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.

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 $I \subseteq Q[x_1,\dots,x_n]$ 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 $\prec$ на моноиде M называется допустимым упорядочением моноида M, если для этого отношения выполняются следующие свойства:*

• Для любых различных элементов ν_1 и ν_2 моноида M всегда выполненяется в точности одно из соотношений $\nu_1 \prec \nu_2$ или $\nu_2 \prec \nu_1$.

• Если $\nu_1 \prec \nu_2$, то для любого $\nu \in M$ выполняется соотношение $\nu \cdot \nu_1 \prec \nu \cdot \nu_2$.

• В любом непустом подмножестве $M_0 \subset M$ всегда существует наименьший элемент $\nu_0 \in M_0$:

$$\forall\, \nu \in M_0 \quad \nu_0 \prec \nu \ \textbf{\textit{или}}\ \nu_0 = \nu.$$

Отношение $\nu \prec \mu$ будем записывать также как $\mu \succ \nu$.

Пусть $X = \{x_1, \ldots, x_n\}$ — конечное множество. Обозначим через $\mathbb{Z}_+$ множество неотрицательных целых чисел. Выражения вида $x_1^{\omega_1} \ldots x_n^{\omega_n}$, где

$$\omega = \{\omega_1, \ldots, \omega_n\} \in \mathbb{Z}_+^n,$$

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

$$x_1^{\omega_1} \ldots x_n^{\omega_n} \cdot x_1^{\eta_1} \ldots x_n^{\eta_n} = x_1^{\omega_1+\eta_1} \ldots x_n^{\omega_n+\eta_n}.$$

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

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

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

• **Лексикографический порядок в градуированном моноиде.** Градуируем моноид $M = \bigcup_{i=0}^{\infty} M_i$, где $M_i = \{\alpha \in \mathbb{Z}_+^n \mid \alpha_1 + \ldots + \alpha_n = i\}$. 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 $M_i = \{\alpha \in \mathbb{Z}_+^n \mid \alpha_1 + \ldots + \alpha_n = i\}$. 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 $\alpha, \beta \in M_i$ выполняется соотношение $\alpha \succ \beta$ тогда и только тогда, когда первая справа ненулевая координата в векторе разности $\alpha - \beta$ отрицательная.

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

$$\sum_{t \in T\langle X\rangle} a_t \cdot t,$$

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

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 $T\langle X\rangle$ 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 $\sigma_i^{(s)}(x_1, \ldots, x_s)$ 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 $F = \{f_i \mid i = 1,\dots,n\}$.

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

$$\sigma_i^{(s)}(x_1,\dots,x_s) + P_{i,s}(x_{s+1},\dots,x_n) \in I.$$

Доказательство. Воспользуемся индукцией по i.

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

$$P_{1,s}(x_{s+1},\dots,x_n) = x_{s+1} + \dots + x_n - k = \sigma_1^{(n-s)}(x_{s+1},\dots,x_n) - k.$$

Тогда

$$f_0(x_1,\dots,x_n) = \sigma_1^{(s)}(x_1 + \dots, x_s) + P_{1,s}(x_{s+1},\dots,x_n) \in I.$$

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

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

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

Положим

$$\begin{aligned} a = x_1 + \dots + x_s &= \sigma_1^{(s)}(x_1,\dots,x_s) \\ b &= -x_{s+1} - \dots - x_n + k \\ &= -\sigma_1^{(n-s)}(x_{s+1},\dots,x_n) + k. \end{aligned}$$

Легко видеть, что

$$a^j = j! \cdot \sigma_j^{(s)}(x_1,\dots,x_s) + L\left(\sigma_1^{(s)}(x_1,\dots,x_s),\dots,\sigma_{j-1}^{(s)}(x_1,\dots,x_s)\right) (\mathrm{mod}\, F),$$

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

$$\begin{aligned} a^j &= j! \cdot \sigma_j^{(s)}(x_1,\dots,x_s) + L\left(\sigma_1^{(s)}(x_1,\dots,x_s),\dots,\sigma_{j-1}^{(s)}(x_1,\dots,x_s)\right) \\ &+ h(x_1,\dots,x_n) \end{aligned}$$

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

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

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

$$\begin{aligned} a^j - b^j = j! \cdot \sigma_j^{(s)}(x_1,\dots,x_s) - L\left(P_{i,s}(x_{s+1},\dots,x_n),\dots,P_{i,s}(x_{s+1},\dots,x_n)\right) - \\ Q_{j,s}(x_{s+1},\dots,x_n) + g(x_1,\dots,x_n) \end{aligned}$$

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

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

Введем обозначение

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

Для $\omega = (i_1,\dots,i_s) \in B^s$ положим

$$|\omega| = i_1 + \dots + i_s.$$

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

$$Y^\omega = x_1^{i_1} \dots x_{k-1}^{i_{k-1}},$$

где $\omega = (i_1,\dots,i_{k-1})$, и для любого $\eta \in B^{n-k+1}$ определен терм

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

где $\eta = (j_1,\dots,j_{n-k+1})$.

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

$$\sum_{\omega \in B^{n-k+1}}^{|\omega| \le k} \lambda_\omega Z^\omega,$$

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

$$\sigma_i^{(k-1)}(x_1,\dots,x_{k-1}) + P_{i,k-1}(x_k,\dots,x_n) \in I.$$

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

$$Q_{i,k}(x_k,\dots,x_n) = \sum_{\omega\in B^{n-k+1}}^{|\omega|\le i} \lambda_{\omega,k} Z^{\omega} \in K[Z],$$

что

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

Тогда

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

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

Заметим, что в силу равенства

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

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

Положим

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

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

$$a^k = \sum_{i=0}^{k-1} \lambda_i \sigma_i^{(k-1)}(x_1,\dots,x_{k-1}) \pmod I b^k = \sum_{i=0}^{k-1} \mu_i \sigma_i^{(n-k+1)}(x_k,\dots,x_n) +$$
$$k!\cdot \sigma_k^{(n-k+1)}(x_k,\dots,x_n) \pmod I.$$

Тогда в силу соотношений (3) выполняется равенство

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

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

$$k!\cdot \sigma_k^{(n-k+1)}(x_k,\dots,x_n) + \sum_{i=0}^{k-1} \mu_i \sigma_i^{(n-k+1)}(x_k,\dots,x_n) - \sum_{\omega\in B^{n-k+1}}^{|\omega|< k} \nu_{\omega} Z^{\omega} \in I.$$

Поскольку характеристика поля K больше k, многочлен

$$k!\cdot \sigma_k^{(n-k+1)}(x_k,\dots,x_n) + \sum_{i=0}^{k-1} \mu_i \sigma_i^{(n-k+1)}(x_k,\dots,x_n) - \sum_{\omega\in B^{n-k+1}}^{|\omega|< k} \nu_{\omega} Z^{\omega}$$

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

Далее покажем, что указанный многочлен единствен. Выберем любой многочлен

$$p(x_k,\dots,x_n) = \sum_{\omega\in B^{n-k+1}}^{|\omega|\le k} \lambda_{\omega} Z^{\omega},$$

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 $i = 0,1,\dots,k-1$. Для этого определим множество M_i как множество корней $(\alpha_1,\dots,\alpha_n)$ идеала, удовлетворяющих условию $\alpha_1 + \dots + \alpha_{k-1} = i$. Множества M_i, очевидно, не пересекаются. Поскольку идеал I булев, то координаты корней могут быть равными только 0 или 1. Поэтому $\alpha_1 + \dots + \alpha_{k-1} < k$. Следовательно, множество корней M идеала I представимо в виде разбиения

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

Докажем, что

$$\lambda_{\omega} = (-1)^{|\omega|} \lambda_{\omega_0}, \quad (4)$$

где

$$\omega_0 = (0,\dots,0).$$

Доказательство проведем индукцией по $i = |\omega|$.

Пусть $|\omega| = 1$. Рассмотрим множество корней $M_{k-1} \subset M$. Поскольку $\alpha_1 + \dots + \alpha_{k-1} = k-1$, то только одна из координат $(\alpha_k,\dots,\alpha_n)$ равна 1, а остальные нулевые. Все эти корни находятся во взимнооднозначном соответствии с такими векторами $\omega \in B^{n-k+1}$, что $|\omega| = 1$. Поскольку многочлен p обращается в нуль на таких векторах, то для всех $|\omega| = 1$ выполняется равенство $\lambda_{\omega} = -\lambda_{\omega_0}$.

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

Рассмотрим множество корней $M_{k-m} \subset M$. Поскольку $\alpha_1 + \dots + \alpha_{k-1} = k-m$, то из координат $(\alpha_k,\dots,\alpha_n)$ в точности m равны 1, а остальные нулевые. Все такие решения находятся во взимнооднозначном соответствии с такими

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

$$p(\alpha_k,\ldots,\alpha_n) = \sum_{\omega\in B^{n-k+1}}^{|\omega|\le m} \lambda_\omega A^\omega = \sum_{\omega\in B^{n-k+1}}^{|\omega|< m} (-1)^{|\omega|}\lambda_{\omega_0} A^\omega + \sum_{\eta\in B^{n-k+1}}^{|\eta|= m} \lambda_\eta A^\eta,$$

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

$$\sum_{\omega\in B^{n-k+1}}^{|\omega|= i} (-1)^{|\omega|}\lambda_{\omega_0} A^\omega = \sum_{\omega\in B^{n-k+1}}^{|\omega|= i} (-1)^i \lambda_{\omega_0} A^\omega = (-1)^i \cdot \binom{m}{i} \cdot \lambda_{\omega_0}.$$

Также выполнено равенство

$$\lambda_{\eta_0} = \sum_{\eta\in B^{n-k+1}}^{|\eta|= m} \lambda_\eta A^\eta,$$

где $\eta_0 = (\alpha_k,\ldots,\alpha_n)$. 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 $(\alpha_k,\ldots,\alpha_n)$, то выполняются равенства

$$p(\alpha_k,\ldots,\alpha_n) = \sum_{i=0}^{m-1} (-1)^i \cdot \binom{m}{i} \cdot \lambda_{\omega_0} + \lambda_{\eta_0} = 0.$$

Учитывая теперь соотношение (5) получаем равенство $\lambda_{\eta_0} = (-1)^m \cdot \lambda_{\omega_0}$. Следовательно, для всех $|\omega| = m$ выполняется равенство $\lambda_\omega = (-1)^{|\omega|} \cdot \lambda_{\omega_0}$.

Поэтому

$$p(\alpha_k,\ldots,\alpha_n) = \lambda_{\omega_0} \cdot \left(\sum_{i=0}^{k} \sigma_i^{(n-k+1)}(x_k,\ldots,x_n) \right).$$

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

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

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* $k = \left[\frac{n}{2}\right]$ *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 Gro□bner 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 Gro□bner 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.