ФОРМУЛА ГАЙДАРА ДЛЯ НАИБОЛЬШЕГО ОБЩЕГО ДЕЛИТЕЛЯ НЕСКОЛЬКИХ ПОЛИНОМОВ

С. В. Дужин, С. В. Чмутов

В заметке приводится доказательство изящной формулы Е. А. Гайдара, выражающей наибольший общий делитель набора полиномов от многих переменных через базис Гребнера порожденного ими идеала. Эта формула была опубликована автором [3] незадолго до его смерти в автомобильной катастрофе. Препринт [3] труднодоступен, при этом он написан чересчур длинно и не слишком аккуратно. Сама же формула Гайдара настолько красива и проста, что мы сочли своим долгом сделать ее достоянием широкой математической общественности.

Идея приводимого ниже доказательства теоремы 1 принадлежит А. И. Каишеву [4]; в выводе теоремы 2 мы следуем оригинальному рассуждению автора. Светлой памяти нашего друга Жени Гайдара мы посвящаем эту публикацию.

Пусть A — кольцо полиномов от конечного числа переменных $x_1, ..., x_n$ над произвольным полем $\mathbb{K}$:

$$A = \mathbb{K}[x_1, ..., x_n].$$

Предположим, что задан некоторый порядок на мономах в A, совместимый с умножением (см. [1]). В дальнейшем под старшими мономами полиномов подразумеваются старшие мономы относительно этого выбранного порядка. Система образующих идеала $I \subset A$ называется *базисом Гребнера*, если старшие мономы ее элементов порождают тот же идеал в A, что и старшие мономы всех полиномов идеала I. Понятие базиса Гребнера допускает множество эквивалентных переформулировок и служит основанием всей конструктивной коммутативной алгебры [1,5].

Теорема 1. *Если $f_1, ..., f_m$ — полиномы, образующие базис Гребнера, то*

$$\mathrm{lm}(\text{НОД}(f_1, ..., f_m)) = \text{НОД}(\mathrm{lm}(f_1), ..., \mathrm{lm}(f_m)),$$

где $\mathrm{lm}(f)$ обозначает старший моном f.

Доказательство. Сначала сведем задачу к случаю взаимно простых полиномов $f_1, ..., f_m$. Для этого предположим, что $\text{НОД}(f_1, ..., f_m) = q$ и $f_i = q \cdot g_i$ для всех $i = 1, ..., m$. Тогда $\mathrm{lm}(f_i) = \mathrm{lm}(q) \cdot \mathrm{lm}(g_i)$ и остается доказать, что

$$\text{НОД}(\mathrm{lm}(g_1), ..., \mathrm{lm}(g_m)) = 1,$$

где $g_1, ..., g_m$ — набор взаимно простых полиномов, образующий базис Гребнера.

Предположим противное: $\text{НОД}(\mathrm{lm}(g_1), ..., \mathrm{lm}(g_m)) \neq 1$, т.е. существует переменная x_k, входящая во все мономы $\mathrm{lm}(g_1), ..., \mathrm{lm}(g_m)$. Рассмотрим полиномы $g_1, ..., g_m$ как элементы кольца $B = \mathbb{K}(x_1, ..., \widehat{x_k}, ..., x_n)[x_k]$. Заметим, что в кольце B эти полиномы также взаимно просты. (Доказательство этого простого утверждения мы опускаем). Поскольку B — кольцо полиномов от одной переменной, то существуют такие $h_1, ..., h_m \in B$, что

$$h_1 \cdot g_1 + ... + h_m \cdot g_m = 1.$$

Пусть $v \in \mathbb{K}[x_1, ..., \widehat{x_k}, ..., x_n]$ — наименьшее общее кратное знаменателей всех коэффициентов $h_1, ..., h_m$. Умножая обе части последнего равенства на v, получим:

$$\widetilde{h}_1 \cdot g_1 + ... + \widetilde{h}_m \cdot g_m = v,$$

где $\widetilde{h}_i \in A$.

Тогда v принадлежит идеалу, порожденному $g_1, ..., g_m$ в A. Поскольку $g_1, ..., g_m$ — базис Гребнера, старший моном $\mathrm{lm}(v)$ полинома v должен принадлежать идеалу, порожденному старшими мономами $\mathrm{lm}(g_1)$,...$\mathrm{lm}(g_m)$. Это, однако, невозможно, ибо старшие мономы $\mathrm{lm}(g_i)$ содержат x_k, а v — нет. Полученное противоречие доказывает теорему.

Замечание. Теорема 1 является частным случаем теоремы Кределя и Вейспфеннинга [2], утверждающей, что размерность алгебраического многообразия V равна размерности многообразия V' нулей старших мономов элементов базиса Гребнера F идеала V. В частности, если элементы F взаимно просты, то $\dim V < n{-}1$ и, следовательно, $\dim V' < n{-}1$. А это означает, что мономы из $\mathrm{lm}(F)$ взаимно просты. Этот факт эквивалентен теореме 1. Однако, доказательство Кределя и Вейспфеннинга их теоремы гораздо сложнее приведенного выше доказательства ее частного случая.

В случае лексикографического порядка на мономах из теоремы 1 вытекает формула, выражающая НОД через базис Гребнера.

Теорема 2 (формула Гайдара).

$$\text{НОД}(P) = \frac{\mathrm{lc}_{x_1,\ldots,x_n}(f_1)\cdot\ldots\cdot\mathrm{lc}_{x_{n-1},x_n}(f_{n-1})\cdot\mathrm{lc}_{x_n}(f_n)}{\mathrm{lc}_{x_2,\ldots,x_n}(f_1)\cdot\ldots\cdot\mathrm{lc}_{x_n}(f_{n-1})}.$$

Пояснение. Здесь P — произвольное множество полиномов из A, $f_1,\ldots,f_n$ — некоторые (возможно, не все) элементы базиса Гребнера F идеала, порожденного P, относительно лексикографического порядка, при котором $x_1 > x_2 > \ldots > x_n$. Эти элементы выбраны из F так, что $\mathrm{lm}(f_i)/\,\text{НОД}(\mathrm{lm}(F))$ не зависит от x_i для каждого $i = 1,\ldots,n$. (Такой выбор возможен в силу теоремы 1; разумеется, он не однозначен). Через $\mathrm{lc}_{x_{i+1},\ldots,x_n}(f)$ обозначен полиномиальный коэффициент при старшем мономе f , рассматриваемом как полином от переменных $x_1, x_2, \ldots, x_i$ над кольцом $\mathbb{K}[x_{i+1},\ldots,x_n]$. Поскольку НОД набора полиномов определен с точностью до умножения на константу, старшие коэффициенты (в обычном смысле) всех возникающих полиномов можно считать единичными.

Доказательство. Пусть $q = \text{НОД}(P)$. Тогда существуют такие полиномы g_i, что $f_i = g_i\cdot q$. Будем последовательно вычислять полиномы $\mathrm{lc}_{x_n}(q)$, $\mathrm{lc}_{x_{n-1},x_n}(q)$,..., $\mathrm{lc}_{x_1,x_2,\ldots,x_n}(q) = q$. Поскольку $\mathrm{lc}_{x_n}(f_n) = \mathrm{lc}_{x_n}(g_n)\cdot\mathrm{lc}_{x_n}(q)$ и $\mathrm{lc}_{x_n}(g_n) = 1$ (согласно выбору g_n), то $\mathrm{lc}_{x_n}(q) = \mathrm{lc}_{x_n}(f_n)$. Предположим, что $\mathrm{lc}_{x_{i+1},\ldots,x_n}(q)$ уже найдено и вычислим $\mathrm{lc}_{x_i,\ldots,x_n}(q)$. Имеем:

$$\mathrm{lc}_{x_i,\ldots,x_n}(f_i) = \mathrm{lc}_{x_i,\ldots,x_n}(g_i)\cdot\mathrm{lc}_{x_i,\ldots,x_n}(q),$$
$$\mathrm{lc}_{x_{i+1},\ldots,x_n}(f_i) = \mathrm{lc}_{x_{i+1},\ldots,x_n}(g_i)\cdot\mathrm{lc}_{x_{i+1},\ldots,x_n}(q).$$

По построению, старший моном $\mathrm{lm}(g_i)$ не зависит от x_i, значит,

$$\mathrm{lc}_{x_i,\ldots,x_n}(g_i) = \mathrm{lc}_{x_{i+1},\ldots,x_n}(g_i),$$

и, следовательно,

$$\mathrm{lc}_{x_i,\ldots,x_n}(q) = \frac{\mathrm{lc}_{x_i,\ldots,x_n}(f_i)}{\mathrm{lc}_{x_{i+1},\ldots,x_n}(f_i)}\cdot\mathrm{lc}_{x_{i+1},\ldots,x_n}(q).$$

Спустившись таким образом до $i = 1$, мы получим нужную формулу для НОД(P).

[1] L. Robbiano. Gröbner Bases: a Foundation for Commutative Algebra. – Preprint, 1989. [2] H. Kredel, V. Weispfenning. Computing Dimension and Independent Sets for Polynomial Ideals. – J. of Symb. Comp., v. 6, p. 231—248, 1988. [3] E. A. Gaydar. The calculation of polynomial GCD by Gröbner basis. – Utrecht University, preprint no. 678, September 1991. [4] А. И. Каишев. Частное сообщение, 1990. [5] Компьютерная алгебра. Символьные и алгебраические вычисления. – М.: Мир, 1986.

Институт программных систем
Российской Академии Наук
Переславль-Залесский