Асимметричный подход к задаче вычисления базиса Грёбнера*

Е. В. ПАНКРАТЬЕВ, А. С. СЕМЁНОВ
Московский государственный университет им. М. В. Ломоносова

УДК 512.62

Ключевые слова: базисы Грёбнера, инволютивные базисы, существенные умножения, алгоритм нормальной формы.

Аннотация

В статье изложен подход к описанию алгоритма Бухбергера, использующий существенные умножения и немультипликативные продолжения вместо традиционных S-полиномов. В его рамках как алгоритм Бухбергера, так и инволютивный алгоритм Гердта—Блинкова получают описание в общих унифицированных терминах. В основе нового подхода лежит взгляд на формирование S-полинома как на построение немультипликативного продолжения $m \cdot f$ полинома f и его редукции относительно некоторого существенного умножения. Преимуществом данной процедуры является автоматическое исключение из рассмотрения ряда «лишних» S-пар.

Abstract

E. V. Pankratiev, A. S. Semenov, Asymmetric approach to computation of Gröbner bases, Fundamentalnaya i prikladnaya matematika, vol. 12 (2006), no. 3, pp. 73—88.

A new approach to Buchberger's algorithm based on the use of essential multiplications and nonmultiplicative prolongations instead of traditional S-polynomials is described. In the framework of this approach, both Buchberger's algorithm for computing Gröbner bases and Gerdt–Blinkov algorithm for computing involutive bases obtain a unified form of description. The new approach is based on consideration of the process of determining an S-polynomial as a process of constructing a nonmultiplicative prolongation of a polynomial and its subsequent reducing with respect to an essential multiplication. An advantage of the method is that some "redundant" S-pairs are automatically excluded from consideration.

Введение

За последние 40 лет был достигнут значительный прогресс в компьютерной алгебре, одной из приоритетных задач которой является развитие методов решения систем нелинейных алгебраических уравнений от нескольких переменных и изучения полиномиальных идеалов на основе анализа стандартных

*Работа была частично поддержана Российским фондом фундаментальных исследований (проект № 05-01-00671) и грантом Президента России НШ-5006.2006.1.

Фундаментальная и прикладная математика, 2006, том 12, № 3, с. 73—88.

базисов, которые строятся в явном виде. Наиболее распространённой формой стандартных базисов алгебраических идеалов являются базисы Грёбнера, алгоритм вычисления которых был предложен Бухбергером ещё в середине 1960-х годов.

Тем не менее появление алгоритма не решило проблемы, поскольку теоретическая сложность алгоритма вычисления базиса Грёбнера оказалась слишком высокой для его непосредственного применения на практике. Поэтому сразу же после появления алгоритма встал вопрос об оптимизации его работы и дальнейших усовершенствованиях. За сорок лет на данном направлении был достигнут значительный успех, причём существенную роль сыграло более детальное изучение алгоритмов и разработка принципиально новых подходов. Одним из них является инволютивный подход, развитый в работах [2, 7, 11, 12]. Основное отличие инволютивного алгоритма от алгоритма Бухбергера состоит в особом способе вычисления нормальной формы, который ограничивает набор возможных редукций. Этот подход был впервые применён значительно ранее в рамках дифференциальной алгебры.

Отправной концепцией инволютивного подхода является теория инволютивных делений, основанная на разделении переменных на мультипликативные и немультипликативные. Вычислительные эксперименты показали, что в ряде случаев инволютивный алгоритм заканчивает работу быстрее, чем алгоритм Бухбергера. Одной из характерных черт инволютивного алгоритма является неявное использование второго критерия Бухбергера. Данный подход основан на «асимметричном» взгляде на S-полином и его разделении на мультипликативную и немультипликативную части. Поэтому актуальной задачей является перенос подобного подхода на стандартный алгоритм Бухбергера.

В работе поставленная задача решается посредством введения понятия *существенного умножения*, являющегося видоизменением аналогичного термина работы [4], и обобщения формализма, развитого для инволютивных делений в [7, 11, 12]. Представлены достаточные условия корректной работы алгоритма: свойства фильтрации, связности и непрерывности, являющиеся обобщениями классификационных свойств инволютивных делений, введённых в [11, 12].

1. Основные понятия теории базисов Грёбнера

Пусть $\mathbb{K}$ — произвольное поле, $X = \{x_1, \ldots, x_n\}$ — множество независимых переменных, $\mathbb{N}$ — множество натуральных чисел, в которое мы также включаем нуль.

Пусть $\mathbb{M} = \{x_1^{i_1} \ldots x_n^{i_n} \mid i_1, \ldots, i_n \in \mathbb{N}\}$ — моноид мономов от переменных $\{x_1, \ldots, x_n\}$, в котором единица есть моном $1 = x_1^0 \ldots x_n^0$, а ассоциативная операция $\cdot$ определена по правилу

$$x_1^{i_1} \ldots x_n^{i_n} \cdot x_1^{j_1} \ldots x_n^{j_n} = x_1^{i_1+j_1} \ldots x_n^{i_n+j_n}.$$

Пусть $\mathbb{K}[X]$ — кольцо полиномов, по определению являющееся линейным пространством над полем $\mathbb{K}$ с базисом $\mathbb{M}$.

Линейное отношение порядка $<$ на множестве $\mathbb{M}$ называется *допустимым*, если выполнены следующие условия:

1) $\forall u \in \mathbb{M}\ (1 < u)$;
2) $\forall u, v, w \in \mathbb{M}\ (u < v \implies uw < vw)$.

Определение 1. Пусть $<$ — допустимое отношение порядка на моноиде $\mathbb{M}$. Наибольший относительно $<$ моном $u \in \mathbb{M}$, входящий в полином $f \in \mathbb{K}[X]$, называется *старшим мономом* полинома f и обозначается $\mathrm{lm}(f)$. Коэффициент при $\mathrm{lm}(f)$ называется *старшим коэффициентом* полинома f и обозначается $\mathrm{lc}(f)$. Старший член $\mathrm{lc}(f)\,\mathrm{lm}(f)$ обозначается $\mathrm{lt}(f)$. Обозначим результат деления f на его старший коэффициент через f^0.

Греческими буквами будут обозначаться мультистепени, т. е. $x^\gamma = x_1^{\gamma_1} \dots x_n^{\gamma_n}$.

Моном $\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))$, где lcm — наименьшее общее кратное, обозначается $\mathrm{lcm}(f, g)$.

Основной операцией в теории стандартных базисов является полиномиальная редукция.

Определение 2. Пусть полином f содержит член $a_\gamma x^\gamma$, делящийся на старший моном $\mathrm{lm}(g)$ полинома g. Операция перехода от f к полиному

$$f' = f - \frac{a_\gamma x^\gamma}{\mathrm{lm}(g)} g^0$$

называется редукцией полинома f по g, а g называется редуцирующим полиномом.

Приведением к нормальной форме полинома f по полиномиальному множеству G называется процесс, который работает по следующей схеме и является обобщением полиномиального деления в случае одной переменной.

Схема приведения к нормальной форме

вход: полином f и полиномиальное множество G
выход: полином $h = \mathrm{NF}(f, G)$
  $h := f$
  пока $h \neq 0$ **и** h содержит член $a_\gamma x^\gamma$, такой что $\exists g \in G\ (\mathrm{lm}(g) \mid x^\gamma)$
    найти максимальный относительно $<$ член $a_\gamma x^\gamma$ в h
      и $g \in G$, такой что $\mathrm{lm}(g) \mid x^\gamma$
    $h := h - \frac{a_\gamma x^\gamma}{\mathrm{lm}(g)} g^0$
  конец
  вернуть h
конец

Если h — нормальная форма полинома f по множеству G, будем использовать обозначение $h = \mathrm{NF}(f, G)$. Следует отметить, что данный процесс не полностью определяет алгоритм, поскольку в случае, если h содержит член $a_\gamma x^\gamma$, делящийся на несколько мономов $\mathrm{lm}(g_i)$, $g_i \in G$, существует возможность выбора одного

делителя из нескольких. Тем не менее данный процесс оканчивает работу за конечное время.

Если полином f не содержит членов $a_\gamma x^\gamma$, делящихся на $\mathrm{lm}(g)$ ни для какого $g \in G$, то полином f нередуцируем по G.

Определение 3. Если полином f может быть представлен в виде суммы

$$f = h_1 g_1 + \ldots + h_s g_s, \tag{1}$$

где h_i — полиномы, g_i — полиномы из множества G и выполнено $\mathrm{lm}(f) \geqslant \geqslant \mathrm{lm}(h_i g_i)$, то говорится, что f эквивалентен 0 по модулю G, и используется обозначение

$$f \equiv 0 \,(\mathrm{mod}\ G).$$

Представление (1) называется G-представлением.

Выражение $f - g \equiv 0 \,(\mathrm{mod}\ G)$ записывается как $f \equiv g \,(\mathrm{mod}\ G)$. Введённое таким образом отношение $\equiv$ является рефлексивным, симметричным и транзитивным, следовательно, это отношение эквивалентности.

Далее будут приведены четыре эквивалентных определения базиса Грёбнера.

Определение 4. Пусть $f = \mathrm{lc}(f)\,\mathrm{lm}(f) + \ldots$, $g = \mathrm{lc}(g)\,\mathrm{lm}(g) + \ldots$ — два полинома. Тогда S-полиномом пары (f, g) называется полином

$$S(f,g) = \mathrm{lc}(g)\frac{\mathrm{lcm}(f,g)}{\mathrm{lm}(f)}f - \mathrm{lc}(f)\frac{\mathrm{lcm}(f,g)}{\mathrm{lm}(g)}g.$$

Определение 5. Пусть задано мономиальное упорядочение. Конечное множество $G = \{g_1, \ldots, g_s\}$ элементов идеала I называется его базисом Грёбнера, если выполнено одно из следующих условий:

- $\forall g \in I \ \ \mathrm{NF}(g, G) = 0$;
- $\forall f, g \in G \ \ \mathrm{NF}(S(f,g), G) = 0$;
- $\forall g \in I \ \ g \equiv 0 \,(\mathrm{mod}\ G)$;
- $\forall f, g \in G \ \ S(f,g) \equiv 0 \,(\mathrm{mod}\ G)$.

Доказательство эквивалентности этих условий можно найти в [3, 5]. Менее формально, множество $G = \{g_1, \ldots, g_s\} \subset I$ называется базисом Грёбнера, если старший член любого элемента из I делится хотя бы на один из старших членов $\mathrm{lm}(g)$, $g \in G$. Базовым результатом компьютерной алгебры является доказательство существования базиса Грёбнера для любого идеала I (см. [3]).

Для конструктивного построения базиса Грёбнера используется алгоритм Бухбергера. Далее он будет сформулирован в том виде, в котором он приведён в [3]. Для оптимизации используются два критерия Бухбергера, позволяющие исключать из рассмотрения S-полиномы, заведомо сравнимые с 0 по модулю G. В алгоритме полиномы в G нумеруются и пары различных полиномов f_i, f_j обозначены (i, j), $i < j$. В списке B находятся те пары, для которых соответствующие им S-полиномы должны быть вычислены и отредуцированы в ходе алгоритма.

Первый критерий Бухбергера состоит в том, что если $\operatorname{lcm}(f,g) = \operatorname{lm}(f)\operatorname{lm}(g)$, то такая пара может быть исключена из рассмотрения, так как она сравнима с 0 по модулю G.

Второй критерий Бухбергера выполнен, если истинна логическая функция $\operatorname{Criterion}(f_i, f_j, B)$. Для её определения вводится новое обозначение для пар:

$$[i,j] = \begin{cases} (i,j), & i < j, \\ (j,i), & j < i. \end{cases}$$

Логическая функция $\operatorname{Criterion}(f_i, f_j, B)$ истинна, если найдётся $l \notin \{i,j\}$, для которого $[i,l]$, $[j,l]$ не принадлежат B и $\operatorname{lm}(f_l) \mid \operatorname{lcm}(f_i, f_j)$.

Схема алгоритма Бухбергера

вход: конечное множество полиномов F
выход: базис Грёбнера G идеала $I = \operatorname{Id}(F)$
  $(f_1, \ldots, f_s) := $ **Авторедукция**(F)
  $G := (f_1, \ldots, f_s)$
  $B := \{(i,j) \mid 1 \leqslant i < j \leqslant s\}$
  $t := s$
  пока $B \neq \varnothing$
    выбрать $(i,j) \in B$
    если $\operatorname{lcm}(f_i, f_j) \neq \operatorname{lm}(f_i)\operatorname{lm}(f_j)$ **и** $\neg\operatorname{Criterion}(f_i, f_j, B)$, **то**
      $S := \operatorname{NF}(S(f_i, f_j), G)$
      если $S \neq 0$, **то**
        $t := t + 1$
        $f_t := S$
        $G = G \cup \{f_t\}$
        $B := B \cup \{(i,t) \mid 1 \leqslant i \leqslant t-1\}$
    $B := B - \{(i,j)\}$
  конец
  вернуть G
конец

В данном алгоритме остаётся неопределённым правило выбора текущей пары $(i,j) \in B$. Правило, согласно которому выбирается пара с наименьшим возможным $\operatorname{lcm}(f_i, f_j)$ относительно некоторого допустимого порядка $\sqsubset$ (не обязательно совпадающего с мономиальным упорядочением $<$), называется *нормальной стратегией*.

2. Существенные умножения

Для приведённого выше изложения основ теории базисов Грёбнера характерны «симметричная» форма (поскольку в S-полином $S(f_i, f_j)$ полиномы f_i и f_j входят равноправно) и неопределённость в выборе последовательности

редукций при приведении полинома к нормальной форме. В действительности любая система компьютерной алгебры при вычислении базисов Грёбнера использует только одно заданное G-представление или однозначно определённый процесс редукции (алгоритм нормальной формы). Данное замечание играет определяющую роль, поскольку приведение к нормальной форме не является однозначно определённым процессом и для превращения его в алгоритм нужны дополнительные параметры. Неоднозначность может быть продемонстрирована следующим примером

Пример 1 ([3]). Пусть $f = xy^2 - x$, $G = \{xy + 1, y^2 - 1\}$, а порядок $<$ представляет собой lex ($y < x$). Рассмотрим $\mathrm{NF}(f, G)$. Если в процессе приведения к нормальной форме f редуцируется по $xy + 1$, то $\mathrm{NF}(f, G) = -x - y$. Если же редукция идёт по $y^2 - 1$, то $\mathrm{NF}(f, G) = 0$.

Таким образом, для задания алгоритма нормальной формы требуется чёткое указание, по какому полиному $h \in G$ нужно редуцировать f, если таких возможностей несколько. Следовательно, процесс приведения к нормальной форме должен включать алгоритм выбора одного полинома h из всех возможных. Если все старшие мономы множества G различны, то алгоритм нормальной формы может быть явно определён следующим образом.

Алгоритм нормальной формы

вход: полином f и полиномиальное множество G
выход: полином $h = \mathrm{NF}(f, G)$
  $h := f$
  пока $h \neq 0$ **и** h содержит член $a_\gamma x^\gamma$, такой что $\exists g \in G\ (\mathrm{lm}(g) \mid x^\gamma)$
    найти максимальный относительно $<$ член $a_\gamma x^\gamma$ в h
      и $g \in G$, такой что $\mathrm{lm}(g) \mid x^\gamma$
    $u := \mathrm{ChooseDivisor}(x^\gamma, \mathrm{lm}(G))$
    найти $g \in G$, такой что $\mathrm{lm}(g) = u$
    $h := h - \frac{a_\gamma x^\gamma}{\mathrm{lm}(g)} g^0$
  конец
  вернуть h
конец

В приведённом алгоритме используется функция $\mathrm{ChooseDivisor}(m, U)$, где m — моном, а U — мономиальное множество. Её результатом является моном $u \in U$, $u \mid m$, или пустое множество, если такого монома в U не существует. Простейшим вариантом функции $\mathrm{ChooseDivisor}(m, U)$ является выбор первого элемента u, делящего m, в упорядоченном списке U.

Другим способом задания функции $\mathrm{ChooseDivisor}(m, U)$ являются существенные умножения [4].

Определение 6. Говорят, что задано существенное умножение E, если для любого множества попарно различных мономов U и каждого монома $u \in U$

определено подмножество $E(u,U)$ моноида $\mathbb{M}$ и подмножества $E(u,U)$ удовлетворяют следующей аксиоме:

$$uE(u,U) \cap vE(v,U) = \varnothing, \quad u,v \in U.$$

Элементы $E(u,U)$ называются *мультипликативными* для u. Если $w \in uE(u,U)$, то используется обозначение $u \mid_E w$ и u называется *E-делителем* или *существенным делителем* w, а w — *E-кратным* или *существенным кратным* u. Моном $v = w/u$ называется *E-мультипликативным* для u, и равенство $w = uv$ записывается как $w = u \times v$. Если u — обычный делитель w, но не E-делитель, равенство записывается как $w = u \cdot v$. В этом случае моном v называется *немультипликативным* для u.

Определение 7. Пусть E — существенное умножение, а U — произвольное конечное множество мономов. Пусть $u \in U$, $w \notin E(u,U)$. Тогда моном w называется минимальным немультипликативным мономом, если для каждого $v \mid w$ выполнено $v \in E(u,U)$. Множество минимальных немультипликативных мономов обозначается $\mathrm{NM}_E(u,U)$.

Одним из способов описания существенных умножений является задание множеств мономов $\mathrm{NM}_E(u,U)$ для всех u и U таким образом, что множества существенных кратных $E(u,U) = \mathbb{M} \setminus \mathrm{NM}_E(u,U)\mathbb{M}$ удовлетворяют определению существенных умножений. Если множество минимальных немультипликативных мономов $\mathrm{NM}_E(u,U)$ для всех u и U состоит из переменных (мономов первой степени), то такое существенное умножение является инволютивным делением в смысле работ [7, 11, 12], а переменные, входящие в множества $\mathrm{NM}_E(u,U)$, называются немультипликативными.

Замечание 1. Описанный выше формализм для существенных умножений является обобщением формализма, введённого Гердтом и Блинковым [11, 12] для инволютивных делений.

Далее будут приведены различные примеры существенных умножений, в том числе инволютивных делений.

Пример 2 (существенное $\succ$-умножение). Пусть дано конечное множество мономов U и произвольный моном m. Тогда $u \mid_\succ m$, если $u \mid m$ и $u = \max_\succ\{v \in U,\ v \mid m\}$.

Каждое допустимое мономиальное упорядочение $\succ$ определяет существенное умножение.

Пример 3 (инволютивное $\succ$-деление). Пусть дано конечное множество мономов U. Для монома $u \in U$ переменная x_i $(1 \leqslant i \leqslant n)$ немультипликативна для u, если существует $u_1 \in U$, $u_1 \succ u$, $i = \min\{j \mid \deg_j(u) < \deg_j(u_1)\}$.

Пример 4 (инволютивное деление Жане). Рассмотрим конечное множество мономов U. Для любого $1 \leqslant i \leqslant n$ множество U можно разделить на подмножества, маркируемые неотрицательными целыми $d_1, \ldots, d_i$:

$$[d_1, \ldots, d_i] = \{u \in U \mid d_j = \deg_j(u),\ 1 \leqslant j \leqslant i\}.$$

Переменная x_i немультипликативна для $u \in U$, если $i = 1$ и найдётся $v \in U$, для которого $\deg_1(u) < \deg_1(v)$, или если $i > 1$, $u \in [d_1, \ldots, d_{i-1}]$ и найдётся $v \in [d_1, \ldots, d_{i-1}]$, для которого $\deg_i(u) < \deg_i(v)$.

В [6] доказано, что деление Жане представляет собой инволютивное lex-деление, где lex — такой лексикографический порядок переменных, что $x_1 >_{\text{lex}} x_2 >_{\text{lex}} \ldots >_{\text{lex}} x_n$.

Пример 5 (аналог умножения Жане [13]). Рассмотрим конечное множество мономов U. Для любого $1 \leqslant i \leqslant n$ множество U можно разделить на подмножества, маркируемые неотрицательными целыми $d_1, \ldots, d_i$:

$$[d_1, \ldots, d_i] = \{u \in U \mid d_j = \deg_j(u),\ 1 \leqslant j \leqslant i\}.$$

Моном x_i^k является минимальным немультипликативным для $u \in U$, если

$$i = 1, \quad k = \min\{\deg_1(v) - \deg_1(u) \mid v \in U,\ \deg_1(u) < \deg_1(v)\}$$

или если

$$i > 1, \quad u \in [d_1, \ldots, d_{i-1}],$$
$$k = \min\{\deg_i(v) - \deg_i(u) \mid v \in [d_1, \ldots, d_{i-1}],\ \deg_i(u) < \deg_i(v)\}.$$

При наличии существенного умножения E функцию $\text{ChooseDivisor}(m, U)$ можно определить следующим образом:

$$\text{ChooseDivisor}(m, U) = \left[\begin{array}{ll} u, & \exists u \in U\ (u \mid_E m), \\ \varnothing, & \nexists u \in U\ (u \mid_E m). \end{array} \right.$$

С её помощью можно определить алгоритм E-нормальной формы.

Алгоритм E-нормальной формы

вход: полином f и полиномиальное множество G
выход: полином $h = \text{NF}_E(f, G)$
  $h := f$
  пока $h \neq 0$ **и** h содержит член $a_\gamma x^\gamma$, такой что $\exists g \in G\ (\text{lm}(g) \mid x^\gamma)$
    найти максимальный относительно $<$ член $a_\gamma x^\gamma$ в h
      и $g \in G$, такой что $\text{lm}(g) \mid x^\gamma$
    $u := \text{ChooseDivisor}(x^\gamma, \text{lm}(G))$
    найти $g \in G$, такой что $\text{lm}(g) = u$
    $h := h - \frac{a_\gamma x^\gamma}{\text{lm}(g)} g^0$
  конец
  вернуть h
конец

Данный алгоритм E-нормальной формы будет алгоритмом нормальной формы лишь в том случае, если

$$\forall U\ \forall m\ \exists u \in U\ (u \mid m) \implies \exists u_1 \in U\ (u_1 \mid_E m).$$

Данное свойство всегда выполнено для существенных $\succ$-умножений, а для инволютивных делений и аналогов умножения Жане может не выполняться на некоторых U. Таким образом, $\succ$-нормальная форма всегда является нормальной формой, а инволютивная нормальная форма может и не являться ею.

Понятие существенного умножения появляется естественным образом при проведении параллелей между теорией полиномиальных идеалов и линейной алгеброй.

Очевидно, что $\mathbb{M}$ образует базис $\mathbb{K}[X]$ как векторного пространства над $\mathbb{K}$, т. е. любой полином $p \in \mathbb{K}[X]$ можно представить в виде конечной линейной комбинации мономов с ненулевыми коэффициентами из поля $\mathbb{K}$ и такое представление *единственно*.

Если I — идеал кольца полиномов $\mathbb{K}[X]$, порождённый конечным числом мономов, то множество $\mathbb{M}$ разбивается на два подмножества: $\mathrm{lm}(I)$ — множество мономов, принадлежащих идеалу I, и $\mathbb{M} \setminus \mathrm{lm}(I)$ — множество мономов, не принадлежащих I. Как векторное пространство $\mathbb{K}[X]$ разлагается в прямую сумму пространств, порождённых множествами $\mathrm{lm}(I)$ и $\mathbb{M} \setminus \mathrm{lm}(I)$; при этом пространство, порождённое $\mathrm{lm}(I)$, совпадает с идеалом I.

В общем случае полиномиального идеала для разделения множество мономов на два подмножества можно использовать допустимое упорядочение мономов $\prec$. Чтобы построить базис идеала I как векторного пространства, достаточно каждому моному $m \in \mathrm{lm}(I)$ поставить в соответствие некий (единственный!) полином $g \in I$ со старшим мономом $\mathrm{lm}(g) = m$. Пусть $G = \{g_1, \ldots, g_s\}$ — базис Грёбнера идеала I, такой что $\mathrm{lm}(g_1) \succ \mathrm{lm}(g_2) \succ \ldots \succ \mathrm{lm}(g_s)$. Базис идеала I как векторного пространства можно построить следующим образом. Рассмотрим множество полиномов $P_1 = \{mg_1\}$, где m пробегает множество всех мономов X. Затем построим множество полиномов $P_2 = \{mg_2\}$, где m пробегает множество всех мономов, удовлетворяющих условию $\mathrm{lm}(mg_2) \notin \mathrm{lm}(P_1)$. Продолжим этот процесс по индукции, т. е. множество P_k $(2 \leqslant k \leqslant s)$ — это множество полиномов вида $\{mg_k\}$, где m пробегает множество всех мономов, удовлетворяющих условию

$$\mathrm{lm}(mg_k) \notin \mathrm{lm}(P_1) \cup \ldots \cup \mathrm{lm}(P_{k-1}).$$

Множество $P_1 \cup \ldots \cup P_s$ является базисом идеала I, рассматриваемого как векторное пространство. Это множество можно использовать для построения алгоритма нормальной формы. Многочлен f принадлежит идеалу I тогда и только тогда, когда он *линейно редуцируется* к нулю по множеству $P_1 \cup \ldots \cup P_s$. Строгое обоснование этого факта вытекает из того, то G — базис Грёбнера.

Введённое понятие существенного $\succ$-умножения является не чем иным, как формализацией вышеописанного подхода. Действительно, множества P_k — это множества полиномов вида $\{m \times g_k\}$, где m пробегает множество всех мономов $E(\mathrm{lm}(g_k), \mathrm{lm}(G))$, а E — существенное $\succ$-умножение на множестве $\mathrm{lm}(G)$. Линейная нормальная форма произвольного полинома по построенному линейному базису I эквивалентна нормальной форме по G относительно E.

3. Асимметричный подход в алгоритме вычисления базиса Грёбнера

Введённая концепция существенных умножений позволяет исключить из рассмотрения в ходе выполнения алгоритма Бухбергера ряд S-пар, заведомо редуцируемых к 0 на основе второго критерия Бухбергера. Данный подход базируется на использовании минимальных немультипликативных продолжений полиномов. Для доказательства корректности исключения из рассмотрения ряда S-полиномов используются такие свойства существенных умножений, как связность, фильтрация и непрерывность.

Определение 8. Пусть E — существенное умножение, $g \in G$ — полином, а w — минимальный немультипликативный моном для $\mathrm{lm}(g)$ относительно E. Тогда произведение $g \cdot w$ называется минимальным немультипликативным продолжением g.

Определение 9. Говорят, что существенное умножение E удовлетворяет *свойству связности*, если

$$w \in E(u, U),\ v \mid w \implies v \in E(u, U).$$

Нетрудно показать, что существенное $\succ$-умножение удовлетворяет данному свойству.

Теорема 1. *Если E — существенное $\succ$-умножение и $g \cdot w$ — минимальное немультипликативное продолжение g, то существует полином h, такой что*

$$\mathrm{lm}(g \cdot w) = \mathrm{lm}(h \times v) = \mathrm{lcm}(g, h).$$

Таким образом, минимальному немультипликативному продолжению g соответствует S-полином.

Доказательство. Пусть для каких-то g, h это неверно, т. е.

$$\mathrm{lm}(g \cdot w) = \mathrm{lm}(h \times v) = \mathrm{lcm}(g, h)m,$$

где $m \neq 1$. Тогда w/m мультипликативен для $\mathrm{lm}(g)$ по минимальности, а v/m мультипликативен для h по свойству связности. Следовательно, моном $\mathrm{lcm}(g, h)$ имеет два существенных кратных, что невозможно. □

Таким образом, процесс формирования и последующей редукции S-полинома, описанного теоремой 1, может быть интерпретирован как домножение полинома на минимальный немультипликативный моном, а затем его редукция с учётом деления E. Таким образом, построение S-полинома и его приведение к E-нормальной форме заменяется единообразным построением E-нормальной формы минимального немультипликативного продолжения полинома g, или $\mathrm{NF}_E(g \cdot w, G)$.

Алгоритм, в котором строятся лишь S-полиномы описанного типа, выглядит следующим образом.

Алгоритм $\mathbf{GB}_E$

вход: конечное множество полиномов F, допустимый порядок $\sqsubset$
выход: базис Грёбнера G идеала $I = \mathrm{Id}(F)$
  $(f_1, \ldots, f_s) := $ **Авторедукция**(F)
  $G := (f_1, \ldots, f_s)$
  $T := 0$
  для каждого $g \in G$ $\;T := T \cup \{(g, \varnothing)\}$
  пока существуют $(g, P) \in T$ и $w \in \mathrm{NM}_E(\mathrm{lm}(g), \mathrm{lm}(G)) \setminus P$
    выбрать (g, P), w с наименьшим $\mathrm{lm}(g) \cdot w$ относительно $\sqsubset$
    $T := T \setminus \{(g, P)\} \cup \{(g, P \bigcup \{w\})\}$
    $h := \mathrm{NF}_E(g \cdot w, G)$
    если $h \neq 0$, **то** $G := G \cup \{h\}$
      $T := T \cup \{(h, \varnothing)\}$
  конец
  вернуть G
конец

Несмотря на формулировку, сходную с инволютивным алгоритмом Гердта—Блинкова [11, 12], алгоритм с использованием существенных $\succ$-умножений представляет собой вариант классического алгоритма Бухбергера, поскольку в ходе этого алгоритма рассматривается часть S-полиномов и алгоритм E-нормальной формы даёт нормальную форму (в инволютивном алгоритме это не всегда выполнено).

Определение 10. Для существенного умножения выполнено *свойство фильтрации*, если

$$U \subseteq V,\ u \in U, V \implies E(u, U) \supseteq E(u, V).$$

Свойство фильтрации играет важную роль в алгоритме, поскольку благодаря ему не возникает ситуации, когда минимальный немультипликативный моном вновь становится мультипликативным после добавления очередного элемента в множество G и требуется исключать из G некоторые уже рассмотренные немультипликативные продолжения. Нетрудно проверить, что для любого допустимого упорядочения $\succ$ свойство фильтрации для существенного $\succ$-умножения будет выполнено.

Для обоснования корректности данного алгоритма нужно доказать, что время его работы конечно и что для вычисления базиса Грёбнера достаточно строить S-полиномы, соответствующие минимальным немультипликативным продолжениям. Конечность времени работы алгоритма для существенных $\succ$-умножений вытекает из того, в его процессе строится лишь часть из всех S-полиномов, которые возникают при выполнении классического алгоритма Бухбергера для тех же существенных умножений. Конечность последнего доказывается посредством леммы Диксона.

Для доказательства достаточности построения S-полиномов лишь указанного в теореме 1 типа используется свойство непрерывности. Данный термин

был введён в [11] для инволютивных делений. В [7] для инволютивных делений было введено аналогичное непрерывности, но не тождественное ему понятие допустимости.

Определение 11 ([11,12]). Пусть задано множество мономов U и существенное умножение E. Если для любой конечной последовательности мономов $\{u_i\}$ $(1 \leqslant i \leqslant k)$ из U, такой что для любого $i < k$ найдётся $w_i \in \mathrm{NM}_E(u_i, U)$, для которого $[u_{i+1} \mid_E u_i \cdot w_i]$, выполнено неравенство $u_j \neq u_i$ для любых $i \neq j$, то E является *непрерывным*.

Доказательство непрерывности существенного $\succ$-умножения следует из факта, что $u_{i+1} \succ u_i$.

Теорема 2. *Пусть E — существенное $\succ$-умножение, а G — такое множество полиномов, что для полиномов $S(f_i, f_j)$ $(f_i, f_j \in G)$, удовлетворяющих свойствам*

1) $\mathrm{lcm}(f_i, f_j) = \mathrm{lm}(f_i) \cdot \frac{\mathrm{lcm}(f_i,f_j)}{\mathrm{lm}(f_i)} = \mathrm{lm}(f_j) \times \frac{\mathrm{lcm}(f_i,f_j)}{\mathrm{lm}(f_j)}$,
2) $\frac{\mathrm{lcm}(f_i,f_j)}{\mathrm{lm}(f_i)}$ *— минимальный немультипликативный моном для* $\mathrm{lm}(f_i)$ *в* $E(\mathrm{lm}(f_i), \mathrm{lm}(G))$,

выполнено $S(f_i, f_j) \equiv 0 \pmod G$. Тогда G — базис Грёбнера идеала $\mathrm{Id}(G)$.

Доказательство. Для доказательства данной теоремы достаточно показать, что для любых $f_i, f_g \in G$ справедливо $S(f_i, f_j) \equiv 0 \pmod G$.

Все S-полиномы $S(p, q)$, $p, q \in G$, разбиваются на два типа:

$$\{\cdot,\cdot\}\colon \quad \mathrm{lcm}(p,q) = \mathrm{lm}(p) \cdot \frac{\mathrm{lcm}(p,q)}{\mathrm{lm}(p)} = \mathrm{lm}(q) \cdot \frac{\mathrm{lcm}(p,q)}{\mathrm{lm}(q)},$$
$$\{\cdot,\times\}\colon \quad \mathrm{lcm}(p,q) = \mathrm{lm}(p) \cdot \frac{\mathrm{lcm}(p,q)}{\mathrm{lm}(p)} = \mathrm{lm}(q) \times \frac{\mathrm{lcm}(p,q)}{\mathrm{lm}(q)}.$$

Пусть f_i, f_j образуют S-полином типа $\{\cdot,\cdot\}$. По определению существенного умножения E найдётся f_k, такой что $f_i \neq f_k \neq f_j$ и $\mathrm{lm}(f_k) \mid_E \mathrm{lcm}(f_i, f_j)$. Тогда

$$\mathrm{lcm}(f_k, f_i) \mid \mathrm{lcm}(f_i, f_j), \quad \mathrm{lcm}(f_k, f_j) \mid \mathrm{lcm}(f_i, f_j).$$

Если $S(f_i, f_k) \equiv 0 \pmod G$ и $S(f_j, f_k) \equiv 0 \pmod G$, то по аддитивности отношения сравнения $S(f_i, f_j) \equiv 0 \pmod G$.

Следовательно, задача сводится к доказательству того, что любой S-полином типа $\{\cdot,\times\}$ сравним с 0 по модулю G.

Пусть $S(g_1, h)$ — такая пара, что $\frac{\mathrm{lcm}(g_1,h)}{\mathrm{lm}(g_1)}$ не минимальный немультипликативный моном для $\mathrm{lm}(g_1)$ в $E(\mathrm{lm}(g_1), \mathrm{lm}(G))$ и $\frac{\mathrm{lcm}(g_1,h)}{\mathrm{lm}(h)}$ — мультипликативный моном для $\mathrm{lm}(h)$ в $E(\mathrm{lm}(h), \mathrm{lm}(G))$.

Пусть u_1 — минимальный немультипликативный моном для $\mathrm{lm}(g_1)$, делящий $\frac{\mathrm{lcm}(g_1,h)}{\mathrm{lm}(g_1)}$ в обычном смысле. Согласно доказанной ранее теореме, существует полином $g_2 \in G$, такой что $u_1 = \frac{\mathrm{lcm}(g_1,g_2)}{\mathrm{lm}(g_1)}$ и $\frac{\mathrm{lcm}(g_1,g_2)}{\mathrm{lm}(g_2)} \in E(\mathrm{lm}(g_2), G)$. По условию теоремы $S(g_1, g_2) \equiv 0 \pmod G$ и $\mathrm{lcm}(g_1, g_2) \mid \mathrm{lcm}(g_1, h)$.

Для доказательства теоремы нужно показать, что $S(g_2, h) \equiv 0 \pmod G$, и воспользоваться аддитивностью отношения $\equiv$. Заметим, что по связности деления получаем $\mathrm{lm}(h) \mid_E \mathrm{lcm}(g_2, h)$, поскольку $\mathrm{lcm}(g_2, h) \mid \mathrm{lcm}(g_1, h)$. То, что $S(g_2, h) \equiv 0 \pmod G$, доказывается нахождением минимального немультипликативного монома u_2 для $\mathrm{lm}(g_2)$, делящего $\frac{\mathrm{lcm}(g_2,h)}{\mathrm{lm}(g_2)}$ в обычном смысле, и полинома $g_3 \in G$, такого что $u_2 = \frac{\mathrm{lcm}(g_2,g_3)}{\mathrm{lm}(g_2)}$, что повторяет предыдущий шаг доказательства.

Окончание процесса гарантируется непрерывностью существенного умножения, поскольку

$$\mathrm{lm}(g_i) \cdot \frac{\mathrm{lcm}(g_i, g_{i+1})}{\mathrm{lm}(g_i)} = \mathrm{lm}(g_{i+1}) \times \frac{\mathrm{lcm}(g_i, g_{i+1})}{\mathrm{lm}(g_{i+1})}. \qquad \square$$

Приведённый алгоритм также допускает первый и второй критерии Бухбергера (в модифицированной форме). В данной работе изучение этого вопроса будет опущено, чтобы преимущества несимметричного подхода были видны в «чистом виде».

Замечание 2. В полученном алгоритме используются три различных допустимых мономиальных упорядочения: порядок $<$ на мономах в каждом полиноме, с помощью которого определяются старшие члены, порядок $\prec$, задающий существенное умножение, и стратегия выбора главного элемента $\sqsubset$.

Далее работа алгоритма будет проиллюстрирована на численном примере.

Полиномы

$$f_1 = x^3yz - xz^2, \quad f_2 = x^2y^2 - z^2, \quad f_3 = xy^2z - xyz$$

не образуют базиса Грёбнера идеала $I = (f_1, f_2, f_3)$ относительно мономиального порядка degrevlex с исходной нумерацией переменных x, y, z. Рассмотрим идеал $I = \mathrm{Id}(F) = \mathrm{Id}(f_1, f_2, f_3)$ и введём существенное lex-умножение E для порядка переменных x, y, z. В таблице ниже представлен результат последовательного выполнения алгоритма Бухбергера в приведённой выше формулировке. В качестве стратегии выбора главного элемента берётся нормальная стратегия относительно мономиального упорядочения lex для порядка переменных x, y, z.

Для выделения уже использованных мультипликативных продолжений используется символ зачёркивания.

В данном примере возникла ситуация, когда рассматриваемое множество полиномов перестало быть авторедуцированным по лидирующим мономам, так как $\mathrm{lm}(f_4) \mid \mathrm{lm}(f_1)$. При вычислении базисов Грёбнера в такой ситуации обычно полином f_1 редуцируют относительно f_4, а сам полином f_1 из дальнейшего рассмотрения выбрасывают.

Приведённый выше алгоритм решает проблему по-другому, а именно та же самая редукция в алгоритме рассматривается как редукция полинома xf_4 относительно f_1 и оба полинома f_1 и f_4 остаются в строящемся базисе. При подобном подходе мы проигрываем в количестве элементов базиса, но выигрываем в размере коэффициентов, поскольку часто полиномы, полученные позднее по ходу

Редукция продолжений	$\mathrm{NM}_i = \mathrm{NM}_E(\mathrm{lm}(f_i), \mathrm{lm}(F))$
$f_1 = x^3yz - xz^2$ $f_2 = x^2y^2 - z^2$ $f_3 = xy^2z - xyz$	$\mathrm{NM}_1 = \varnothing$, $\mathrm{NM}_2 = \{xz\}$, $\mathrm{NM}_3 = \{x\}$
$f_3 \cdot x \to f_4 = x^2yz - z^3$	$\mathrm{NM}_1 = \varnothing$, $\mathrm{NM}_2 = \{xz\}$, $\mathrm{NM}_4 = \{x, y\}$, $\mathrm{NM}_3 = \{\not x\}$
$f_4 \cdot y \to f_5 = yz^3 - z^3$	$\mathrm{NM}_1 = \varnothing$, $\mathrm{NM}_2 = \{xz\}$, $\mathrm{NM}_4 = \{x, \not y\}$, $\mathrm{NM}_3 = \{\not x\}$, $\mathrm{NM}_5 = \{xy, x^2\}$
$f_5 \cdot xy \to 0$	—
$f_5 \cdot x^2 \to f_6 = x^2z^3 - z^5$	$\mathrm{NM}_1 = \varnothing$, $\mathrm{NM}_2 = \{xz\}$, $\mathrm{NM}_4 = \{x, \not y\}$, $\mathrm{NM}_6 = \{y\}$, $\mathrm{NM}_3 = \{\not x\}$, $\mathrm{NM}_5 = \{\not x\not y, \not x^2\}$
$f_6 \cdot y \to 0$	—
$f_4 \cdot x \to f_7 = xz^3 - xz^2$	$\mathrm{NM}_1 = \varnothing$, $\mathrm{NM}_2 = \{xz\}$, $\mathrm{NM}_4 = \{\not x, \not y\}$, $\mathrm{NM}_6 = \{\not y\}$, $\mathrm{NM}_3 = \{\not x\}$, $\mathrm{NM}_7 = \{x, y^2\}$, $\mathrm{NM}_5 = \{x, \not x\not y, \not x^2\}$
$f_5 \cdot x \to f_8 = xyz^2 - xz^2$	$\mathrm{NM}_1 = \varnothing$, $\mathrm{NM}_2 = \{xz\}$, $\mathrm{NM}_4 = \{\not x, \not y\}$, $\mathrm{NM}_6 = \{\not y\}$, $\mathrm{NM}_3 = \{\not x\}$, $\mathrm{NM}_8 = \{x, y\}$, $\mathrm{NM}_7 = \{x, y\}$, $\mathrm{NM}_5 = \{\not x, \not x\not y, \not x^2\}$
$f_7 \cdot y \to 0$	—
$f_8 \cdot y \to 0$	—
$f_7 \cdot x \to f_9 = z^5 - x^2z^2$	$\mathrm{NM}_1 = \varnothing$, $\mathrm{NM}_2 = \{xz\}$, $\mathrm{NM}_4 = \{\not x, \not y\}$, $\mathrm{NM}_6 = \{\not y\}$, $\mathrm{NM}_3 = \{\not x\}$, $\mathrm{NM}_8 = \{x, \not y\}$, $\mathrm{NM}_7 = \{\not x, \not y\}$, $\mathrm{NM}_5 = \{\not x, \not x\not y, \not x^2\}$, $\mathrm{NM}_9 = \{x, y\}$
$f_9 \cdot y \to f_{10} = x^2z^2 - z^4$	$\mathrm{NM}_1 = \varnothing$, $\mathrm{NM}_2 = \{xz\}$, $\mathrm{NM}_4 = \{\not x, \not y\}$, $\mathrm{NM}_6 = \{\not y\}$, $\mathrm{NM}_{10} = \{y, z\}$, $\mathrm{NM}_3 = \{\not x\}$, $\mathrm{NM}_8 = \{x, \not y\}$, $\mathrm{NM}_7 = \{\not x, \not y\}$, $\mathrm{NM}_5 = \{\not x, \not x\not y, \not x^2\}$, $\mathrm{NM}_9 = \{x, \not y\}$
$f_9 \cdot x \to 0$	—
$f_{10} \cdot z \to 0$	—
$f_{10} \cdot y \to 0$	—
$f_8 \cdot x \to 0$	—
$f_2 \cdot xz \to 0$	—

алгоритма, имеют более длинные (по занимаемому объёму памяти) коэффициенты, чем полиномы, появлявшиеся в алгоритме ранее в случае рациональной арифметики. Сохраняя полиномы, полученные на более ранних этапах вычислений и используя их в процессе редукций, мы «замедляем» рост коэффициентов.

Легко проверить, что получившаяся система полиномов является нередуцированным базисом Грёбнера идеала, порождённого полиномами f_1, f_2, f_3. Для его построения мы использовали 16 S-полиномов, в то время как стандартный алгоритм Бухбергера (без первого и второго критериев) требует рассмотрения 45 S-полиномов.

4. Заключение

В работе был изложен «асимметричный» подход к изложению алгоритма Бухбергера с использованием существенных умножений, позволяющий интерпретировать формирование S-полиномов и их последующие редукции как часть единого процесса приведения к нормальной форме. Существенное умножение также позволяет исключить из рассмотрения ряд S-полиномов, заведомо редуцирующихся к 0. Данный метод родствен инволютивному подходу Гердта и Блинкова, однако приведённая в работе процедура остаётся алгоритмом Бухбергера.

Темой для дальнейшего исследования может стать рассмотрение наряду с существенными $\succ$-умножениями существенных умножений более общего вида, и инволютивные деления будут частным их случаем. Формулирование алгоритма Бухбергера и инволютивного алгоритма в общем виде поможет построить чёткие методы сравнения двух алгоритмов и проанализировать их вычислительные преимущества.

Литература

[1] Гердт В. П., Янович Д. А., Блинков Ю. А. Быстрый поиск делителя Жане // Программирование. — 2001. — № 1. — С. 32—36.

[2] Жарков А. Ю., Блинков Ю. А. Инволютивные системы алгебраических уравнений // Программирование. — 1994.

[3] Кокс Д., Литтл Дж., О'Ши Д. Идеалы, многообразия и алгоритмы. — М.: Мир, 2000.

[4] Латышев В. Н. Комбинаторная теория колец. Стандартные базисы. — М.: Изд-во Моск. ун-та, 1988.

[5] Михалёв А. В., Панкратьев Е. В. Компьютерная алгебра. Вычисления в дифференциальной и разностной алгебре. — М.: Изд-во Моск. ун-та, 1989.

[6] Семёнов А. С. Парный анализ инволютивных делений // Фундамент. и прикл. мат. — 2003. — Т. 9, вып. 3. — С. 199—212.

[7] Apel J. The theory of involutive divisions and an application to Hilbert function computations // J. Symbolic Comput. — 1998. — Vol. 25, no. 6. — P. 683—704.

[8] Calmet J., Hausdorf M., Seiler W. M. A constructive introduction to involution // Proc. Int. Symp. Applications of Computer Algebra — ISACA 2000. — New Delhi, 2001. — P. 33—50.

[9] Gebauer R., Möller H. M. Buchberger's algorithm and staggered linear bases // Proc. 5th ACM Symp. on Symbolic and Algebraic Computations. Waterloo, Ontario, Canada, 1986. — P. 218—221.

[10] Gerdt V. P. Involutive division technique: Some generalizations and optimizations // J. Math. Sci. — 2002. — Vol. 108, no. 6. — P. 1034—1051.

[11] Gerdt V. P., Blinkov Yu. A. Involutive bases of polynomial ideals // Math. Comput. Simulation. — 1998. — Vol. 45. — P. 519—542.

[12] Gerdt V. P., Blinkov Yu. A. Minimal involutive bases // Math. Comput. Simulation. — 1998. — Vol. 45. — P. 543—560.

[13] Gerdt V. P., Blinkov Yu. A. Janet-like monomial division, Janet-like Gröbner bases // Computer Algebra in Scientific Computing / CASC 2005. — Springer, 2005. — P. 174—195.

[14] Zharkov A. Yu., Blinkov Yu. A. Involutive bases of zero-dimensional ideals. — Preprint No. E5-94-318. — Dubna: Joint Institute for Nuclear Research, 1994.