Нахождение корней систем алгебраических уравнений с помощью базиса Гребнера

А.В. Шокуров, shok@ispras.ru
ИСП РАН

Аннотация. Описан и обоснован алгоритм нахождения решения системы алгебраических уравнений над полем k для идеалов нулевой размерности, в случае если задан базис Гребнера идеала этой системы для лексикографического порядка на термах от ее переменных. Полученное решение лежит в алгебраическом замыкании основного поля. Приведен пример системы алгебраических уравнений, имеющей единственное решение в основном поле, а общее число решений экспоненциально относительно описания этой системы.

Ключевые слова. Базис Гребнера, идеал,

1. Введение

Пусть k — поле, а K — его алгебраическое замыкание. Напомним, что алгебраическое замыкание кольца рациональных функций над полем κ от бесконечного числа независимых переменных называется универсальным расширением поля *K*. Будем обозначать его Ω. Идеал, порожденный конечным множеством $F \subseteq k[x_1, \dots, x_n]$, обозначим через (*F*). Согласно теореме Гильберта о базисе, для любого идеала существует конечное множество многочленов, порождающее этот идеал.

Многообразием идеала (см. [1]) $I \subseteq k[x_1, \dots, x_n]$ в K^n будем называть множество

$$V(I) = \{\xi \in K^n \mid \forall p \in I \text{ выполняется равенство } p(\xi) = 0\}.$$

Элемент $\xi \in \Omega^n$ называется общим корнем простого идеала *I*, если выполнены условия:

- $\xi \in V(I)$
- $p \in I \Leftrightarrow p(\xi) = 0.$

Задача 1. Задано конечное множество F элементов в кольце многочленов над полем и базис Гребнера *G* идеала (F). Определить, что выполняется:

- $V\big((F)\big) = \emptyset$, или
- $V((F)) \neq \emptyset$ и конечно, или
- $V((F)) \neq \emptyset$ и бесконечно.

Задача 2. Задано конечное множество F элементов в кольце многочленов над полем и базис Гребнера *G* идеала *(F).* Определить, что выполняется:

- $dim_k\ (F) = 0$ или
- $dim_k\ (F) \neq 0.$

Напомним определение лексикографического порядка на множестве термов от переменных $x_1, \dots, x_n$. Поскольку имеется взаимнооднозначное соответствие множества термов от переменных $x_1, \dots, x_n$ и элементами прямого произведения *n* экземпляров множества неотрицательных чисел $\mathbb{Z}^n$, достаточно определить порядок на $\mathbb{Z}_+^n$. Для $\alpha, \beta \in \mathbb{Z}_+^n$ будем считать, что $\alpha \succ \beta,$ если $\alpha \neq \beta$ и при некотором $1 < i_0 \leq n$

- $\alpha_{i_0} > \beta_{i_0}$
- $\alpha_{i_0} = \beta_{i_0}$ при любом $n \geq i \geq i_0.$

В частности, $x_1 \prec x_2 \prec \cdots \prec x_n.$

Задача 3. Задано конечное множество F элементов в кольце многочленов $k[x_1, \dots, x_n]$, для которого $dim_k\ (F) = 0$, и базис Гребнера G идеала (F) относительно лексикографического порядка. Найти (построить) множество V((F)).

Приводятся алгоритмы решения поставленных задач и доказана их корректность.

2. Идеалы нулевой размерности

Лемма 1. Многообразие V(I) решений идеала $I \subseteq k[x_1, \dots, x_n]$ конечно тогда и только тогда, когда $k[x_1, \dots, x_n]/I$ — конечномерное над k векторное пространство.

Доказательство. **Необходимость.** Если решений нет, то согласно теореме Гильберта о нулях идеал I содержит единицу и, поэтому, совпадает с кольцом многочленов $k[x_1, \dots, x_n]$. Следовательно,

$$dim_k\ k[x_1, \dots, x_n]/I = 0.$$

Пусть теперь множество $V(I)$ непусто, конечно и $(\lambda_{i,1},\dots,\lambda_{i,n})$, при $i = 1,\dots,m$, — все его элементы. Поскольку $\lambda_{i,j}$ принадлежат алгебраическому замыканию поля k, то для каждого такого $\lambda_{i,j}$ существует многочлен $p_{\lambda_{i,j}}(x) \in k[x]$ с корнем $\lambda_{i,j}$. Тогда многочлены

$$p_j(x_j) = \prod_{i=1}^{m} p_{i,j}(x_j) \in k[x_1,\dots,x_n],\ \ j = 1,\dots,n$$

обращаются в ноль на всех решениях идеала, и, следовательно, по теореме Гильберта о нулях существуют такие k_j, что $p_j^{k_j} \in I$. Поэтому,

$$deg_k\, k[x_1,\dots,x_n]/I \le \prod_{i=1}^{m}(m_j\, k_j + 1),$$

где $m_j = \deg p_j$.

Достаточность. Пусть теперь $dim_k\ k[x_1,\dots,x_n]/I$ конечна. Если эта размерность нулевая, то $I = k[x_1,\dots,x_n]$ и, следовательно, множество решений пусто, т.е. конечно.

Рассмотрим случай когда размерность $dim_k\ k[x_1,\dots,x_n]/I$ конечна, но не равна нулю. Рассмотрим базис Гребнера идеала I для лексикографического порядка на множестве многочленов. Согласно определению базиса Гребнера, каждый многочлен из $k[x_1,\dots,x_n]$ редуцируется к единственному нередуцируемому многочлену, т.е. все термы полученного многочлена не содержат термы, делящиеся на старшие термы многочленов из базиса Гребнера идеала I. Рассмотрим многочлены вида $f(x_1)$. По определению лексикографического порядка, любой терм, в который входит хотя бы одна из переменных $x_2,\dots,x_n$, старше любого терма вида x_1^m. Поэтому, существует многочлен $p_1(x_1)$, принадлежащий базису Гребнера идеала I (в противном случае размерность векторного пространства $k[x_1,\dots,x_n]/I$ над полем $к$ была бы бесконечной), а следовательно, и идеалу I. Аналогично для всех остальных переменных существуют $p_i(x_i) \in I$. Тогда все решения идеала I лежат в произведении всех решений $p_i(x_i) = 0$, т.е. в конечном множестве. □

Лемма 2. *Размерность идеала $I \subseteq k[x_1,\dots,x_n]$ равна нулю тогда и только тогда, когда многообразие $V(I)$ конечно и непусто.*

Доказательство. Пусть $I = [I_1,\dots,I_s]$ — неприводимое представление идеала I примарными идеалами и $p_1,\dots,p_s$ — ассоциированные с этим представлением простые идеалы (согласно теореме Ласкера, см. [1]). Размерность идеала I, по определению, равна максимальной из размерностей простых идеалов $p_1,\dots,p_s$.

Предположим, что $dim_k\, I = 0$. Тогда для всех $i = 1,\dots,s$ выполнено $dim_k\, p_i = 0$. Непосредственно из определений следует, что $V(p_i) = V(I_i)$ и, следовательно, множества $V(I_i)$ конечны. Поэтому и множество решений $V(I) = V(I_1) \cup \dots \cup V(I_s)$ конечно.

Пусть теперь множество $V(I)$ — конечно. Тогда и все $V(p_i)$ конечны. Достаточно проверить, что для простого идеала p размерности большей нуля множество $V(p)$ бесконечно. Для этого, согласно лемме 1, достаточно убедиться, что величина $dim_k\ k[x_1,\dots,x_n]/p$ бесконечна. Пусть $(\xi_1,\dots,\xi_n)$ — общий корень идеала p. Тогда определены вложения

$$k \subset k[\xi_1,\dots,\xi_n] \subset k(\xi_1,\dots,\xi_n) \subset \Omega.$$

Поскольку dim p > 0, компоненты общего корня этого идеала содержат трансцендентные элементы. Без ограничения общности можно считать, что ξ_1 трансцендентен. Тогда элементы $\xi_1, \xi_1^2,\dots,\xi_1^m,\dots$ — линейно независимы над k. Следовательно, $dim_k\ k[\xi_1,\dots,\xi_n]$ бесконечна, а поскольку, в силу определения общего корня $(\xi_1,\dots,\xi_n)$ простого идеала p, выполняется равенство $k[\xi_1,\dots,\xi_n] = k[x_1,\dots,x_n]/p$, то и величина $dim_k\ k[x_1,\dots,x_n]/p$ бесконечна.

Лемма 3. Пусть G — базис Гребнера идеала I. Отображение

$$\pi: k[x_1,\dots,x_n]/I \longrightarrow k[x_1,\dots,x_n]$$

заданное формулой $f + I \mapsto h$, где $f \to_{G^*} \underline{h}$ — неприводимая редукция, определено корректно, взаимно однозначно и является k-гомоморфизмом векторных пространств.

Доказательство. Формула $f \to_{G^*} \underline{h}$ задает гомоморфизм k-векторных пространств

$$\varphi: k[x_1,\dots,x_n] \longrightarrow k[x_1,\dots,x_n]$$

ядром которого является идеал I. Следовательно, π определено корректно и является k-мономорфизмом. □

Следствие 1. Пусть G — базис Гребнера идеала I. Размерность идеала I равна нулю тогда и только тогда, когда множество неприводимых относительно базиса Гребнера G термов конечно.

Теорема 1. Пусть G — базис Гребнера собственного идеала кольца многочленов $k[x_1,\dots,x_n]$. Этот идеал имеет размерность 0 тогда и только тогда, когда для любого допустимого порядка при каждом $1 \le i \le n$ существует многочлен $g_i \in G$ со старшим термом $x_i^{\nu_i}$ где ν_i — некоторое неотрицательное целое число.

Доказательство. Если для некоторого i не существует элемента базиса Гребнера идеала I со старшим термом $x_i^{\nu_i}$, то термы x_i^m неприводимы.

Следовательно, множество неприводимых термов бесконечно, и, поэтому, согласно следствию 1 размерность идеала I не равна нулю.

Пусть базис Гребнера идеала I содержит многочлены g_i, старшими термами которых являются $x_i^{\nu_i}$. В этом случае необходимым условием неприводимости терма t является выполнение соотношений $deg_{x_i}t < \nu_i$ для всех i=1,...,n. Поэтому, мощность множества неприводимых термов не превосходит величину $\nu_1 \cdot \ldots \cdot \nu_n$, и, следовательно, конечна. А тогда, согласно следствию 1, размерность идеала I равна нулю. □

3. Решение систем уравнений

Решение задачи 1. Согласно теореме Гильберта о нулях, условие $V\big((F)\big) = \emptyset$ эквивалентно условию $1 \in (F)$, или, эквивалентно, $1 \in G$.

Пусть теперь $1 \notin G$. Тогда $V((F)) \neq \emptyset$. Вопрос о конечности или бесконечности многообразия $V((F))$ решается теперь теоремой 1 и леммой 2. Достаточно преверить, содержит ли базис Гребнера G многочлены со старшими термами $x_i^{\nu_i}$ при всех i = 1, ..., n.

Задача 2 полностью решается в теореме 1.

Для решения **задачи 3** потребуется решить следующую задачу.

Задача нахождения хотя бы одного решения идеала нулевой размерности, если задан приведенный базис Гребнера этого идеала относительно лексикографического порядка. Предположим, что задан базис Гребнера $g_1, \ldots, g_m$ идеала $I \subseteq k[x_1, \ldots, x_n]$ нулевой размерности. Пусть также имеется оракул $\mathcal{A}$, решающий задачу нахождения корня любого многочлена одной переменной над K, где K — алгебраическое замыкание поля k.

Отметим, что имея базис Гребнера относительно некоторого порядка, всегда можно найти соответствующий базис Гребнера относительно лексикографического порядка (см., например, [3])

Решение задачи нахождения хотя бы одного решения идеала нулевой размерности, если задан его приведенный базис Гребнера относительно лексикографического порядка.

Пусть $I \subseteq k[x_1, \ldots, x_n]$ — идеал и G — приведенный базис Гребнера относительно лексикографического порядка этого идеала. Тогда пересечение $G \cap k[x_1]$ состоит в точности из одного многочлена $f(x_1) \in k[x_1]$ и является базисом Гребнера идеала $I_1 = I \cap k[x_1]$ кольца $k[x_1]$. Находим с помощью оракула $\mathcal{A}$ решение $\xi_1 \in K$ уравнения $f(x_1) = 0$ (K — алгебраическое замыкание поля k). Заметим, что для любого решения $(x_1^0, \ldots, x_n^0)$ идеала I выполняется соотношение $f(x_1^0) = 0$.

Предположим теперь, что найдено решение $(\xi_1, \ldots, \xi_i)$ идеала $I_i = I \cap k[x_1, \ldots, x_i]$. Чтобы найти продолжение $(\xi_1, \ldots, \xi_i, \xi_{i+1})$ полученного выше решения, вычислим элементы базиса Гребнера G, находящиеся в кольце $k[x_1, \ldots, x_{i+1}]$. Затем выполним подстановки $x_j = \xi_j$ для всех j=1,..., i в полученные многочлены базиса Гребнера. Получим набор многочленов, зависящих только от одной переменной x_{i+1}. Вычислим их наибольший общий делитель $g(x_{i+1})$. Как будет показано ниже, полученный многочлен имеет степень не менее единицы и, следовательно, имеет непустое множество решений в алгебраическом замыкании поля k. Находим с помощью оракула $\mathcal{A}$ решение $\xi_{i+1} \in K$ уравнения $g(x_{i+1}) = 0$. Тогда вектор $(\xi_1, \ldots, \xi_i, \xi_{i+1})$ является решением идеала $I_{i+1} = I \cap k[x_1, \ldots, x_{i+1}]$.

Далее повторяем описанную процедуру до тех пор, пока не найдем полный вектор решения идеала I.

Ниже приведен алгоритм для описанной процедуры нахождения решения алгебраической системы уравнений.

Алгоритм А. Дано: Базис Гребнера $G = (g_1, \ldots, g_m)$ относительно лексикографического порядка идеала $I \subseteq k[x_1, \ldots, x_n]$ нулевой размерности.

Выход: Точка $(x_1^0, \ldots, x_n^0) \in K^n$, где K алгебраическое замыкание поля k.

Шаг 1 $i := 1$.

Шаг 2 Находим пересечение $G_1 = G \cap k[x_1]$, состоящее в точности из одного многочлена $g(x_1)$.

Шаг 3 $x_i^0 := \mathcal{A}(g(x_i))$ — некоторое решение уравнения $g(x_i) = 0$.

Шаг 4 $i := i + 1$.

Шаг 5 Если $i > n$, перейти к шагу 10.

Шаг 6 Находим пересечение $G_i = G \cap k[x_1, \ldots, x_i]$.

Шаг 7 $G_i(x_1^0, \ldots, x_{i-1}^0) := \{g(x_1^0, \ldots, x_{i-1}^0, x_i) \big| g \in G_i\} \subseteq K[x_i]$.

Шаг 8 Находим $g(x_i)$ — наибольший общий делитель элементов множества $G_i(x_1^0, \ldots, x_{i-1}^0)$.

Шаг 9 Переходим к шагу 3.

Шаг 10 Выход: Точка $(x_1^0, \ldots, x_n^0) \in K^n$, где K алгебраическое замыкание поля k, является решением идеала I.

Теорема 2. Для любого идеала размерности ноль алгоритм А находит некоторое его решение.

Для доказательства теоремы достаточно доказать, что на шаге 8 приведенного выше алгоритма всегда получаем многочлен степени не меньше единицы, или, эквивалентно, каждое решение $(\xi_1, \dots, \xi_i) \in K^i$ идеала $I_i = I \cap k[x_1, \dots, x_i]$ продолжается до решения $(\xi_1, \dots, \xi_{i+1}) \in K^{i+1}$ идеала $I_{i+1} = I \cap k[x_1, \dots, x_{i+1}]$. Доказательство этого утверждения потребует несколько вспомогательных утверждений.

Для любого подмножества *M* кольца $k[x_1, \dots, x_n]$ и любого 0 < *i*< *n* будем использовать следующее **обозначение:** $M_i = M \cap k[x_1, \dots, x_i]$. Заметим, что если *I* — идеал кольца $k[x_1, \dots, x_n]$,*то* I_i — идеал кольца $k[x_1, \dots, x_i]$.

Лемма 4. Если G — приведенный базис Гребнера относительно лексикографического порядка идеала $I \subseteq k[x_1, \dots, x_i]$, то d — приведенный базис Гребнера идеала I_i в кольце многочленов от переменных $x_1, \dots, x_i$ относительно лексикографического порядка на термах.

Доказательство. Следует из определения базиса Гребнера для лексикографического порядка. □

Лемма 5. Пусть $I \subseteq k[x_1, \dots, x_n]$ — простой идеал. Тогда для любого 0 < i < п идеал I_i простой.

Доказательство. Действительно, если $pq \in I_i$, то тем более $pq \in I$, и, *следовательно*, $p \in I$ или $q \in I$. Поскольку $pq \in k[x_1, \dots, x_i]$, то и $p \in k[x_1, \dots, x_i]$ и $q \in k[x_1, \dots, x_i]$. Поэтому, $p \in I_i$ или $q \in I_i$. □

Аналогично доказывается

Лемма 6. Пусть $I \subseteq k[x_1, \dots, x_n]$ — примарный идеал. Тогда для любого 0 < i < п идеал I_i примарный.

Лемма 7. Пусть $I \subseteq k[x_1, \dots, x_n]$ — примарный идеал и J — ассоциированный с ним простой идеал. Тогда множества корней идеалов I и J совпадают.

Доказательство. Следует непосредственно из определения ассоциированного простого идеала примарного идеала. □

Лемма 8. Пусть $I \subseteq k[x_1, \dots, x_n]$ — примарный идеал и J — ассоциированный с ним простой идеал. Тогда простой идеал J_i ассоциирован с идеалом I_i.

Доказательство. Следует из лемм 5 и 6 и определения ассоциированного простого идеала примарного идеала. □

Лемма 9. *Если* $I \subseteq k[x_1, \dots, x_n]$ *— идеал размерности 0, то* I_m *является идеалом размерности 0 в кольце многочленов* $k[x_1, \dots, x_m]$ для всех m=1,…,n.

Доказательство. Пусть *G* — приведенный базис Гребнера идеала *I* размерности ноль. Согласно теореме 1, для всех *i* = 1, . . . , *n* существуют многочлены $g_i \in G$ со старшими термами $x_i^{\nu_i}$. Если *G* — базис Гребнера идеала *I* относительно лексикографического порядка, то $g_i \in G_i$ и для любого $1 \le i \le m$ элементы $g_i \in I_m$. Поскольку старший терм g_i равен $x_i^{\nu_i}$, то, по теореме 1, размерность идеала I_m равна нулю. □

Следствие 2. *Пусть G — базис Гребнера относительно лексикографического порядка идеала* $I \subseteq k[x_1, \dots, x_n]$ *размерности 0. Тогда* G_1 *состоит в точности из одного многочлена* $f \in k[x_1]$ *положительной степени.*

Лемма 10. *Пусть* $I \subseteq k[x_1, \dots, x_n]$ *— простой идеал размерности 0 и* $(\xi_1, \dots, \xi_i) \in K^i$ *— корень идеала* I_i. *Тогда при 1 < i < n — 1 существует* $\xi_{i+1} \in K$ *такой, что* $(\xi_1, \dots, \xi_{i+1}) \in K^{i+1}$*— корень идеала* I_{i+1}.

Доказательство. Поскольку идеал I размерности 0, он не совпадает со своим кольцом и, следовательно, по теореме Гильберта имеет некоторый корень $(\omega_1, \dots, \omega_n)$ в K^n. В частности, $(\omega_1, \dots, \omega_i) \in K^i$, также как и $(\xi_1, \dots, \xi_i) \in K^i$, является корнем идеала I_i. Поскольку согласно леммам 5 и 9 идеал I_i прост и имеет нулевую размерность, а все корни простого идеала сопряжены, то имеется изоморфизм подполей поля K

$$\varphi: k(\omega_1, \dots, \omega_i) \longrightarrow k(\xi_1, \dots, \xi_i)$$

заданный соответствиями $\omega_j \mapsto \xi_j$ для всех *j* = 1, . . . ,*i.*

Пусть G — базис Гребнера идеала I и многочлен $h \in k(\omega_1, \dots, \omega_n)[x_{i+1}]$ является наибольшим общим делителем многочленов $f(x_{i+1}) = g(\omega_1, \dots, \omega_i, x_{i+1})$, где g_i пробегает G_{i+1}. Поскольку $(\omega_1, \dots, \omega_{i+1})$ является корнем идеала I_{i+1}, элемент ω_{i+1} удовлетворяет соотношению $h(\omega_{i+1}) = 0$. Верно и обратное, для любого корня ζ уравнения *h(x)* = 0, точка $(\omega_1, \dots, \omega_i, \zeta)$ также корень идеала I_{i+1}, а поскольку размерность простого идеала I_{i+1} равна нулю, то эта точка также является общим корнем этого идеала. Поскольку число корней идеала размерности нуль конечно, то и число решений уравнения *h(xi+i)* = 0 не пусто и конечно. Поэтому степень многочлена *h* положительна.

Обозначим через $\tilde{h}$ наибольший общий делитель многочленов $f(x_{i+1}) = g(\xi_1, \dots, \xi_i, x_{i+1})$, где g пробегает G_{i+1}. Тогда согласно определению изоморфизма φ выполняется соотношение $\varphi^*(h) = \tilde{h}$ и степени многочленов h и $\tilde{h}$ совпадают. Следовательно, степень многочлена $\tilde{h}$ положительна. Поэтому уравнение $\tilde{h}(x_{i+1}) = 0$ всегда разрешимо в *K.* Пусть его решение ξ_{i+1}. Тогда $(\xi_1, \dots, \xi_{i+1}) \in K^{i+1}$ — корень идеала I_{i+1}.

Лемма 11. *Пусть* $(\xi_1, \dots, \xi_n) \in \Omega^n$ *— общий корень идеала простого идеала I. Тогда* $(\xi_1, \dots, \xi_i) \in \Omega^i$ *— общий корень простого идеала* I_i.

Доказательство. Обозначим через J_i — простой идеал, состоящий из всех многочленов кольца $k[x_1, \dots, x_i]$, обращающихся в ноль в точке $(\xi_1, \dots, \xi_i)$. Тогда точка $(\xi_1, \dots, \xi_i)$ является общим корнем идеала J_i.

Очевидно, что $J_i \supseteq I_i$, а поскольку точка $(\xi_1, \dots, \xi_n) \in \Omega^n$ является общим корнем идеала I, то и $J_i \subseteq I$. Следовательно, $J_i \subseteq I_i$. Поэтому $J_i = I_i$ и $(\xi_1, \dots, \xi_i) \in \Omega^i$— общий корень идеала I_i. □

Лемма 12. *Пусть $I \subseteq k[x_1, \dots, x_n]$ —примарный идеал и $(\xi_1, \dots, \xi_i) \in \Omega^i$ — общий корень простого идеала ассоциированного с идеалом I_i. Тогда существует $\xi_{i+1} \in \Omega$ такой, что $(\xi_1, \dots, \xi_{i+1}) \in \Omega^{i+1}$ — общий корень идеала I_{i+1}.*
Доказательство. Следует из лемм 8 и 11. □

Лемма 13. *Пусть $I \subseteq k[x_1, \dots, x_n]$ — примарный идеал размерности 0 и $(\xi_1, \dots, \xi_i) \in K^i$ — корень идеала I_i. Тогда существует $\xi_{i+1} \in K$ такой, что $(\xi_1, \dots, \xi_{i+1}) \in K^{i+1}$ — корень идеала I_{i+1}.*
Доказательство. Является частным случаем леммы 12, поскольку каждый корень простого идеала размерности ноль является его общим корнем. □
Напомним, что *V(I)* — многообразие идеала $I \subseteq k[x_1, \dots, x_n]$.

Лемма 14. *Если идеал I является пересечением идеалов q_j где j пробегает от 1 до m, то $V(I) = \bigcup_{j=1}^{m} V(q_j)$.*
Доказательство. Пусть $\xi \in \bigcup_{j=1}^{m} V(q_j)$. Тогда при некотором $1 \le j \le m$ выполняется $\xi \in V(q_j)$. А поскольку $I \subseteq q_j$, то и $\xi \in V(I)$. Следовательно, $V(I) \supseteq \bigcup_{j=1}^{m} V(q_j)$
Пусть теперь $\xi \notin \bigcup_{j=1}^{m} V(q_j)$. Тогда для всех *j* = 1, ..., *m* существуют $p_j \in q_j$ для которых $p_j(\xi) \neq 0$. Поскольку все q_j являются идеалами, то произведение $p = \prod_{s=1}^{m} p_s$ является их общим элементом и, следовательно, принадлежит идеалу *I*. Элемент ξ не принадлежит многообразию *V(I),* проскольку выполняется $p(\xi) = \prod_{s=1}^{m} p_s(\xi) \neq 0$. Следовательно, $V(I) \subseteq \bigcup_{j=1}^{m} V(q_j)$. □

Лемма 15. *Пусть $I \subseteq k[x_1, \dots, x_n]$ — идеал нулевой размерности и $(\xi_1, \dots, \xi_i) \in K^i$ — корень идеала I_i. Тогда существует $\xi_{i+1} \in K$ такой, что $(\xi_1, \dots, \xi_{i+1}) \in K^{i+1}$ — корень идеала I_{i+1}.*
Доказательство. Согласно теореме Ласкера (см. [1]) существует представление идеала I в виде пересечения конечного множества примарных идеалов

$$I = \bigcap_{j=1}^{m} q_i.$$

Напомним, что размерностью идеала называется максимальная из размерностей ассоциированных с его примарными компонентами простых идеалов. Поскольку *I* — идеал размерности ноль, то и все идеалы q_j также нулевой размерности. Очевидно, выполняется равенство

$$I_i = \bigcap_{j=1}^{m} q_{j,i} \qquad (1)$$

где $q_{j,i} = q_j \cap k[x_1, \dots, x_i]$ — примарные идеалы размерности ноль. Поэтому, согласно лемме 14, для всех *i* = 1, . . . ,*n* имеет место разложение

$$V(I_i) = \bigcup_{j=1}^{m} V(q_{j,i}). \qquad (2)$$

Поскольку $(\xi_1, \dots, \xi_i) \in K^i$ — корень идеала I_i, то из представления (2) следует, что при некотором j элемент $(\xi_1, \dots, \xi_i) \in K^i$ является корнем идеала $q_{j,i}$. Поэтому, по лемме 13 существует $\xi_{i+1} \in K$ такой, что $(\xi_1, \dots, \xi_{i+1}) \in K^{i+1}$ — корень идеала $q_{j,i+1}$, а, следовательно, согласно формулам (1) и (2), является корнем идеала I_{i+1}. □

Определение 1. *Размерностью системы алгебраических уравнений называется размерность соответствующего идеала этой системы. Системы алгебраических уравнений размерности ноль будем называть полными.*

Лемма 16. *Пусть $p(x) \in \mathbb{Q}[x]$ — многочлен с рациональными коэф-фициентами от одной переменной. Тогда уравнение p(x) = 0 алгоритмически разрешимо в поле рациональных чисел.*

Поскольку задача нахождения базиса Гребнера идеала *I* относительно произвольного порядка является алгоритмически разрешимой, а по теореме 1 для идеала размерности ноль для каждой переменной x_i существуют многочлены $f_i(x_i)$, зависящие только от этой переменной и принадлежащие идеалу *I*, то задача построения таких многочленов алгоритмически разрешима. Пусть X_i — множество рациональных решений уравнения $f_i(x_i) = 0$. Тогда все рациональные решения системы идеала *I* принадлежат произведению $X_1 \times \dots \times X_n$. Поэтому из леммы 16 следует алгоритмическая разрешимость полной системы алгебраических уравнений над полем $\mathbb{Q}$.

Следствие 3. *Задача нахождения решения полной системы алгебраических уравнений над полем рациональных чисел является алгоритмически разрешимой.*

Для неполных систем уравнений, например, диафантовых уравнений утверждение следствия 3 не получается.

4. Пример системы алгебраических уравнений

Рассмотрим систему алгебраических уравнений

$$\begin{cases} x_1^2 - x_1 = 0 \\ \dots\dots\dots\dots \\ x_{n-2}^2 - x_{n-2} = 0 \\ x_{n-1}^2(n-2-x_1-\dots-x_{n-2}) + \quad x_{n-1}+1 = 0 \\ x_1+\dots+x_n-n+2=0 \end{cases}$$

Эта система уравнений имеет единственное вещественное решение

$$\begin{cases} x_1 = 1 \\ \dots\dots\dots\dots \\ x_{n-2} = 1 \\ x_{n-1} = -1 \\ x_n = 1 \end{cases}$$

Это решение будет получено алгоритмом A, только в том случае, если для первых (n-2) уравнений оракул укажет в качестве решений именно решение

$$\begin{cases} x_1 = 1 \\ \dots\dots\dots. \\ x_{n-2} = 1 \end{cases}$$

Отметим, что общее число решений этой системы равно 2^{n-2}. Базис Гребнера относительно лексикографического порядка совпадает с левыми частями частями уравнений, т.е. имеет ту же сложность, что и описание идеала. В работе [2] был приведен пример идеала, для которого базис Гребнера с экспоненциального размера относительно описания самого идеала. В этом случае алгоритм A всегда приводит к рациональному (целочисленному) решению, поскольку иных решений попросту нет.

Литература.

[1]. Ван дер Варден Б.Л., Алгебра, Москва, Наука, 1976.
[2]. А.В. Шокуров, Сравнение сложностей задач нахождения базиса Гребнера идеала и решений этого идеала. Труды Института системного программирования РАН, том 22, 2012 г. ISSN 2220-6426 (Online), ISSN 2079-8156 (Print), стр. 463-474. DOI: 10.15514/ISPRAS-2012-22-25.
[3]. Faugere J.C., Gianni P., Lazard D., Mora T., Efficient computation of zero-dimensional Grobner bases by change of ordering, Journal of Symbolic Computation, 1993,v.16, issue 4,pp.329-344.

On Solving The Systems of Algebraic Equations Using Gröbner Bases

Alexander Shokurov, shok@ispras.ru
ISP RAS

Abstract. Described and proved the algorithm for finding some solution of algebraic equations over arbitrary field k for zero dimension ideals if Gröbner basis of this ideal over lexicographic order is given. The found Solution lies in the algebraic closure of k. An example for a system of algebraic equations having a unique solution in the main field, and exponentially many solutions of this system is suggested.

Keywords. Gröbner basis, ideal,

References

[1]. B.L. van der Waerden, Algebra I, Achte Auflage der Modernen Algebra, Springer-Verlag Berlin New York 1971. Algebra II, Fünfte Auflage, Springer-Verlag Berlin New York 1967.
[2]. Shokurov A.V., Sravnenie slozhnostej zadach nakhozhdeniya bazisa Groybnera ideala i reshenij e'togo ideala [Comparing complexities of problems of determining of Grebner's basis of ideal and solving this ideal]. Trudy ISP RAN [The Proceedings of ISP RAS], 2012, vol. 22, pp. 463-474. DOI: 10.15514/ISPRAS-2012-22-25. (in Russian)
[3]. Faugere J.C., Gianni P., Lazard D., Mora T., Efficient computation of zero-dimensional Gröbner bases by change of ordering, Journal of Symbolic Computation, 1993,v.16, issue 4,pp.329-344.