

С. Ю. Оревков

О МОДУЛЯРНОМ ВЫЧИСЛЕНИИ БАЗИСОВ ГРЕБНЕРА С ЦЕЛЫМИ КОЭФФИЦИЕНТАМИ

§1. ВВЕДЕНИЕ

Пусть $A = \mathbb{Z}[X]$, $X = (x_1, \dots, x_n)$. Мы рассматриваем A как подмножество в $\mathbb{Q}[X]$, тем самым, если I – идеал кольца A , то $\mathbb{Q}I$ – порожденный им идеал кольца $\mathbb{Q}[X]$. Для кольца R обозначим естественное отображение $A \rightarrow A \otimes R = R[X]$ через ι_R . Данная заметка посвящена решению следующей алгоритмической задачи (см. в [1] определение и свойства базисов Гребнера идеалов в полиномиальных кольцах над \mathbb{Z}).

Задача (P). *Предположим, что задана бесконечная последовательность f_1, f_2, \dots элементов кольца A (черный ящик, генерирующий их один за другим). Пусть $I = (f_1, f_2, \dots)$ – идеал, порожденный всеми f_i . Вычислить базис Гребнера идеала I в предположении что базис Гребнера идеала $\mathbb{Q}I$ и базисы Гребнера идеалов $\iota_{\mathbb{Z}/m\mathbb{Z}}(I)$, $m \in \mathbb{Z}$, известны.*

Эта алгоритмическая задача возникает в [5, 6] (см. подробнее в §2). Предлагаемое решение основано на вычислении экспоненты подгруппы кручения абелевой группы A/I (см. [3]) и на основной лемме из §3 настоящей статьи.

§2. МОТИВАЦИЯ

Алгоритмическая задача, возникшая в [5, 6], на самом деле заключается в следующем. Пусть F – свободный A -модуль конечного ранга, M_0 – его подмодуль, заданный конечным набором образующих G_0 , $\tau \in \text{Hom}_A(F, A)$, и $\rho_1, \dots, \rho_p \in \text{End}_A(F)$. Требуется вычислить идеал $\tau(M)$ (его базис Гребнера), где M – это минимальный подмодуль модуля F такой что $M_0 \subset M$ и $\rho_i(M) \subset M$ для всех $i = 1, \dots, p$. Теоретически эта задача имеет очевидное решение, а именно, мы можем

Ключевые слова: базис Гребнера, модулярные вычисления.

последовательно вычислять базисы Гребнера подмодулей M_j , рекурсивно задаваемых как $M_{j+1} = \sum_{i=1}^p \rho_i(M_j)$, до тех пор, пока не выполнится равенство $M_{j+1} = M_j$. Когда это случится, положим $M = M_j$ и $I = \tau(M)$.

Однако если ранг модуля F велик, то вычисление базисов Гребнера A -модулей M_j может оказаться настолько трудоемким, что на практике его нельзя будет выполнить. В то же время, базисы Гребнера $(\mathbb{Z}/m\mathbb{Z})[X]$ -модулей $M_j \otimes (\mathbb{Z}/m\mathbb{Z})$ вычисляются гораздо быстрее. Зная их, можно найти базисы Гребнера $\mathbb{Q}[X]$ -модулей $M_j \otimes \mathbb{Q}$ (см. [2] и §5 ниже). Поэтому можно вычислить модули $M \otimes (\mathbb{Z}/m\mathbb{Z})$ и $M \otimes \mathbb{Q}$, а значит, и идеалы $\iota_{\mathbb{Z}/m\mathbb{Z}}(I)$ и $\mathbb{Q}I$. Кроме того, мы можем последовательно вычислять образующие идеала I вида $\tau\rho_{i_1}\rho_{i_2}\dots\rho_{i_k}(g)$, $g \in G_0$. Поэтому естественно возникает задача (P).

§3. РЕШЕНИЕ ЗАДАЧИ (P)

Пусть обозначения будут как во введении.

Основная лемма. Пусть I и J – идеалы в A , причем $J \subset I$. Обозначим через t экспоненту подгруппы кручения абелевой группы A/J , т.е., t – наименьшее положительное число, при котором $t(\mathbb{Q}J \cap A) \subset J$. Пусть m_1, \dots, m_t – попарно взаимно простые числа, произведение которых равно t . Предположим, что

- (i) $\mathbb{Q}J = \mathbb{Q}I$, т. е. I и J порождают один и тот же идеал в $\mathbb{Q}[X]$,
- (ii) $\iota_{\mathbb{Z}/m_i\mathbb{Z}}(J) = \iota_{\mathbb{Z}/m_i\mathbb{Z}}(I)$, $i = 1, \dots, t$.

Тогда $I = J$.

Доказательство. Положим $c_i = t/m_i = \prod_{j \neq i} m_j$, $i = 1, \dots, t$. Поскольку числа m_i попарно взаимно просты, существуют целые числа $b_1, \dots, b_t \in \mathbb{Z}$, для которых выполнено равенство

$$b_1c_1 + \dots + b_tc_t = 1 \quad (1)$$

Нам требуется показать, что $I \subset J$. Пусть $f \in I$. По условию (ii) для любого $i = 1, \dots, t$, имеем $f = f_i + m_i h_i$, где $f_i \in J$ и $h_i \in A$. По условию (i) имеем $kf \in J$ при некотором $k \in \mathbb{Z}$, следовательно, для любого i имеем $km_i h_i = kf - kf_i \in J$, т. е., h_i представляет элемент подгруппы

кручения группы A/J . По определению числа m это влечет $mh_i \in J$, а значит $c_i f = c_i f_i + c_i m_i h_i = c_i f_i + mh_i \in J$. Вместе с (1) это дает

$$f = b_1(c_1 f) + \dots + b_t(c_t f) \in J. \quad \square$$

Таким образом, мы получаем следующее решение задачи (\mathcal{P}). Фиксируем произвольный допустимый порядок на мономах кольца A . Будем перебирать все идеалы J вида (f_1, \dots, f_k) , $k = 1, 2, \dots$ и для каждого из них выполнять следующие действия:

- (1) Вычислить редуцированные базисы Гребнера идеалов $\mathbb{Q}I$ и $\mathbb{Q}J$. Если они не совпадают, перейти к следующему J .
- (2) Вычислить число m (введенное в основной лемме), воспользовавшись одним из алгоритмов, приведенных в [3] (см. также §4). Пусть $m = p_1^{\alpha_1} \dots p_t^{\alpha_t}$ — разложение числа m на простые множители, и пусть $m_i = p_i^{\alpha_i}$.
- (3) Для каждого $i = 1, \dots, t$, вычислить редуцированные базисы Гребнера идеалов $\iota_{\mathbb{Z}/m_i\mathbb{Z}}(I)$ и $\iota_{\mathbb{Z}/m_i\mathbb{Z}}(J)$. Если они не совпадают, перейти к следующему J . Если же они совпадают, то вычислить базис Гребнера идеала J и завершить работу алгоритма.

§4. ВЫЧИСЛЕНИЕ ЧИСЛА m

В [3] обсуждается несколько алгоритмов вычисления числа m (введенного в основной лемме). Для удобства читателя приведем тот алгоритм, который (цитируя [3]) ‘представляется наиболее подходящим для практических вычислений’. Он состоит из следующих шагов:

- (1) Фиксируем произвольный допустимый порядок на мономах и вычислим базис Гребнера G идеала J . Обозначим через s наибольшее общее кратное старших коэффициентов элементов базиса G . Тогда $\mathbb{Q}J \cap A = \mathbb{Z}[1/s]J \cap A$.
- (2) Введем новую переменную Y . Тогда $\mathbb{Z}[1/s]J \cap A = (I, sY - 1) \cap A$. Базис Гребнера G_s этого идеала можно вычислить, используя мономиальный порядок для исключения переменной (elimination term ordering).
- (3) Найдем m такое что $mg \in J$ для всех $g \in G_s$.

§5. О МОДУЛЯРНОМ ВЫЧИСЛЕНИИ БАЗИСОВ ГРЕБНЕРА НАД \mathbb{Q}

В наших обозначениях теорема Элизабет Арнольд формулируется следующим образом (аналогичная теорема имеет место для модулей).

Теорема [2, Th. 7.1]. Пусть I – однородный идеал в $\mathbb{Z}[X]$ и $G \subset \mathbb{Z}[X]$. Пусть $\mathbb{Q}I$ – идеал в $\mathbb{Q}[X]$, порожденный идеалом I . Пусть p – простое число. Обозначим $I_p = \iota_{\mathbb{F}_p}(I)$, $G_p = \iota_{\mathbb{F}_p}(G)$. Предположим:

- (1) G_p является базисом Гребнера идеала I_p ,
- (2) G является базисом Гребнера им порожденного идеала $\langle G \rangle_{\mathbb{Q}}$ кольца $\mathbb{Q}[X]$,
- (3) $\mathbb{Q}I \subset \langle G \rangle_{\mathbb{Q}}$,
- (4) $\text{LM}(G_p) = \text{LM}(G)$, где “LM” обозначает множество старших мономов.

Тогда G – базис Гребнера идеала $\mathbb{Q}I$.

В [4, Th. 2.4] утверждается, что это теорема верна также для неоднородных идеалов. Однако это не так, что видно на простейшем примере $I = (px + 1)$, $G = \{1\}$.

Когда идеал не однороден, его можно сделать таковым, добавив новую переменную, и после этого применить теорему Э. Арнольд. Например, если сделать однородным вышеприведенный контр-пример, т. е. положить $I = (px + y)$, $G = \{y\}$, то перестанет выполняться условие (3) и, тем самым, противоречие исчезнет.

Благодарность. Я признателен В. П. Гердту за полезные обсуждения.

ЛИТЕРАТУРА

1. W. W. Adams, P. Loustaunau, *An Introduction to Gröbner Bases*. — Graduate Studies in Mathematics **3**, A.M.S., RI (1994).
2. E. A. Arnold, *Modular algorithms for computing Gröbner bases*. — J. of Symbolic Computations **35** (2003), 403–419.
3. M. Aschenbrenner, *Algorithms for computing saturations of ideals in finitely generated commutative rings*. — Appendix to: Automorphisms mapping a point into a subvariety J. of Algebraic Geom. **20** (2011), 785–794. (by B. Poonen)
4. V. Idrees, G. Pfister, S. Steidel, *Parallelization of modular algorithms*. — J. of Symbolic Computations **46** (2011), 672–684.
5. S. Yu. Orevkov, *Markov trace on the Funar algebra*. — arXiv:1206.0765.
6. С. Ю. Оревкин, *Кубические алгебры Гекке и инварианты трансверсальных зацеплений*. — ДАН (в печати) arXiv:1307.5862

Orevkov S. Yu. On modular computation of Gröbner bases with integer coefficients.

Let $I_1 \subset I_2 \subset \dots$ be an increasing sequence of ideals of the ring $\mathbb{Z}[X]$, $X = (x_1, \dots, x_n)$ and let I be their union. We propose an algorithm to compute the Gröbner base of I under the assumption that the Gröbner bases of the ideal $\mathbb{Q}I$ of the ring $\mathbb{Q}[X]$ and the the ideals $I \otimes (\mathbb{Z}/m\mathbb{Z})$ of the rings $(\mathbb{Z}/m\mathbb{Z})[X]$ are known.

Such an algorithmic problem arises, for example, in the construction of Markov and semi-Markov traces on cubic Hecke algebras.

Математический институт
им. В. А. Стеклова РАН, Москва, Россия;
Университет им. Поля Сабатье (Тулуса-3),
Тулуса, Франция
E-mail: `orevkv@math.ups-tlse.fr`

Поступило 18 ноября 2013 г.