Сравнение сложностей задач нахождения базиса Гребнера идеала и решений этого идеала

А. В. Шокуров

Аннотация. Сравниваются сложности задач нахождения решения системы алгебраических уравнений и базисов Гребнера идеалов этих систем.

Ключевые слова: базис Гребнера, вычислительная сложность

1. Введение

В диссертации Б. Бухбергера [Buc06] в 1965 году был предложен новый метод исследования идеалов в кольцах многочленов. В основании метода положено использование базиса идеала специального вида — базиса Гребнера, названного им так в честь своего научного руководителя. Предложенный подход позволил доказать алгоритмическую сводимость задачи нахождения решений системы алгебраических уравнений от многих переменных к задаче нахождения решений алгебраического уравнения от одной переменной. В дальнейшем этот метод нашел множество применений в различных теоретических и прикладных разделах математики, механики, криптографии и др. (см. [Buc01], [Laz83]).

Однако практическое использование метода сопряжено с колоссальными вычислительными затратами. Первые оценки трудоемкости этого метода были получены еще тогда, когда понятие базиса Гребнера еще не было известно. В работе [Her25] еще в 1925 г. была получена необходимая верхняя оценка в виде двойной экспоненты от числа переменных и максимальных степеней входящих описание задачи многочленов для степеней разложения элемента идеала по его произвольному базису. Как оказалось позднее [Dube] эта оценка не может быть улучшена.

Поскольку базис Гребнера зависит от допустимого упорядочения на множестве термов, естественно был поставлен вопрос о возможной зависимости трудоемкости вычисления такого базиса от такого прядочения. Поэтому сначала потребовалось описать такие упорядочения. Полное описание таких опорядочений было дано в работе [Rob85]. Однако этот же результат можно извлечь из более ранних работ [МИ53] и [Gio52].

В дальнейшем эти упорядочения использовались при построении специальных алгоритмов нахождения базиса Гребнера. Выделим особо алгоритмы F_4 и F_5 предложенные Фожеро ([Fau99], [Fau02]).

Экспоненциальная оценка для сложности задачи нахождения базиса Гребнера в общем случае получена в [KM96]. Среди других работ в этом направлении выделим [Bar04], [Bro87], [Giu84], [HL11], [Laz83], [May89], [May97], [MM82].

Для булевых идеалов в статье [KM96] доказана

Теорема. 1 *Для заданных базиса булева идеала* $I \subset Q[x_1,\ldots,x_n]$ *и допустимого порядка на термах* $<$ *единственный приведенный базис Гребнера для* I *относительно порядка* $<$ *(задача 1) может быть вычислен алгоритмом, объем используемой памяти которого ограничен сверху полиномом от длины входных данных.*

В данной работе доказано, что размер базиса Гребнера G булева идеала I может иметь экспоненциальный размер относительно размера описания базиса идеала I, т.е. выполняется

Теорема. 2 *Задача построения базиса Гребнера булева идеала не принадлежит классу* FP.

2. Основные определения

Пусть M — произвольное множество. Отображение

$$M \times M \to M \qquad (1)$$

будем называть операцией. Для операции могут использоваться мультипликативная и аддитивная запись — xy и $x+y$ соответственно. Аддитивная запись обычно используется только для коммутативной операции, т.е. когда $x+y=y+x$ для всех пар (x,y).

Операция называется ассоциативной, если для всех троек (x,y,z) выполняются соотношения $(xy)z = x(yz)$.

Если для всех пар x,y из M выполняются соотношения $xy = yx$, то операция называется коммутативной.

Элемент $e \in M$ называется единичным элементом, если для всех $x \in M$ выполняются соотношения $ex = x = xe$. (В случае аддитивной записи операции единичный элемент обозначается через 0 и называется нулевым элементом.) Единичный элемент единствен, если он существует. Действительно, пусть e' — другой единичный элемент. Тогда выполняются соотношения

$$e = ee' = e'.$$

Определение 1. 3 *Множество* M *с ассоциативной операцией называется полугруппой. Полугруппа, содержащая единицу, называется моноидом.*

Определение 2. 4 *Отношение* $\preceq$ *на моноиде* M *называется допустимым упорядочением моноида* M, *если для этого отношения выполняются следующие свойства:*

• Для любых различных элементов n_1 и n_2 моноида M всегда выполненяется в точности одно из соотношений $n_1 \preceq n_2$ или $n_2 \preceq n_1$.

• Если $n_1 \preceq n_2$, то для любого $n \in M$ выполняется соотношение $n \cdot n_1 \preceq n \cdot n_2$.

• В любом непустом подмножестве $M_0 \subseteq M$ всегда существует наименьший элемент $n_0 \in M_0$:

$$\forall\, n \in M_0 \quad n_0 \preceq n \ \textbf{\textit{или}}\ n_0 = n.$$

Отношение $n \preceq m$ будем записывать также как $m \succeq n$.

Пусть $X = \{x_1, \ldots, x_n\}$ — конечное множество. Обозначим через $\mathbb{N}_+$ множество неотрицательных целых чисел. Выражения вида $x_1^{w_1} \cdot \ldots \cdot x_n^{w_n}$, где

$$w = \{w_1, \ldots, w_n\} \in \mathbb{N}_+^n,$$

будем называть термами на множестве X и обозначать $T(X)$. Множество $T(X)$ является моноидом относительно операции умножения, заданной формулой

$$x_1^{w_1} \cdot \ldots \cdot x_n^{w_n} \cdot x_1^{h_1} \cdot \ldots \cdot x_n^{h_n} = x_1^{w_1+h_1} \cdot \ldots \cdot x_n^{w_n+h_n}.$$

На моноиде термов $T(X)$ существует бесконечно много допустимых упорядочений. Из определения моноида термов следует, что достаточно описать допустимое упорядочение на множестве $\mathbb{N}_+^n$.

Примеры допустимых упорядочений на множестве векторов из $\mathbb{N}_+^n$.

• **Лексикографический порядок.** Для $a, b \in \mathbb{N}_+^n$ будем считать, что $a \succ b$, если в векторе разности $a - b$ первая слева ненулевая координата положительна.

• **Лексикографический порядок в градуированном моноиде.** Градуируем моноид $M = \bigcup_{i=0}^{\infty} M_i$, где $M_i = \{a \in \mathbb{N}_+^n \mid a_1 + \ldots + a_n = i\}$. При $i > j$ всякий элемент множества M_i больше любого элемента множества M_j. Порядок в каждом M_i зададим как лексикографический.

• **Обратный лексикографический порядок в градуированном моноиде.** Градуируем моноид $M = \bigcup_{i=0}^{\infty} M_i$, где $M_i = \{a \in \mathbb{N}_+^n \mid a_1 + \ldots + a_n = i\}$. При $i > j$ всякий элемент множества M_i больше любого элемента множества M_j. Порядок в каждом M_i зададим как обратный лексикографический, т. е. для элементов $a, b \in M_i$ выполняется соотношение $a \succ b$ тогда и только тогда, когда первая справа ненулевая координата в векторе разности $a - b$ отрицательная.

Фиксируем некоторый допустимый порядок $\preceq$ на множестве термов $T(X)$. Фиксируем также некоторое поле K. Элементами кольца многочленов на множестве переменных $X = \{x_1, \ldots, x_n\}$ являются выражения вида

$$\sum_{t \in T(X)} a_t \cdot t,$$

где $a_t \in K$ и $a_t \neq 0$ только для конечного множества термов $t \in T(X)$.

Определение. 5 *Пусть* A — *поле. Конечное множество* G *называется базисом Гребнера идеала* I *кольца* $A[X]$, *если*

• G — базис идеала I,

• $\forall f \in I\ \exists g \in G \mid HT(g) \mid HT(f)$.

Поскольку A — поле, старший моном любого элемента идеала делится на старший моном некоторого элемента базиса Гребнера этого идеала. Отметим также, что базисы Гребнера идеала для различных допустимых порядков на множестве термов $T(X)$ различны.

3. Простая система уравнений со сложным базисом Гребнера

Теорема 1. 6 *Задача построения базиса Гребнера булева идеала не принадлежит классу* FP.

Рассмотрим кольцо многочленов $K[X]$ от переменных множества $X = \{x_1, \ldots, x_n\}$ над произвольным полем K. Фиксируем целое число $0 < s \leq n$. Для целого $0 < i \leq s$ обозначим через $s_i^{(s)}(x_1, \ldots, x_s)$ i-й симметрический многочлен. Далее будем предполагать, что хактерика поля K либо 0, либо больше s.

Фиксируем неотрицательное целое число $k \leq n$, где n — число переменных в кольце многочленов. Рассмотрим идеал I, порожденный многочленами

$$f_0(x_1, \ldots, x_n) = x_1 + \ldots + x_n - k, \qquad f_i(x_1, \ldots, x_n) = x_i^2 - x_i,\ i = 1, \ldots, n. \quad (2)$$

Рассмотрим множество многочленов $F = \{ f_i \mid i = 1,\K, n\}$.

Лемма 1. 7 *Пусть идеал I определен многочленами из формулы (2) и заданы два целых числа $0 < i \J s < n$. Тогда существует такой многочлен $P_{i,s}(x_{s+1},\K, x_n)$ степени не выше i от переменных $x_{s+1},\K, x_n$, что*

$$s_i^{(s)}(x_1,\K, x_s) + P_{i,s}(x_{s+1},\K, x_n) \O I.$$

Доказательство. Воспользуемся индукцией по i.

При $i = 1$ определим многочлен $P_{i,s}(x_{s+1},\K, x_n)$ формулой

$$P_{1,s}(x_{s+1},\K, x_n) = x_{s+1} + \K + x_n - k = s_1^{(n-s)}(x_{s+1},\K, x_n) - k.$$

Тогда

$$f_0(x_1,\K, x_n) = s_1^{(s)}(x_1 + \K, x_s) + P_{1,s}(x_{s+1},\K, x_n) \O I.$$

Предположим, что существование многочленов $P_{i,s}$ доказано для всех $i < j \J s$. Докажем существование многочлена $P_{j,s}$. Заметим, что для любых a и b в силу равенства

$$a^j - b^j = (a - b)(a^{j-1} + \K + b^{j-1})$$

и определения идеала из соотношения $a - b \O I$ следует, что $a^j - b^j \O I$.

Положим

$$a = x_1 + \K + x_s \quad = \quad s_1^{(s)}(x_1,\K, x_s) b = - x_{s+1} - \K - x_n + k$$
$$= \quad - s_1^{(n-s)}(x_{s+1},\K, x_n) + k.$$

Легко видеть, что

$$a^j = j! \Ч s_j^{(s)}(x_1,\K, x_s) + L\left(s_1^{(s)}(x_1,\K, x_s),\K, s_{j-1}^{(s)}(x_1,\K, x_s)\right) (\mathrm{mod}\, F),$$

где L — линейная форма. Тогда при некотором $h \O I$ выполняется соотношение

$$a^j \quad = \quad j! \Ч s_j^{(s)}(x_1,\K, x_s) + L\left(s_1^{(s)}(x_1,\K, x_s),\K, s_{j-1}^{(s)}(x_1,\K, x_s)\right)$$
$$+ \quad h(x_1,\K, x_n)$$

Согласно предположению индукции для для всех $i = 1,\K, j - 1$ существуют $h_i \O I$ для которых выполняются соотношения

$$s_i^{(s)}(x_1,\K, x_s) = h_i(x_1,\K, x_n) - P_{i,s}(x_{s+1},\K, x_n).$$

Поскольку $a^j - b^j \O I$, и $b^j = Q_{j,s}(x_{s+1},\K, x_n)$ и $\deg Q_{j,s} \J j$, то при некотором $g \O I$ выполняется соотношение

$$a^j - b^j = j! \Ч s_j^{(s)}(x_1,\K, x_s) - L\left(P_{i,s}(x_{s+1},\K, x_n),\K, P_{i,s}(x_{s+1},\K, x_n)\right) -$$
$$Q_{j,s}(x_{s+1},\K, x_n) + g(x_1,\K, x_n)$$

и, следовательно, можно определить многочлен $P_{j,s}$ формулой

$$P_{j,s}(x_{s+1},\ldots, x_n) = \frac{1}{j!}(Q_{j,s}(x_{s+1},\ldots, x_n) + L(P_{i,s}(x_{s+1},\ldots, x_n),\ldots, P_{i,s}(x_{s+1},\ldots, x_n)))$$

Введем обозначение

$$B^s = \underbrace{\{0\,1\} \r \K \r \{0\,1\}}_{s \text{ сомножителей}}.$$

Для $w = (i_1,\K, i_s) \O B^s$ положим

$$|w| = i_1 + \K + i_s.$$

Для любого целого $0 < k < n$ определим разбиение множества X на два множества $Y = \{x_1,\K, x_{k-1}\}$ (в случае $k = 1$ это множество пустое) и множество $Z = \{x_k,\K, x_n\}$. Напомним, что для любого $w \O B^{k-1}$ определен терм

$$Y^w = x_1^{i_1} \K x_{k-1}^{i_{k-1}},$$

где $w = (i_1,\K, i_{k-1})$, и для любого $h \O B^{n-k+1}$ определен терм

$$Z^h = x_k^{j_1} \K x_n^{j_{n-k+1}},$$

где $h = (j_1,\K, j_{n-k+1})$.

Лемма 2. 8 *Пусть $0 < k < 2k < n$ и характеристика поля K больше n или равна 0. Тогда в кольце многочленов $K[x_k,\K, x_n]$ существует единственный, с точностью до умножения на ненулевую константу, ненулевой многочлен вида*

$$\sum_{w \O B^{n-k+1}} l_w Z^w,$$

принадлежащий идеалу I.

Доказательство. Вначале докажем существование указанного многочлена, воспользовавшись леммой 1.

Положим $s = k - 1$. Согласно лемме 1 для всех $i < k$ определены многочлены $P_{i,k-1}$, удовлетворяющие условиям

$$s_i^{(k-1)}(x_1,\K, x_{k-1}) + P_{i,k-1}(x_k,\K, x_n) \O I.$$

Поскольку $\deg P_{i,k-1} < i$, а идеал I — булев (см. определение 3), то существуют такие многочлены $h_{i,k} \in I$ и

$$Q_{i,k}(x_k,\ldots,x_n) = \sum_{w\in B^{n-k+1},\ |w|<i} l_{w,k} Z^w \in K[Z],$$

что

$$P_{i,k-1}(x_k,\ldots,x_n) = Q_{i,k}(x_k,\ldots,x_n) + h_{i,s}(x_k,\ldots,x_n).$$

Тогда

$$s_i^{(k-1)}(x_1,\ldots,x_{k-1}) + Q_{i,s}(x_k,\ldots,x_n) \in I \qquad (3)$$

для всех пар i,k, удовлетворяющих условию $0 < i < k-1 < n$.

Заметим, что в силу равенства

$$a^k - b^k = (a-b)(a^{k-1} + \ldots + b^{k-1})$$

и определения идеала из соотношения $a - b \in I$ следует, что $a^k - b^k \in I$.

Положим

$$a = x_1 + \ldots + x_{k-1} b = -x_k - \ldots - x_n + k.$$

Раскрывая скобки и используя соотношения $x_i^2 = x_i$ при всех $i = 1,\ldots,n$ получаем равенства

$$a^k = \sum_{i=0}^{k-1} l_i s_i^{(k-1)}(x_1,\ldots,x_{k-1}) \pmod I b^k = \sum_{i=0}^{k-1} m_i s_i^{(n-k+1)}(x_k,\ldots,x_n) + k! s_k^{(n-k+1)}(x_k,\ldots,x_n) \pmod I.$$

Тогда в силу соотношений (3) выполняется равенство

$$a^k = \sum_{w\in B^{n-k+1},\ |w|<k} n_w Z^w \pmod I$$

и, учитывая, что $a^k - b^k \in I$, получаем

$$k! s_k^{(n-k+1)}(x_k,\ldots,x_n) + \sum_{i=0}^{k-1} m_i s_i^{(n-k+1)}(x_k,\ldots,x_n) - \sum_{w\in B^{n-k+1},\ |w|<k} n_w Z^w \in I.$$

Поскольку характеристика поля K больше k, многочлен

$$k! s_k^{(n-k+1)}(x_k,\ldots,x_n) + \sum_{i=0}^{k-1} m_i s_i^{(n-k+1)}(x_k,\ldots,x_n) - \sum_{w\in B^{n-k+1},\ |w|<k} n_w Z^w$$

не равен 0, принадлежит кольцу многочленов $K[Z]$ и идеалу I.

Далее покажем, что указанный многочлен единствен. Выберем любой многочлен

$$p(x_k,\ldots,x_n) = \sum_{w\in B^{n-k+1},\ |w|<k} l_w Z^w,$$

удовлетворяющий условиям леммы 2. Необходимым условием принадлежности многочлена p идеалу I является равенство этого многочлена нулю во всех корнях идеала I.

Разобьем множество M всех корней идеала I на непересекающиеся подмножества M_i, где $i = 0,1,\ldots,k-1$. Для этого определим множество M_i как множество корней $(a_1,\ldots,a_n)$ идеала, удовлетворяющих условию $a_1 + \ldots + a_{k-1} = i$. Множества M_i, очевидно, не пересекаются. Поскольку идеал I булев, то координаты корней могут быть равными только 0 или 1. Поэтому $a_1 + \ldots + a_{k-1} < k$. Следовательно, множество корней M идеала I представимо в виде разбиения

$$M = \bigcup_{i=0}^{k-1} M_i.$$

Докажем, что

$$l_w = (-1)^{|w|} l_{w_0}, \quad (4)$$

где

$$w_0 = (0,\ldots,0).$$

Доказательство проведем индукцией по $i = |w|$.

Пусть $|w| = 1$. Рассмотрим множество корней $M_{k-1} \subset M$. Поскольку $a_1 + \ldots + a_{k-1} = k-1$, то только одна из координат $(a_k,\ldots,a_n)$ равна 1, а остальные нулевые. Все эти корни находятся во взимнооднозначном соответствии с такими векторами $w \in B^{n-k+1}$, что $|w| = 1$. Поскольку многочлен p обращается в нуль на таких векторах, то для всех $|w| = 1$ выполняется равенство $l_w = -l_{w_0}$.

Пусть равенство (4) доказано для всех $|w| < m < k$. Докажем равенство (4) для всех $|w| = m$.

Рассмотрим множество корней $M_{k-m} \subset M$. Поскольку $a_1 + \ldots + a_{k-1} = k-m$, то из координат $(a_k,\ldots,a_n)$ в точности m равны 1, а остальные нулевые. Все такие решения находятся во взимнооднозначном соответствии с такими

$w \in B^{n-k+1}$, что $|w| = m$. Заметим, что согласно определению множества M_{k-m} и предположения индукции для таких решений выполняется равенство

$$p(a_k,\ldots,a_n) = \sum_{w\in B^{n-k+1}}^{|w|\ge m} l_w A^w = \sum_{w\in B^{n-k+1}}^{|w|<m} (-1)^{|w|} l_{w_0} A^w + \sum_{h\in B^{n-k+1}}^{|h|=m} l_h A^h,$$

где $A = (a_k,\ldots,a_n)$. Согласно определению множества M_{k-m} и ввиду неравенства $2k < n$ при $0 \le i < m$ на решениях из M_{k-m} справедливо равенство

$$\sum_{w\in B^{n-k+1}}^{|w|=i} (-1)^{|w|} l_{w_0} A^w = \sum_{w\in B^{n-k+1}}^{|w|=i} (-1)^i l_{w_0} A^w = (-1)^i \binom{m}{i} l_{w_0}.$$

Также выполнено равенство

$$l_{h_0} = \sum_{h\in B^{n-k+1}}^{|h|=m} l_h A^h,$$

где $h_0 = (a_k,\ldots,a_n)$. Заметим, что справедливы равенства

$$\sum_{i=0}^{m} \binom{m}{i} (-1)^i = (1-1)^m = 0. \qquad (5)$$

Поскольку многочлен p равен нулю на таких векторах $(a_k,\ldots,a_n)$, то выполняются равенства

$$p(a_k,\ldots,a_n) = \sum_{i=0}^{m-1} \binom{m}{i} (-1)^i l_{w_0} + l_{h_0} = 0.$$

Учитывая теперь соотношение (5) получаем равенство $l_{h_0} = (-1)^m l_{w_0}$. Следовательно, для всех $|w| = m$ выполняется равенство $l_w = (-1)^{|w|} l_{w_0}$.

Поэтому

$$p(a_k,\ldots,a_n) = l_{w_0} \left(\sum_{i=0}^{k} s_i^{(n-k+1)}(x_k,\ldots,x_n) \right)$$

Следствие 1. 9 *Пусть выполняются предположения леммы 2. Тогда многочлен*

$$p(a_k,\ldots,a_n) = \sum_{i=0}^{k} s_i^{(n-k+1)}(x_k,\ldots,x_n). \qquad (6)$$

является неприводимым элементом базиса Гребнера идеала I для лексикографического упорядочения термов на множестве переменных $X = \{x_1,\ldots,x_n\}$.

Доказательство. Предположим, что многочлен p приводим. Тогда существует элемент g неприводимого базиса Гребнера идеала I, старший терм которого делит один из термов многочлена p. Следовательно, этот старший терм многочлена g содержит только переменные из множества $Z = \{x_k,\ldots,x_n\}$. Поскольку термы многочлена g упорядочены лексикографически, все его остальные термы также зависят только от переменных из множества Z. Поэтому многочлен g удовлетворяет условиям леммы 8, и многочлен $p \in K[x_k,\ldots,x_n]$ отличается от g ненулевым множителем, т.е. p неприводим.

Следующее утверждение завершает доказательство теоремы 1.

Следствие. 10 *При* $k = \left\lfloor \frac{n}{2} \right\rfloor$ *размер базис Гребнера идеала* I *экспоненциален относительно описания идеала* I *формулами (2).*

Доказательство. Многочлен p является неприводимым элементом базиса Гребнера идеала I и содержит $\binom{n}{k+1} > 2^{n/2}$ термов с коэффициентами 1.

4. Нахождение решений систем алгебраических уравнений с использованием базиса Гребнера

Определение 3. 11 *Идеал* I *в кольце многочленов* $K[x_1,\ldots,x_n]$ *над полем* K *называется булевым, если* $x_i^2 - x_i \in I$ *для любого* $0 < i \le n$. *Система уравнений, определяющая такой идеал, называется булевой.*

Теорема 2. 12 *Если булева система уравнений над полем* K *имеет единственное решение, то приведенный базис Гребнера идеала этой системы определен однозначно с точностью до коэффициентов и не зависит от выбора допустимого порядка на множестве мономов.*

Доказательство. В силу соотношений $x_i^2 = x_i$ все x_i принимают значения в множестве $\{0,1\}$, и следовательно, решения, принадлежащие алгебраическому замыканию поля K, лежат в поле K. Пусть единственным решением булевой системы уравнений является набор $x_i = a_i, i = 1,\ldots,n$. Докажем вначале, что идеал

$$I = \{x_1 - a_1,\ldots,x_n - a_n\}$$

совпадает в этом случае с идеалом, заданным булевыми уравнениями исходной системы уравнений. Действительно, поскольку $x_i - a_i$ обращается в нуль во всех решениях исходной системы, то согласно теореме Гильберта о нулях идеала при некотором натуральном k многочлен $(x_i - a_i)^k$ принадлежит идеалу, заданному исходной булевой системой уравнений, а тогда и сам многочлен $x_i - a_i$ принадлежит этому идеалу, поскольку выполняется равенство $x_i^2 = x_i$. Следовательно, идеал I лежит в идеале J, заданном булевыми уравнениями исходной системы уравнений. Очевидно, что для любого многочлена $f \in J$ выполняется соотношение $f \to_{F^*} \underline{a}$, где $a \in \{0,1\}$. Если этот элемент ненулевой, то система не имеет решения. Если этот элемент нулевой, то это означает, что $f \in I$. Поэтому $I = J$.

Пусть F_0 — приведенный базис Гребнера, относительно некоторого допустимого порядка. Пусть x_n — наименьший моном положительной степени относительно этого порядка. Тогда из $x_n - a_n \in I$ следует существование многочлена $h \in F_0$ старший моном которого делит моном x_n. Поскольку моном x_n — наименьший, этот моном делится на старший моном многочлена h. Следовательно, $x_n - a_n \in F_0$. Переменная x_n не входит ни в один оставшихся многочленов базиса Гребнера F_0. Следовательно, рассуждая как выше получаем, что в базис Гребнера входит также $x_{n-1} - a_{n-1}$, где x_{n-1} следующая по старшинству переменная.

Следствие 3. 13 *Задачи нахождения базиса Гребнера и единственного решения для булевых идеалов, имеющих единственное решение эквивалентны.*

Литература.

[Bar04] Bardet, M. and Faugere, J.C and Salvy, B. “On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations”.In: International Conference on Polynomial System Solving - ICPSS. Paris, France, Nov. 2004, pp. 71 – 75.

[Bro87] D. Brownawell. “Bounds for the degrees in the Nullstellensatz”. In: Annals of Math. Second Series 126.3 (1987), pp. 577–591.

[Buc06] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal (An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal).* PhD thesis, Universität Innsbruck, 1965. English translation in J. of Symbolic Computation, Special Issue on Logic, Mathematics, and Computer Science: Interactions. 41(3/4):475--511, 2006.

[Buc01] B. Buchberger. Gröbner Bases : A Short Introduction for Systems Theorists, Computer Aided Systems Theory—EUROCAST 2001 (2001) Volume: 330, Issue: 9, Publisher: Springer, Pages: 1–19.

[Gio52] Trevisan Giorgio. “Classificazione dei semplici ordinamenti di un gruppo libero commutativo con n generatori”. In: vol. 22. CEDAM, 1952, pp. 143–156.

[Giu84] Marc Giusti.“Some Effectivity Problems in Polynomial Ideal Theory”. In: Proceedings of the International Symposium on Symbolic and Algebraic Computation. EUROSAM’84. London, UK: Springer-Verlag, 1984, pp. 159–171.

[Fau02] J.-C. Faugere. “A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)”. In: Proceedings of the 2002 international symposium on Symbolic and algebraic computation. ISSAC ’02. Lille, France: ACM, 2002, pp. 75–83.

[Fau99] J.-C. Faugere. “A new efficient algorithm for computing Gröbner bases (F4).” In: Journal of Pure and Applied Algebra 139. 1–3(June 1999), pp. 61–88.

[Her25] G. Hermann. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale: Unt. Benutzung nachgelassener Satze v .Kurt Hentzelt. Springer, 1925.

[HL11] Amir Hashemi and Daniel Lazard. “Sharper Complexity Bounds for Zero-Dimensional Gröbner Bases and Polynomial System Solving”. In: IJAC 21.5 (2011), pp. 703–713.

[KM96] Klaus Kühnle and Ernst W. Mayr. “Exponential space computation of Gröbner bases”. In: Proceedings of the 1996 international symposium on Symbolic and algebraic computation. ISSAC’96. Zurich, Switzerland: ACM, 1996, pp. 63–71.

[Laz83] Daniel Lazard. “Gröbner-Bases, Gaussian elimination and resolution of systems of algebraic equations”. In: Proceedings of the European Computer Algebra Conference on Computer Algebra. London, UK: Springer-Verlag, 1983, pp. 146–156.

[May89] Ernst W. Mayr. “Membership in Polynomial Ideals over Q Is Exponential Space Complete”. In: STACS. Ed. by Burkhard Monien and Robert Cori. Vol. 349. Lecture Notes in Computer Science. Springer, 1989, pp. 400–406.

[May97] Ernst W. Mayr. “Some Complexity Results for Polynomial Ideals”. In: J. Complexity 13.3 (1997), pp. 303–325.

[MM82] E. Mayr and A. Meyer. “The complexity of the word problems for commutative semigroups and polynomial ideals”.English.In:Adv.Math., Beijing 46.3 (Dec. 1982), pp. 305–329.

[Riq10] C. Riquier. Les systèmes d’équations aux dérivées partielles. Cornell University Library historical math monographs. Gauthier-Villars, 1910.

[Rob85] Lorenzo Robbiano. Term orderings on the polynomial ring. Computer algebra, EUROCAL ’85, Proc. Eur. Conf., Linz/Austria 1985, Vol. 2, Lect. Notes Comput. Sci. 204, 513-517 (1985). 1985.

[МИ53] Зайцева М.И.. “О совокупности упорядочений абелевой группы”. Успехи математических наук 8 (1953), pp. 135–137.

[Dube] T. W. Dube, The structure of polynomial ideals and Grobner bases, SIAM Jornal of Computing, 19: 750-773, 1990.

Comparing complexities of problems of determining of Grebner's basis of ideal and solving this ideal

Shokurov A.V. ISP RAS, Moscow, Russia

Abstract. A new method of investigation of ideals in the rings of polynomials was proposed by B. Buchberger in 1965. He proposed to use special basis in such rings named "Gröbner Basis" in the honor of his teacher. The proposed approach has allowed to prove the algorithmic reducibility of the task of finding solutions of a system of algebraic equations in many variables to the problem of solving algebraic equation of one variable. However, the practical use of the method needs enormous computational cost. The first estimate of the computational complexity of this method was obtained by G. Hermann in 1925, when the concept of Gröbner basis was not yet known. Was obtained the required upper estimate in the form of dual exponent of the number of variables and the maximum degree of incoming task description polynomials of degree of decomposition element ideal for an arbitrary basis. As it turned out later by T.W. Dube this estimate cannot be improved.

In 1996 K. Kühnle and E. W. Mayr proved, that for Boolean ideals the upper bound of memory capacity is exponential on input size. For zero-dimensional ideals A. Hashemi and D. Lazard proved the exponential complexity of finding Gröbner basis. Here we prove the lower bound of computation of such bases, by giving an example of an ideal having Gröbner basis of exponential size on input.

Keywords: Gröbner basis, computational complexity

References.

[Bar04] Bardet, M. and Faugere, J.C and Salvy, B. "On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations".In: International Conference on Polynomial System Solving - ICPSS. Paris, France, Nov. 2004, pp. 71 – 75.

[Bro87] D. Brownawell. "Bounds for the degrees in the Nullstellensatz". In: Annals of Math. Second Series 126.3 (1987), pp. 577–591.

[Buc06] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal (An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal).* PhD thesis, Universität Innsbruck, 1965. English translation in J. of Symbolic Computation, Special Issue on Logic, Mathematics, and Computer Science: Interactions. 41(3/4):475--511, 2006.

[Buc01] B. Buchberger. Gröbner Bases : A Short Introduction for Systems Theorists, Computer Aided Systems Theory—EUROCAST 2001 (2001) Volume: 330, Issue: 9, Publisher: Springer, Pages: 1–19.

[Gio52] Trevisan Giorgio. "Classificazione dei semplici ordinamenti di un gruppo libero commutativo con n generatori". In: vol. 22. CEDAM, 1952, pp. 143–156.

[Giu84] Marc Giusti."Some Effectivity Problems in Polynomial Ideal Theory". In: Proceedings of the International Symposium on Symbolic and Algebraic Computation. EUROSAM'84. London, UK: Springer-Verlag, 1984, pp. 159–171.

[Fau02] J.-C. Faugere. "A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)". In: Proceedings of the 2002 international symposium on Symbolic and algebraic computation. ISSAC '02. Lille, France: ACM, 2002, pp. 75–83.

[Fau99] J.-C. Faugere. "A new efficient algorithm for computing Gröbner bases (F4)." In: Journal of Pure and Applied Algebra 139. 1–3(June 1999), pp. 61–88.

[Her25] G. Hermann. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale: Unt. Benutzung nachgelassener Satze v .Kurt Hentzelt. Springer, 1925.

[HL11] Amir Hashemi and Daniel Lazard. "Sharper Complexity Bounds for Zero-Dimensional Gröbner Bases and Polynomial System Solving". In: IJAC 21.5 (2011), pp. 703–713.

[KM96] Klaus Kühnle and Ernst W. Mayr. "Exponential space computation of Gröbner bases". In: Proceedings of the 1996 international symposium on Symbolic and algebraic computation. ISSAC'96. Zurich, Switzerland: ACM, 1996, pp. 63–71.

[Laz83] Daniel Lazard. "Gröbner-Bases, Gaussian elimination and resolution of systems of algebraic equations". In: Proceedings of the European Computer Algebra Conference on Computer Algebra. London, UK: Springer-Verlag, 1983, pp. 146–156.

[May89] Ernst W. Mayr. "Membership in Polynomial Ideals over Q Is Exponential Space Complete". In: STACS. Ed. by Burkhard Monien and Robert Cori. Vol. 349. Lecture Notes in Computer Science. Springer, 1989, pp. 400–406.

[May97] Ernst W. Mayr. "Some Complexity Results for Polynomial Ideals". In: J. Complexity 13.3 (1997), pp. 303–325.

[MM82] E. Mayr and A. Meyer. "The complexity of the word problems for commutative semigroups and polynomial ideals".English.In:Adv.Math., Beijing 46.3 (Dec. 1982), pp. 305–329.

[Riq10] C. Riquier. Les systèmes d'équations aux dérivées partielles. Cornell University Library historical math monographs. Gauthier-Villars, 1910.

[Rob85] Lorenzo Robbiano. Term orderings on the polynomial ring. Computer algebra, EUROCAL '85, Proc. Eur. Conf., Linz/Austria 1985, Vol. 2, Lect. Notes Comput. Sci. 204, 513-517 (1985). 1985.

[МИ53] Зайцева М.И.. "О совокупности упорядочений абелевой группы". Успехи математических наук 8 (1953), pp. 135–137.

[Dube] T. W. Dube, The structure of polynomial ideals and Grobner bases, SIAM Jornal of Computing, 19: 750-773, 1990.