Школа современного программирования

Васильев Николай Николаевич

УПРОЩЕНИЕ СИСТЕМ ПОЛИНОМИАЛЬНЫХ УРАВНЕНИЙ И БАЗИСЫ ГРЁБНЕРА

От редакции: статья является продолжением статьи «Как компьютер помогает упрощать алгебраические уравнения, или немного о базисах Грёбнера», опубликованной в предыдущем номере журнала. В первую часть статьи не вошли важные более сложные вопросы обсуждаемой темы, которые включены в данную статью. Также в статью вошли примеры автоматизации доказательства геометрических теорем и вывода сложных формул, основанные на теории базисов Грёбнера.

В предыдущей статье мы познакомились с методами упрощения систем полиномиальных уравнений и пришли к понятию базиса Грёбнера полиномиального идеала. Сейчас мы обсудим почему такой базис существует и конечен. Также будет рассказано и о способах его нахождения.

Как и в предыдущей статье, мы стартуем с произвольной системы полиномиальных уравнений

$$\begin{cases} P_1(x_1, x_2, ..., x_n) = 0 \\ P_2(x_1, x_2, ..., x_n) = 0 \\ ... \\ P_m(x_1, x_2, ..., x_n) = 0 \end{cases}. \qquad (1)$$

Напомним, что набор полиномов

$$\begin{cases} g_1(x_1, x_2, ..., x_n) \\ g_2(x_1, x_2, ..., x_n) \\ ... \\ g_m(x_1, x_2, ..., x_n) \end{cases}$$

называется базисом Грёбнера идеала J, если старший моном любого полинома из идеала J делится на старший моном одного из полиномов g_i. Такой базис называют вполне редуцированным, если ни один из членов любого из полиномов $\{g_i\}$ не делится на старший член никакого другого полинома g_j. Это означает, что мы не можем уже применить алгоритм редукции к полиномам из такого базиса Грёбнера. Еще раз напомним также, что у нас зафиксировано упорядочение мономов, например лексикографическое, так что мы можем выбрать в любом полиноме его старший член.

Сейчас мы докажем одну замечательную лемму, называемую леммой Диксона, которая лежит в основе доказательства как существования, так и конечности редуцированного базиса Грёбнера произвольного идеала J. Заметим, что старшие члены редуцированного базиса Грёбнера идеала J взаимно не делят друг друга. Лемма Диксона утверждает, что все такие множества одночленов конечны. Теперь дадим точную формулировку.

Лемма Диксона.

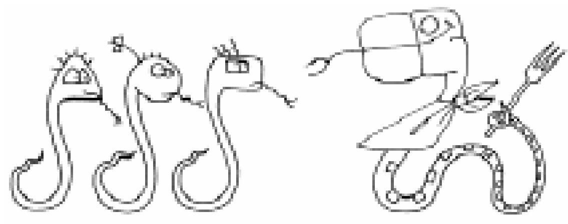
Пусть $T = \{t_1, t_2, t_3, ..., t_n\}$ – произвольное бесконечное множество мономов. Тогда в множестве T существуют два монома t_i и t_j такие, что моном t_i делит моном t_j.

Мы записываем такое отношение делимости так: $t_i \mid t_j$.

Доказательство леммы Диксона будем вести индукцией по количеству переменных. Для мономов от одной переменной, скажем x, утверждение очевидно: для любых двух степеней x^n и x^m меньшая степень делит большую. Пусть теперь утверждение верно для любых бесконечных множеств от k переменных. Возьмем теперь множество $T = \{t_1, t_2, t_3, ..., t_n\}$ мономов от $k+1$ переменных. Допустим, что они попарно друг друга не делят. Рассмотрим первый моном $t_1 = x_1^{n_1} x_2^{n_2} ... x_{k+1}^{n_{k+1}}$. Любой другой моном t из множества T не делит t_1, следовательно его степень по одной из переменных $x_1, x_2, x_3, ..., x_k, x_{k+1}$ строго меньше, чем соответствующая степень в мономе t_1. Разобьем множество T на $(k+1)$ подмножеств T_1, T_2, ..., T_{k+1}. К T_i отнесем те мономы, в которых степень при переменной x_i меньше соответствующей степени в мономе t_1. Если это правило позволяет отнести моном сразу к нескольким подмножествам T_i, то выбираем любое из возможных. Так как наше множество T бесконечно, то бесконечно одно их множеств T_i. В этом множестве мономов степень при переменной x_i строго меньше n_i. Множество T_i можно разбить теперь на n_i подмножеств. В первом из них степень при переменнолй x_i равна 0, во втором 1, а в n_i-ом множестве степень при переменной x_i равна $n_i - 1$. Снова одно из этих множеств бесконечно, но во всех мономах этого бесконечного множества степень при переменной x_i одна и та же. Они могут отличаться только степенями при других переменных. Сократив на эту степень все мономы, мы получим бесконечное множество мономов от k переменных, попарно не делящих друг друга, что противоречит предположению индукции.

Задача 1. Докажите, что лемма Диксона эквивалентна следующему утверждению.

Из любой последовательности мономов $T = \{t_1, t_2, t_3, ..., t_n\}$ можно выбрать бесконечную подпоследовательность $t_{n_1}, t_{n_2}, t_{n_3}, ...$, в которой каждый член делит последующий.



...называется базисом Грёбнера ...,
если старший моном ... делится...

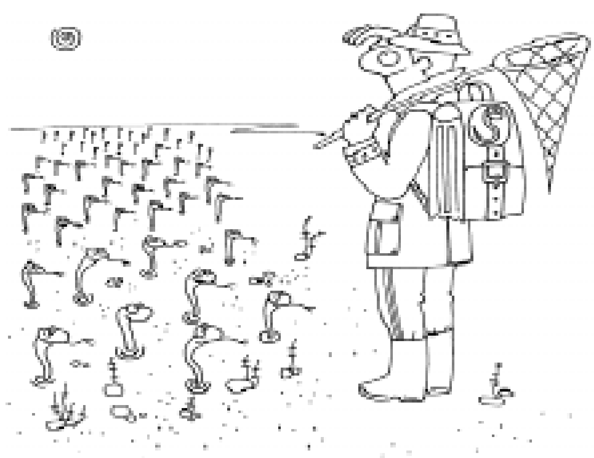
Теперь, вооружившись этой важной теоремой конечности, мы уже сможем доказать одну из важнейших теорем о полиномиальных идеалах. Она была открыта Гильбертом задолго до появления понятия базиса Грёбнера, но на самом деле оказалась эквивалентна существованию и конечности таких базисов для любых полиномиальных идеалов.

Теорема Гильберта о базисе

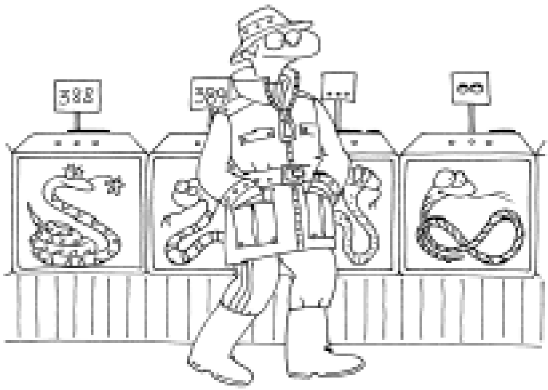
Любой полиномиальный идеал порожден конечным набором полиномов $\{g_i\}_{i=1}^{r}$.

Мы докажем более сильное утверждение, а именно: любой идеал J обладает конечным базисом Грёбнера: $G_r = \{g_1, g_2, g_3, ..., g_r\}$.

Доказательство. Для нашего идеала J рассмотрим бесконечное множество мономов $Mon(J)$, которое состоит из всех старших членов полиномов идеала J. В этом множестве обязаны существовать «минимальные» элементы, которые не делятся сами на другие мономы из множества $Mon(J)$. Действительно, возьмем любой моном $t_1 \in Mon(J)$. Если он не минимален,



...бесконечное множество мономов.



Любой полиномиальный идеал порожден конечным набором полиномов...

то делится на некоторый моном t_2, который в свою очередь делится на t_3 и т.д. Такая цепочка не может быть бесконечной, поэтому она заканчивается минимальным мономом. Все минимальные мономы друг друга попарно не делят, следовательно по лемме Диксона их число конечно. Пусть это множество $\{t_1, t_2, t_3, ..., t_k\}$. Каждый из мономов t_i есть старший член какого-то полинома из J, скажем g_i. Оказывается полиномы $\{g_i\}_{i=1}^{r}$ и образуют базис Грёбнера идеала J. Действительно, каждый полином из J обладает старшим членом из множества $Mon(J)$, который делится на один из минимальных по делимости мономов t_i. Но t_i – старшие члены полиномов $\{g_i\}_{i=1}^{r}$, и мы видим, что эти полиномы в точности удовлетворяют определению базиса Грёбнера.

Теорема доказана.

Отметим, что этот базис не обязан быть вполне редуцированным, но мы можем применить к нему алгоритм редукции и получим вполне редуцированный базис, который, как было доказано в первой части статьи, уже единственен, как только мы зафиксировали упорядочение мономов.

Теперь, наконец-то, мы знаем, что базисы Грёбнера существуют, но вот беда – наше доказательство опять не конструктивно, и никакого алгоритма для его построения мы не указали. Определяющее базисы Грёбнера свойство делимости старших членов полиномов из идеала J на один из старших членов элементов базиса нам не поможет: не можем же мы проверить это свойство для всех элементов идеала J.

Как же все-таки построить базис Грёбнера?

Впервые алгоритм построения базисов Грёбнера был предложен австрийским математиком Б. Бухбергером, который и ввел в математический обиход само это понятие.

Прежде чем говорить об алгоритме построения, мы обсудим более скромную задачу. Пусть нам задан произвольный идеал с помощью какой-либо системы уравнений и набор полиномов, принадлежащих этому идеалу. Как можно проверить, образуют ли они базис Грёбнера этого идеала? Вспомним, что определение базиса требует проверки условия делимости старшего члена любого элемента из идеала на старший член одного из элементов базиса. Так как в идеале бесконечное количество полиномов, то мы в такой формулировке это условие проверить не в состоянии. Давайте попробуем его перевести на алгоритмический язык и немного переформулируем. Тот факт, что старший член любого полинома из идеала J делится на старший член одного из элементов базиса говорит о том, что к любому элементу идеала можно применить алгоритм редукции относительно множества $\{g_1, g_2, g_3, ..., g_r\}$. Результат также принадлежит идеалу J и к нему также можно применить алгоритм редукции. Этот процесс либо должен заканчиваться нулем, либо продолжаться бесконечно. Но ведь смысл редукции состоит в уменьшении старшего члена редуцируемого полинома. Нетрудно понять, хотя все же этот факт и требует небольшого рассуждения, что процесс уменьшения старшего члена не может быть бесконечным. Это накладывает некоторое условие на упорядочение мономов, но лексикографические порядки ему удовлетворяют. Следовательно, любой полином из идеала J редуцируется к нулю с помощью множества $\{g_1, g_2, g_3, ..., g_r\}$. Идея проверки состоит в том, чтобы явно указать такое конечное множество полиномов, для которых надо проверить это условие, так чтобы их редуцируемость к нулю влекла бы за собой редуцируемость к нулю любого элемента идеала. Оказалось, что такое конечное множество полиномов можно построить. Строить его несложно, а вот теорема Бухбергера о том, что их редуцируемость к нулю влечет за собой редуцируемость к нулю всех элементов идеала, довольна сложна, и мы ее здесь примем без доказательства. Что же это за полиномы?

Возьмем произвольную пару (g_i, g_j) элементов из множества $\{g_1, g_2, g_3, ..., g_r\}$. Пусть их старшие члены равны соответственно t_i и t_j, а коэффициенты при этих членах равны c_i и c_j. Мономы t_i и t_j могут иметь общий делитель, который мы обозначаем НОД (t_i, t_j). Образуем теперь из них новый полином, который обозначим $S(g_i, g_j)$ по формуле

$$S(i, j) = \frac{c_j t_j g_i - c_i t_i g_j}{НОД(t_i, t_j)}.$$

Эти полиномы так и называются S-полиномами.

Теперь сформулируем замечательную теорему Бухбергера.

Теорема. Пусть задано упорядочение мономов. Конечное множество полиномов $\{g_1, g_2, g_3, ..., g_r\}$ из идеала J тогда и только тогда образует базис Грёбнера этого идеала для этого порядка, если все возможные S-полиномы $S(i, j)$ редуцируются к нулю относительно множества $\{g_1, g_2, g_3, ..., g_r\}$.

Такое конечное условие уже можно эффективно проверить за конечное число шагов, хотя это очень трудоемкая процедура.

На этой теореме и основан алгоритм построения базиса, который позволяет в принципе любую систему уравнений привести к простейшей канонической форме.

Алгоритм Бухбергера

Пусть идеал задан конечным набором полиномов

$$\begin{cases} P_1(x_1, x_2, ..., x_n) \\ P_2(x_1, x_2, ..., x_n) \\ ... \\ P_m(x_1, x_2, ..., x_n) \end{cases}.$$

Сначала мы попробуем просто редуцировать полиномы P_i относительно друг друга и получим редуцированное множество $G = \{g_1, g_2, g_3, ..., g_k\}$. Теперь проверим, не является ли оно уже базисом Грёбнера. Если да, то процесс останавливается. Если нет, то какой-то из S-полиномов $S(i, j)$ не редуцируется к нулю. Добавляем теперь его редукцию к множеству G в качестве полинома g_{k+1} и снова проводим всевозможные редукции. То, что этот процесс не может продолжаться до бесконечности, также может быть выведено из леммы Диксона. В конце концов мы получим искомый базис Грёбнера.

Отметим здесь, что результат процедуры не зависит от того, в каком порядке мы выбираем S-полиномы и в каком порядке мы проводим возможные редукции. Базис Грёбнера определяется только самим идеалом и выбранным упорядочением мономов.

Однако скорость работы такого алгоритма существенно зависит от этих факторов. Оказалось, что существует много возможностей, для того чтобы ускорить эту процедуру.

Во-первых, оказывается, можно проверять не все возможные S-полиномы, а только удовлетворяющие некоторым дополнительным условиям. Такие условия принято называть критериями, и наиболее мощные

Эти полиномы так и называются S-полиномами.

Базис Гребнера определяется только самим идеалом и выбранным упорядочением мономов.

из таких критериев также были придуманы Бухбергером и называются критериями Бухбергера. При этом приходится доказывать уточнение теоремы Бухбергера, говорящее о том, что редуцируемость только *S*-полиномов, удовлетворяющих критериям, достаточна, для того чтобы множество являлось базисом Грёбнера. Другой возможностью является поиск наилучшей стратегии выбора *S*-полиномов на каждом шаге. Все шаги, которые приводят к нулевым редукциям, в принципе лишние, и хотелось бы как-то предсказывать такой результат заранее. За последние 30 лет было придумано множество самых разнообразных стратегий, и поиски в этом направлении все еще продолжаются.

Какую же информацию можно извлечь из базиса?

Теперь мы уже не только знаем, что такое базис Грёбнера, но даже представляем себе алгоритм, по которому его получает компьютерная программа. К сожалению, сложность построения базиса Грёбнера довольно велика, и мы не будем рекомендовать вам решать на практике системы полиномиальных уравнений, приводя систему к виду базиса Грёбнера с карандашом и листочком бумаги. Это можно сделать лишь в самых простейших случаях. К счастью, существуют мощные компьютерные программы, где этот алгоритм реализован, например MAPLE, MATHEMATIKA, SINGULAR и некоторые другие. Если у вас установлена на компьютере программа MAPLE или MATHEMATIKA, вы можете сделать это на компьютере. Давайте теперь разберемся, какие задачи мы сможем решить, приводя системы уравнений к виду базиса Грёбнера. Оказывается, что, имея перед собой базис Грёбнера, вычисленный для какой-либо системы уравнений, про эту систему и ее решения можно узнать практически все. Мы уже знаем, как определить совместность системы уравнений: базис Грёбнера несовместной системы будет состоять из одной константы 1. То есть наша система окажется эквивалентной одному уравнению 0 = 1.

Если мы интересуемся комплексными решениями, то по базису Грёбнера легко подсчитать количество решений вашей системы. Мы сейчас ограничимся для наглядности случаем двух переменных, но абсолютно также решается этот вопрос и в общем случае.

Возьмем какую-нибудь систему уравнений, например

$$3x^3y + 5xy^6 + 2 = 0$$
$$x^5 + y^5 = 1$$

Вычислим ее базис Грёбнера. Если мы используем для упорядочения мономов упорядочение по общей степени мономов, то результатом будут три полинома:

$$x^5 + y^5$$
$$3x^3y + 5xy^6 + 2$$
$$25y^{11} - 9x^4y - 10x^4 - 6x$$

Посмотрим теперь на их старшие члены. Этими членами будут x^5, xy^6 и y^{11}. Нарисуем теперь на клетчатой бумаге три точки с целочисленными координатами, соответствующие этим мономам. Это будут точки (5; 0), (1; 6) и (0; 11) (рисунок 1).

Теперь подсчитаем все точки с целыми координатами, находящиеся левее и ниже наших отмеченных точек. Нетрудно подсчитать, что их ровно 35. Это означает, что наша система уравнений имеет ровно 35 комплексных решений. Если бы мы использовали другой порядок мономов, то мы могли получить другой базис с другими старшими членами, но вот количество целых точек, находящихся левее и ниже точек, изображающих старшие члены базиса, оказалось бы ровно 35.

Если бы нам необходимо было найти все эти 35 решений, то пришлось бы вычислить лексикографический базис Грёбнера. Мы уже объясняли, что в таком базисе система, имеющая конечное число решений, будет приведена к треугольному виду. Вычислив на компьютере такой базис, вы сразу почувствуете сложность этой процедуры. Еще бы, результат состоит всего из двух полиномов. Первый из них, как и положено, не зависит от переменной x. Он равен

$$-3125y^{30}-1500y^{13}+1500y^{18}-2700y^{14}+$$
$$+3125y^{35}+1350y^{19}-729y^{15}-32+$$
$$+243y^{20}+1350y^{9}-243y^{5}+729y^{10}$$

Как видим, его степень равна ровно 35, и у нас уравнение для y имеет ровно 35 корней.

А вот второе получившееся уравнение способно впечатлить кого угодно (см. рисунок 2).

Тем не менее, как бы страшно оно не выглядело, его структура чрезвычайно проста. Второе уравнение имеет старшим членом 36794462693441470642178675290680506672 5649001902683192x. Остальные члены зависят только от y, и чтобы решить систему надо во второе уравнение подставить 35 корней первого. Каждый раз будет получаться линейное относительно x уравнение, правда с коэффициентом 3679446269344147 0642178675290680506672564900190268319 2.

Мы не будем вам советовать проделать эти вычисления вручную.

А теперь мы покажем, как, используя базисы Грёбнера, можно решать геометрические задачи.

Вывод формул

Давайте попытаемся вывести какую-нибудь формулу, связывающую элементы произвольного треугольника. Попробуем

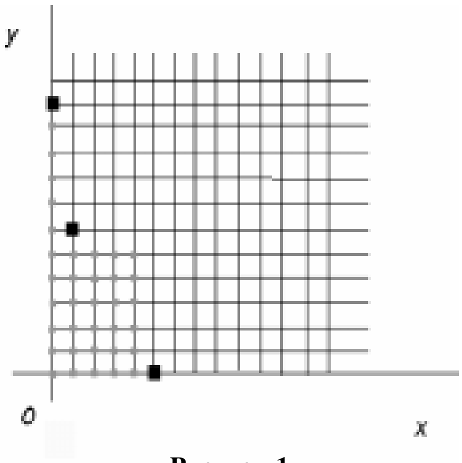


Рисунок 1.

решить такую задачу: выразить площадь треугольника через его высоты. Для этого вспомним известные нам простые формулы.

$$S=\frac{1}{2}h_a a,\quad S=\frac{1}{2}h_b b,\quad S=\frac{1}{2}h_c c$$
$$S=\sqrt{p(p-a)(p-b)(p-c)}$$

Добавим сюда выражение для полупериметра

$$2p=a+b+c$$

Мы получили некоторую систему уравнений, которую можно записать в полиномиальном виде, заменив уравнение для S:

$$S^2=p(p-a)(p-b)(p-c)$$

Вычислим теперь ее базис Грёбнера, так чтобы младшими переменными оказались h_a, h_b, h_c и S.

Одно из уравнений базиса окажется равным

$$h_b{}^4 h_a{}^4 S^4-2h_c{}^2 h_b{}^2 h_a{}^4 S^4+h_c{}^4 h_a{}^4 S^4-$$
$$-2h_c{}^2 h_b{}^4 h_a{}^2 S^4-2h_c{}^4 h_b{}^2 h_a{}^2 S^4+$$
$$+h_c{}^4 h_b{}^4 S^4+h_c{}^4 h_b{}^4 h_a{}^4 S^2$$

Сократив это выражение на S^2, получим искомую формулу

$$S^2=\frac{h_a^4 h_b^4 h_c^4}{2h_c^2 h_b^2 h_a^4+2h_c^2 h_b^4 h_a^2+2_c^4 h_b^2 h_a^2-h_a^4 h_b^4-h_b^4 h_c^4-h_a^4 h_c^4}.$$

Отметим, что мы получили эту формулу, просто исключив ненужные нам переменные в процессе вычисления базиса Грёбнера.

$$
\begin{aligned}
&3679446269344147064217867529068050667256490019026831 92x + \\
&+ 18457980566150441031462963228820288042681185600000000y - \\
&- 478373399178720619326165012350492607196315374940800 00y^4 - \\
&- 1187127261687848932908178699628015334225831757131 00000y^5 + \\
&+ 1475016293249642976377422779648631570690515330000000 00y^6 + \\
&+ 1275135882509770980129837504202984282987393930318855773y^3 + \\
&+ 1229683990717206105320707714803729209935798136039062500y^{11} - \\
&- 2693432915837055863182578041641226958868012753125000 00y^{23} - \\
&- 1663019327008960327936733660188057361636856077940000 00y^{22} - \\
&- 41353085543424887443521943621538852392295771872552484 10y^7 - \\
&- 229529278691284068717086995716706987718037047580000 00y^2 + \\
&+ 4487854652923127253798502669551307298022131269078404660y^{12} + \\
&+ 8440010302600781519861654744393097713783071739105718 75y^{18} + \\
&+ 3983530889601453864204082255447180725242723379325120 23y^{13} + \\
&+ 1827199827768440789761997299920864818543933070968437 50y^{17} + \\
&+ 108186143735118655698001887099014614389974191830000000 0y^{21} - \\
&- 2484345038018692705179854575596784401429132733139062500y^{16} - \\
&- 4702481231361680238976760985922930898258708009560546875y^{33} + \\
&+ 3345026001464375609256495663185167297621749829968750000y^{34} + \\
&+ 4873108756630221837208275582749794993216954108380346875y^{28} - \\
&- 8497539163216235632123759047401095828674717734190000 00y^{27} - \\
&- 785038885302723876628446506017052989787296714233390 00y^{10} + \\
&+ 4427829934814886931743030585940627783675419412806900 00y^9 - \\
&- 2365809859512150586426932483455319705848717586480139671y^8 - \\
&- 1540264934212267797350840701562791284535597977346875000y^{20} - \\
&- 1466775518490861285719272803735592836579270965622120 00y^{15} + \\
&+ 4908556171365022753423119859463706087679353187500000 00y^{32} - \\
&- 6207601328445676492245736729117915434370797343686000 00y^{14} - \\
&- 4136742787355922126727337083675526850857957812500000 00y^{31} + \\
&+ 4056503452430590549680913455728201086275118966500000 00y^{26} + \\
&+ 4592489754745131315257299093383123346717471654406250 00y^{30} + \\
&+ 1417544508950925268306336664932085108385489821353125000y^{25} + \\
&+ 7719235257585343257993976712307411032043219485312500 00y^{29} - \\
&- 3943318746679694151635746319537033237761775129312500 000y^{24} + \\
&+ 1252816091626567495324997536323971006897569586221200 00y^{19} - \\
&- 19121961277149639001581974898205471805982052725888000.
\end{aligned}
$$

Рисунок 2.

Рассмотрим теперь следующую задачу. Пусть на плоскости заданы своими уравнениями три окружности. Как по координатам их центров и их радиусам определить, имеют ли они общую точку. Сделаем одно упрощение: поместим центр первой окружности в начало координат, а ее радиус положим равным 1.

Выпишем теперь уравнения трех окружностей.

$$
\begin{aligned}
&x^2 + y^2 - 1 = 0 \\
&(x - x_1)^2 + (y - y_1)^2 - r_1^{\,2} = 0 \\
&(x - x_2)^2 + (y - y_2)^2 - r_2^{\,2} = 0
\end{aligned}
.
$$

Попробуем определить, при каких условиях эта система не имеет даже комплексных решений.

Вместо того, чтобы решать эти уравнения, мы найдем базис Грёбнера этой

$$
\begin{aligned}
P = {} & {y_1}^2{y_2}^4 - 2y_2{x_2}^2y_1{x_1}^2 - 2x_1 2{x_2}^2r_2^2 + 2y_2{x_2}^2y_1{r_1}^2 - 2x_1x_2 3y_1 2 - 2y_2x_2 2y_1 3 - \\
& - 2y_2 2y_1 2r_2 + 2x_1 2x_2 2y_2^2 - 2x_1 2r_2 2 + 4x_1 2_2 2 + x_1 2 - 2x_1r_2 2x_2r_1 2 - 2x_2x_1y_2^2y_1^2 - \\
& - 2y_1y_2 + 2x_1x_2^3r_1^2 - 2y_2^2x_2x_1^3 + x_2^4y_1^2 - 2x_1x_2 + x_2^2y_1^4 + 2x_2y_1^2x_1r_2^2 + y_1^2r_2^4 + 2y_1^2x_2^2y_2^2 - \\
& - 2x_2^2r_2^2y_1^2 + 2y_2^2x_2x_1r_1^2 - 2x_2^2y_1^2r_1^2 + 2y_2y_1^3r_2^2 + 2y_2y_1x_1^2r_2^2 + y_2^2x_1^4 + y_2^2y_1^4 + y_2^2r_1^4 + \\
& + 2y_2^2x_1^2y_1^2 + 2y_1r_1^2y_2^3 - 2y_2^2x_1^2r_1^2 - 2y_2^2y_1^2r_1^2 + x_1^2y_2^4 - 2y_1^3y_2^3 + 2x_2^2x_1^2y_1^2 + 2x_2x_1^3r_2^2 + \\
& + y_1^2 - 2y_1x_1^2y_2^3 - 2x_1^2y_2^2r_2^2 + x_2^2x_1^4 - 2x_2^2x_1^2r_1^2 + x_2^2 + y_2^2 + x_2^2r_1^4 - 2y_2y_1r_1^2r_2^2 - \\
& - 2x_2x_1y_2^2 - 2y_2x_1^2y_1 - 2y_2y_1x_2^2 + 2y_2y_1r_1^2 - 2y_2y_1^3 + 8x_2x_1y_1y_2 - 2x_2^3x_1 + 2x_2x_1r_2^2 + \\
& + 2y_2y_1r_2^2 - 2y_1y_2^3 - 2x_2x_1y_1^2 + 2x_2x_1r_1^2 - 2x_2x_1^3 + 4y_1^2y_2^2 - 2y_1^2r_2^2 + x_1^2r_2^4 - 2r_1^2x_2^2 - \\
& - 2r_1^2y_2^2 - 2x_1^3x_2^3 + x_1^2x_2^4
\end{aligned}
$$

Рисунок 3.

системы, расположив переменные лексикографически в следующем порядке $(x_1, x_2, r_1, r_2, x, y)$.

Базис Грёбнера этой системы, содержит один полином, не содержащий переменных x и y.

Вспомним, что если в принципе возможно исключить переменные из системы уравнений, то лексикографический базис Грёбнера будет содержать уравнение с исключенными переменными.

Этот полином имеет вид (см. рисунок 3).

$P = 0$ служит необходимым условием разрешимости уравнений.

Формула не выглядит простой, но ведь мы ее получили, не решая уравнений!

Если бы мы положили переменные $x_1 = x_2$ и $y_1 = y_2$, то, очевидно, что наша геометрическая задача имела бы решение только в том случае, если $r_1 = r_2$. А что бы сказал нам базис Грёбнера?

Заменим в системе уравнений переменные x_2 и y_2 на x_1 и y_1.

Снова вычислим базис. Он теперь содержит полином ${r_1}^2 - {r_2}^2$. Конечно, его равенство нулю есть необходимое условие наличия общей точки.

Заключение

Мы познакомились с очень мощным средством упрощения систем полиномиальных уравнений – теорией базисов Грёбнера. На сегодня это самый сильный алгоритмический метод решения и исследования систем полиномиальных уравнений. Он позволяет полностью исследовать множество решений системы и в случае, если система имеет конечное число решений, – найти эти решения. Умело применяя это средство, можно исключать переменные из систем, выводить новые формулы и решать множество других, самых разнообразных задач.

Васильев Николай Николаевич,
кандидат физико-математических наук, старший научный сотрудник Санкт-Петербургского отделения Математического института им. В.А. Стеклова.