms for Galois groups. *Lect. Notes Comput. Sci.* (1984) **174**, 225–236.
59. Latyshev V. N., An improved version of standard bases. *Proc. 12th Int. Conf. Formal Power Series Algebra Comb.* MSU, 2000, 496–505.

60. Lazard D., Resolution des systemes d'equations algebriques. *Teor. Comp. Sci.* (1981) **15**, 77–110.
61. Lazard D., Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. *Lect. Notes Comput. Sci.* (1983) **162**, 146–156.
62. Miller J. L., Analogs of Gröbner bases in polynomial rings over a ring. *J. Symbolic Comp.* (1996) **21**, 139–153.
63. Möller H. M., Mora F., Upper and lower bounds for the degree of Gröbner bases. *Lect. Notes Comput. Sci.* (1984) **174**, 172–183.
64. Mora T., Seven variations on standard bases. Preprint. Univ. di Genova, Dip. di Matematica, 1988.
65. Norton G. H., Salagean A., Strong Gröbner bases and cyclic codes over a finite-chain ring. *Proc. Int. Workshop on Coding and Cryptography*, Paris, 2001, 391–401.
66. Pan L., On the D -bases of polynomial ideals over principal ideal domains. *J. Symbolic Comput.* (1988) **7**, 55–69.
67. Robbiano L., Term orderings on the polynomial ring. *Lect. Notes Comput. Sci.* (1985) **204**, 513–517.
68. Robbiano L., On the theory of graded structures. *J. Symbolic Comp.* (1986) **5**, 139–170.
69. Stifter S., A generalization of reduction rings. *J. Symbolic Comput.* (1987) **6**, 351–364.
70. Trinks W. L., Über B. Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen. *J. Number Theory* (1978) **10**, 475–488.
71. Winkler F., On the complexity of the Gröbner bases algorithm over $K[x, y, z]$. *Lect. Notes Comput. Sci.* (1984) **174**, 184–194.
72. Zacharias G., *Generalized Gröbner bases in commutative polynomial rings*. Bachelor Thesis. MIT, Boston, 1978.

Статья поступила 20.10.2003.