Компьютерная алгебра
(курс лекций)

Игорь Алексеевич Малышев
Computer.Algebra@yandex.ru

Лекция 10

Каноническое упрощение полиномиальных уравнений

Содержание лекции

- Задача полиномиального упрощения
- Редукция полиномов
- Базисы Грёбнера
- Решение системы полиномиальных уравнений
- Алгоритм Бухбергера

План лекции: тема подраздела

- **Задача полиномиального упрощения**
- Редукция полиномов
- Базисы Грёбнера
- Решение системы полиномиальных уравнений
- Алгоритм Бухбергера

Задача полиномиального упрощения

Сущность полиномиального упрощения

Сущностью полиномиального упрощения является
построение решения систем полиномиальных уравнений.
(В общем случае, рассматриваются полиномы от нескольких переменных).

Системы полиномиальных уравнений являются соотношениями,
которым должны удовлетворять различные изменения
состояний динамических объектов.

Пример. Положение механической структуры,
образованной двумя сегментами длин 1 и 2 соответственно,
соединёнными в одной точке, определяется девятью переменными
(три точки по три координаты каждая) с помощью системы из двух уравнений:

$$(x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2 = 1$$
$$(x_1 - x_3)^2 + (y_1 - y_3)^2 + (z_1 - z_3)^2 = 4$$

Замечание. Выбранное для объекта представление не является единственным

Задача полиномиального упрощения

Подзадачи полиномиального упрощения

Таким образом, обобщённо, задача полиномиального упрощения
состоит из трёх взаимосвязанных подзадач:

(1) Выбор исходного представления для системы полиномиальных уравнений.

(2) Построение системы (элементарных) преобразований
одного (более сложного) представления для получения
другого (более простого) представления.

(3) Выбор из построенной системы преобразований списка соотношений,
выполняющих направленные (т.е. упорядоченные определённым образом),
преобразования исходного представления
к упрощённому (в некотором смысле) представлению,
причём гарантирующие (с помощью конструктивных процедур проверки)
эквивалентность таких преобразований.

Задача полиномиального упрощения

Полиномиальный идеал

Известно, что **идеалом** в полугруппе называется множество, замкнутое относительно полугрупповой операции (обычно называемой умножением), причём умножение на любой его элемент приводит к элементу этого множества.

Семейством образующих идеала называется множество элементов, умножением на которые элементов полугруппы можно получить все элементы идеала.

Конкретизируя вышеуказанные определения на случай кольца полиномов, имеем:

Определение. Идеалом, порождённым семейством образующих, называется множество линейных комбинаций этих образующих с полиномиальными коэффициентами.

Определение. Полиномы f и g называются эквивалентными относительно идеала I , если $(f - g) \in I$.

Задача полиномиального упрощения

Уточнённая постановка задачи

Если мы рассматриваем образующие идеала как полиномы, которые мы приравниваем нулю,
то последнее из вышеприведённых определений утверждает, что рассматриваемые полиномы не различаются.

Поэтому для получения решения задачи полиномиального упрощения требуется исследовать следующие вопросы:

(1) Как определить идеал ?

(2) Как выяснить, эквивалентны ли два полинома относительного данного идеала ?

План лекции: тема подраздела

- Задача полиномиального упрощения
- **Редукция полиномов**
- Базисы Грёбнера
- Решение системы полиномиальных уравнений
- Алгоритм Бухбергера

Редукция полиномов

Простота системы образующих идеала – 1

Очевидно, что у одного и того же идеала
существует несколько систем образующих.
(Всегда можно добавить любую линейную комбинацию образующих
или удалить одну из них,
если она является линейной комбинацией остальных).

Важный вопрос: существует ли **простая** система образующих ?

Для правильного ответа требуется уточнить, что означает «простая».

Покажем, что простота зависит от типа отношения порядка на мономах, определённого для полиномов.

Редукция полиномов

Простота системы образующих идеала – 2

Рассмотрим полиномы от переменных x_1 , x_2 , … , x_n ,
коэффициенты которых принадлежат некоторому полю F
(иными словами, такие коэффициенты можно складывать, вычитать, умножать и делить).

Введём на множестве мономов некоторое отношение порядка, обозначаемое символом $<$
и удовлетворяющее двум следующим условиям:

(1) Для любых мономов a , b , c из соотношения $a < b$, следует $a\,c < b\,c$.
(2) Для любых мономов a , b , если $b \neq 1$, то $a < a\,b$.

Легко проверить, что вышеприведённым условиям удовлетворяют три отношения порядка:

(1) лексикографический;
(2) общей степени, затем лексикографический;
(3) общей степени, затем обратный лексикографический.

Редукция полиномов

Понятие «редукция полинома» – 1

Любой ненулевой полином можно представить в порядке убывания (заданном отношением <) своих мономов.

$$a_1 X_1 + a_2 X_2 + \ldots + a_i X_i + \ldots + a_n X_n \qquad \text{для любого } i \ a_i \neq 0 \ \text{ и } \ X_{i+1} < X_i$$

При такой записи X_1 называется старшим мономом, $a_1 X_1$ – старшим членом полинома.

Пусть G – конечное множество полиномов (система образующих полиномиального идеала) и < – фиксированный порядок, удовлетворяющий сформулированным выше условиям.

Определение 1. Полином f **редуцирован относительно** G , если ни один старший моном элемента множества G не делит старшего монома полинома f .

Иными словами, старший моном никакой из линейных комбинаций следующего вида:

$$f - h\, g_i \qquad g_i \in G,\ h \text{ – произвольный полином}$$

полинома f и элемента множества G не меньше (относительно порядка <) старшего монома полинома f .

Понятие «редукция полинома» – 2

Таким образом, утверждение «полином f редуцирован относительно G» эквивалентно тому, что «степень» полинома f не может быть понижена вычитанием из него произведения $h\,g_i$, где $g_i \in G$, h – произвольный полином.

Если полином f нередуцирован относительно G,
то из него можно вычесть кратное некоторого элемента множества G
(а именно: $h\,g_i$, где $g_i \in G$, h – произвольный полином),
(чтобы исключить его старший моном)
так, что в результате получится новый полином:

$$f_1 = f - h\,g_i$$

старший моном которого меньше, чем старший моном полинома f .

Переход от f к f_1 называется **редукцией** f относительно G.

Полиномы f и f_1 эквивалентны относительно идеала, порождённого множеством G.

Пример редукции полинома

Пример.

Пусть

$$G = \{ g_1 = x - 1 , g_2 = y - 2 \}$$
$$f = x y$$

Тогда имеются две возможные редукции полинома f относительно G :

(1) Редукция с помощью g_1 , в результате применения которой получим:

$$f - y g_1 = x y - y (x - 1) = x y - y x + y = + y$$

(2) Редукция с помощью g_1 , в результате применения которой получим:

$$f - x g_2 = x y - x (y - 2) = x y - x y + 2 x = + 2 x$$

Редукция полиномов

Цепочки редукций полинома

Последовательные редукции
образуют **цепочку редукций** для f относительно G.

Как видно из вышеприведённого примера такая цепочка,
вообще говоря, не является единственной.

Очевидно, что полином f не может иметь бесконечной цепочки редукций,
поэтому всякая цепочка редукций в конце концов
приводит к редуцированному полиному.

Очевидно, что для каждого нередуцированного полинома
существует конечная цепочка редукций,
приводящего его к редуцированному полиному.

Редукция полиномов

«Запасной» метод редукции полинома

Ранее введённое определение редуцированного полинома :

(1) включает в себя понятие старшего монома полинома f,
(2) требует, чтобы ни у какой линейной комбинации $f_1 = f - h\, g_i$ старший моном не был меньше, чем у f .

Однако возможны следующие случаи:

(1) Если полином f ранее был редуцирован, то (по определению) полинома f_1 не существует, т.е. с помощью G нельзя исключить из f старший моном.

(2) В полиноме f существуют другие (не старшие) мономы, которые могут быть исключены, чтобы сделать линейную комбинацию «меньшей».

Редукция полиномов

Применение «запасного» метода редукции

Пример. Пусть переменные x и y подчинены лексикографическому порядку $y < x$
$G = \{ g_1 = y - 1 \}$
Тогда полином $f = x + y^2 + y$ редуцирован относительно G
(его старший моном равен x).

Вместе с тем из полинома f можно исключить мономы y^2 и y относительно G .

Действительно, умножая $g_1 = y - 1$ на y и вычитая полученное произведение из f , получим:
$f^*_1 = f - y\, g_1 = x + 2y$

Далее, умножая $g_1 = y - 1$ на 2 и вычитая полученное произведение из f^*_1 , получим:
$f^*_2 = f^*_1 - 2 g_1 = x - 2$

Таким образом, с помощью следующей цепочки редукций: $f \to f^*_1 \to f^*_2$
получим полином с «меньшей линейной комбинацией».

Редукция полиномов

Вполне редуцированный полином

Полином f называется **вполне редуцированным** относительно G,
если ни один моном полинома f
не делится
ни на один старший моном элемента множества G.

Замечание. Свойство «вполне редуцированности»
является более сильным,
чем свойство «редуцированности».

План лекции: тема подраздела

- Задача полиномиального упрощения
- Редукция полиномов
- **Базисы Грёбнера**
- Решение системы полиномиальных уравнений
- Алгоритм Бухбергера

Базисы Грёбнера

Определение стандартного базиса

Очевидным следствием предшествующих рассуждений является тезис о том,
что систему образующих G (называемую также **базисом**) идеала I
могут составлять различные наборы элементов.

Поэтому поставим задачу –
выбор системы образующих наилучшим (в некотором смысле) образом.

Определение. Система образующих G идеала I называется **стандартным базисом**
(**базисом Вольфганга Грёбнера**) (относительно порядка <),
если в результате <u>любой редукции</u> элемента f идеала I
к редуцированному полиному относительно G всегда получается нуль.

Определение (эквивалент предыдущего)**.** Стандартным базисом
называется такое множество G образующих рассматриваемого идеала I,
что любой полином f обладает единственной редуцированной относительно G формой.

Пример построения стандартного базиса – 1

Замечание 1. В случае наличия у идеала стандартного базиса говорят, что редукция относительно G обладает свойством Чёрча – Россера.

Замечание 2. Стандартные базисы идеала, как правило, дают нам гораздо больше информации об этом идеале, чем любые другие базисы.

Пример. Рассмотрим идеал I, порождённый тремя полиномами:

$g_1 = x^3 y z - x z^2$

$g_2 = x y^2 z - x y z$

$g_3 = x^2 y^2 - z$

Дополнительно заметим, что для кольца полиномов (т.е. для исходной постановки задачи полиномиального упрощения) множество, на котором обращаются в нуль все полиномы идеала, определяется порождающими полиномами.

Очевидно, что при $x = y = z = 0$ все три полинома обращаются в нуль.
Но не очевидно: есть ли другие решения ?

Пример построения стандартного базиса – 2

Стандартный базис идеала I
(относительно лексикографического упорядочения $z < y < x$)
образуют следующие полиномы:

$g_2 = x y^2 z - x y z$
$g_3 = x^2 y^2 - z$
$g_4 = x^2 y z - z^2$
$g_5 = y z^2 - z^2$
$g_6 = x^2 z - z^3$

Заметим, что полиномы g_2 и g_3 уже были определены ранее,
а полиномы g_4 , g_5 и g_6 были добавлены.

Мы не будем доказывать стандартность построенного базиса,
но заметим, что число элементов стандартного базиса
может быть больше числа элементов исходного базиса.

Базисы Грёбнера

Пример построения стандартного базиса – 3

Ввиду следующих представлений (полученных с помощью факторизации):

$g_2 = x\,y\,z\,(y - 1)$
$g_3 = x^2 y^2 - z$
$g_4 = z\,(x^2 y - z)$
$g_5 = z^2\,(y - 1)$
$g_6 = z^2\,(x^2 - z)$

ясно, что $g_1 = x\,z\,(x^2 y - z) = z\,g_4$

С другой стороны, одновременное обращение в нуль полиномов стандартного базиса (т.е. $g_2 = 0$, $g_3 = 0$, $g_4 = 0$, $g_5 = 0$, $g_6 = 0$) возможно в двух случаях:

(1) либо $z = 0$, и тогда должно быть $x\,y = 0$
(т.к. полиномы редуцируются к $x^2 y^2$ и поэтому $x = 0$ или $y = 0$)

(2) либо $z \neq 0$, и тогда должно быть $y = 1$ и $x^2 - z = 0$
(т.к. полиномы редуцируются к $y = 1$ и $x^2 = z$)

Пример построения стандартного базиса – 4

Итак, множество нулей следующей системы:

$$\{ g_2 = 0 , g_3 = 0 , g_4 = 0 , g_5 = 0 , g_6 = 0 \}$$

имеет вид:

$$\{ (x , y , z) \mid (x y = 0 \wedge z = 0) \vee (x^2 - z = 0 \wedge y = 1) \}$$

Иными словами, это множество состоит из :

(1) двух прямых $x = 0$ и $y = 0$ в плоскости (x , y)
и
(2) одной параболы $z = x^2$ в плоскости $y = 1$, параллельной координатной плоскости (x , z)

Базисы Грёбнера

Теоремы о стандартных базисах – 1

Теорема 1. Любой идеал обладает стандартным базисом (относительно любого порядка, удовлетворяющего сформулированным выше условиям).

Определение. Редуцированным базисом называется базис, каждый полином которого вполне редуцирован относительно всех остальных.

Это ограничение необходимо, чтобы исключить тривиальности следующего типа: два базиса $\{ x - 1 , (x - 1)^2 \}$ и $\{ x - 1 \}$ различаются лишь тем, что первый из них не редуцирован (после редукции он превращается во второй).

Теорема 2. Два идеала равны тогда и только тогда, когда они имеют один и тот же редуцированный стандартный базис (относительно одного и того же порядка).

Базисы Грёбнера

Теоремы о стандартных базисах – 2

Замечание. Теорема 2 даёт каноническое представление идеалов
(как только мы фиксируем порядок)

Теорема 3. Система полиномиальных уравнений несовместна

(т.е. не может быть удовлетворена,
даже если допустить алгебраические расширения –
например, над полем комплексных чисел **C**)

тогда и только тогда, когда соответствующий стандартный базис

(относительно любого порядка,
удовлетворяющего сформулированным выше условиям)

содержит константу.

План лекции: тема подраздела

- Задача полиномиального упрощения
- Редукция полиномов
- Базисы Грёбнера
- **Решение системы полиномиальных уравнений**
- Алгоритм Бухбергера

Решение системы полиномов

Теорема о числе решений системы

Если необходимо знать,
конечно ли число решений системы полиномиальных уравнений,
полезно следующее утверждение:

Теорема. Система полиномиальных уравнений в поле комплексных чисел **C**
имеет не более конечного числа решений,

(т.е. если имеет решения, то их число конечно,
однако может не иметь ни одного решения)

если каждая переменная появляется изолированно (например, как z^n)
в одном из старших членов соответствующего стандартного базиса
относительно лексикографического порядка.

Решение системы полиномов

Метод определения решений – 1

При выполнении условий сформулированной выше теоремы
мы можем определить все решения системы с помощью следующего метода.

Пусть имеющиеся переменные $x_1, x_2, \ldots, x_{n-1}, x_n$ упорядочены,
т.е. $x_n < x_{n-1} < \ldots < x_2 < x_1$

По условию переменная x_n появляется одна в старшем члене одного из полиномов,
входящих в стандартный базис (полином является образующей базиса).

Поскольку все остальные члены старше (в смысле отношения $<$),
чем этот член, то они не могут содержаться в этом базисном полиноме.
(Напротив, в нём могут содержаться лишь x_n в различных степенях
и числовые коэффициенты).

Таким образом, у нас есть полином от x_n,
(причём только один, потому что при наличии двух полиномов
мы всегда можем редуцировать один из них относительно другого),
который имеет только конечное число корней.

Если степень рассматриваемого полинома k, то получим не более k различных корней в $\mathbf{C}$.

Решение системы полиномов

Метод определения решений – 2

Теперь определим тот полином стандартного базиса,
в котором появляется изолированно x_{n-1} в его старшем члене.
Пусть степень переменной x_{n-1} в старшем члене равна k .

Тогда, в силу отношения упорядочения переменных,
в остальных членах такого полинома
могут содержаться лишь переменная x_{n-1} (в степени меньшей, чем k)
и, возможно, переменная x_n (т.к. мы пользуемся лексикографическим порядком).

Для каждого возможного значения переменной x_n ,
имеем в общем случае не более k_1 возможных значений переменной x_{n-1}
(т.е. корней рассматриваемого полинома относительно x_{n-1}),
где k_1 – степень этого полинома по переменной x_{n-1} .

Замечание. Указав «не более k» , предполагаем, что могут быть кратные корни
(которые уменьшают общее количество различных корней)

Решение системы полиномов

Метод определения решений – 3

Совместно рассматривая два выше построенных базисных полинома,
получим что общее число допустимых значений пары (x_{n-1} , x_n)
не больше, чем произведение $k_1 * k$.

Замечание. Возможно, что имеются другие полиномы от x_{n-1} и x_n
и что некоторые комбинации значений x_{n-1} и x_n
не удовлетворяют этим полиномам
и потому должны быть отброшены,
однако, наверняка, имеется только конечное число возможностей для x_{n-1} и x_n .

Продолжая аналогичные вышеприведённым
рассуждения о переменных x_{n-2} , x_{n-3} и т д. до x_1 ,
получим все решения системы полиномов.

Решение системы полиномов

Гипотеза об изолированности переменной

Замечание. Ранее мы предполагали, что каждая переменная появляется изолированно.

Покажем (на примере), что это предположение нельзя заменить на более слабое предположение о том, что каждая переменная появляется в качестве старшей переменной.

Пример. Рассмотрим две переменные x и y, где $x > y$.
Пусть идеал порождён двумя следующими полиномами:
$g_1 = (y - 1)x + (y - 1)$ и $g_2 = y^2 - 1$
образующими стандартный базис (доказательство этого утверждения опускаем).
Однако очевидно, что этот базис не удовлетворяет условиям вышерассмотренной теоремы, т.к. переменная x не появляется изолированно.

Для y имеем два возможных решения: $y = 1$ и $y = -1$.
Если $y = -1$, то «всё нормально»,
т.к. вторая образующая принимает вид $(-2x - 2)$ и обращается в нуль при $x = -1$.
Если $y = 1$, то «всё НЕ нормально»,
т.к. вторая образующая обращается в нуль тождественно,
и в этом случае значение x не определено (т.е. может принимать произвольное значение).

Решение системы полиномов

Размерность множества решений – 1

Замечание. Условия вышерассмотренной теоремы
гарантируют нульмерность множества решений системы образующих идеала.
Однако в общем случае определение искомой размерности – непростая задача.

Для вышерассмотренной теоремы имеется очевидное обратное утверждение:

Утверждение. Идеал имеет размерность, отличную от нуля,
тогда и только тогда, когда имеется переменная,
которая не появляется как единственная (изолированная) переменная
ни в одном из старших членов стандартного базиса
(относительно лексикографического порядка).

Естественно предположить,
что число таких переменных определяет размерность идеала

(равна 1, если существует кривая, на которой обращаются в нуль все полиномы)
(равна 2, если речь идёт о поверхности и т.д.).

Но эта гипотеза не верна. Покажем это (на примере).

Размерность множества решений – 2

Пример. Пусть имеем два следующих идеала:

$I_1 = \{ x^2 - 1 , (x - 1) y , (x + 1) z \}$
$I_2 = \{ x^2 - 1 , (x - 1) y , (x - 1) z \}$

Их стандартные базисы относительно лексикографического порядка $z < y < x$ суть

$I_1 = \{ x^2 - 1 , (x - 1) y , (x + 1) z , y z \}$
$I_2 = \{ x^2 - 1 , (x - 1) y , (x - 1) z \}$

В обоих переменная x появляется изолированно,
но ни переменная y , ни переменная z изолированно не появляются.

Однако размерность идеала I_1 равна 1,
т.к. его решения суть две прямые $x = 1 , z = 0$ и $x = -1 , y = 0$.

В то же время размерность идеала I_2 равна 2,
т.к. его решения – это плоскость $x = 1$ и изолированная точка $x = -1 , y = z = 0$.

Решение системы полиномов

Размерность множества решений – 3

Замечание 1. Размерность идеала не превосходит 1,
если для любой пары переменных найдётся элемент базиса Грёбнера,
старший моном которого содержит только эти переменные.

Замечание 2. В общем случае размерность идеала не превосходит k ,
если для любых (k+1) переменных найдётся элемент базиса Грёбнера,
старший моном которого зависит только от этих переменных.

Замечание 3. Более тонкой характеристикой размерности
алгебраического многообразия является его функция (или полином) Гильберта,
степень которого совпадает с размерностью многообразия.
Существуют алгоритмы, вычисляющие полином Гильберта
по известному базису Грёбнера.

План лекции: тема подраздела

- Задача полиномиального упрощения
- Редукция полиномов
- Базисы Грёбнера
- Решение системы полиномиальных уравнений
- **Алгоритм Бухбергера**

Алгоритм Бухбергера

Постановка задачи

По условиям одной из ранее сформулированных теорем,
любой идеал обладает стандартным базисом.

Возникают два вопроса:

(1) Как **вычислить** стандартный базис идеала ?
(2) Как **проверить**, является ли построенный базис идеала стандартным ?

Решение обеих задач можно получить с помощью алгоритма,
предложенного **Бруно Бухбергером**.

Замечание. Далее полагаем, что мы выбрали раз и навсегда порядок мономов,
удовлетворяющий ранее сформулированным условиям.

Алгоритм Бухбергера

Определение S – полинома

Определение. Пусть f и g – два ненулевых полинома
со старшими членами f_p и g_p,
h – их наименьшее общее кратное (НОК).
Тогда S – полином полиномов f и g определяется следующей формулой:

$$S(f, g) = (h f) / f_p - (h g) / g_p$$

Под НОК двух членов или мономов понимается произведение всех переменных, каждая в степени, равной максимуму её степеней в этих мономах.

Замечание. При вычислении НОК старших членов
нужно перемножать не только степени переменных, но и коэффициенты.

Замечание. Определение S – полинома выбирается таким образом,
чтобы старшие члены уменьшаемого и вычитаемого взаимно уничтожились.

Алгоритм Бухбергера

Свойства S – полинома

(1) S – полином – это линейная комбинация полиномов f и g
с полиномиальными коэффициентами (т.к. h / f_p и h / g_p суть мономы).
S – полином принадлежит любому идеалу,
в число порождающих элементов которого входят f и g .

(2) Старшие члены полиномов $(h f) / f_p$ и $(h g) / g_p$ равны,
(они равны старшему члену полинома h)
и потому в формуле S – полинома они взаимно сокращаются.

(3) Справедливы очевидные соотношения:

$$S (f , f) = 0$$
$$S (f , g) = - S (g , f)$$

Алгоритм Бухбергера

Критерий стандартности базиса

Теорема. Базис G является стандартным тогда и только тогда,
когда для любой пары полиномов f и g из множества G
их S – полином S (f , g) редуцируется к нулю относительно G .

Замечание. Приведённая выше теорема не только позволяет проверить,
является ли базис стандартным,
но и определяет путь к построению стандартного базиса.

Чтобы проверить стандартность базиса,
достаточно вычислить все S – полиномы и проверить,
что все они редуцируются к нулю.

Алгоритм Бухбергера

Вычисление стандартного базиса

Теперь поясним идею метода вычисления стандартного базиса
(на основе нестандартного)

Если имеем не стандартный базис, то это в точности означает,
что один из S – полиномов (пусть это будет S (f , g)) не редуцируется к нулю.

Т.к. его редукция является линейной комбинацией элементов множества G ,
можно добавить её к G , не изменив при этом порождаемый идеал.
После этого добавления S (f , g) редуцируется к нулю,
но появляются новые S – полиномы, которые также нужно рассматривать.
Важно, что этот процесс конечен (это факт, доказанный Бухбергером)
и даёт стандартный базис идеала.

Замечание. Идея метода построения стандартного базиса та же,
что и в методе пополнения, рассмотренном в предыдущей лекции.

Алгоритм Бухбергера

Пример построения стандартного базиса – 1

Пример. Пусть $G = \{ g_1 , g_2 , g_3 \}$, $z < y < x$,

$$g_1 = x^3 y z - x z^2$$
$$g_2 = x y^2 z - x y z$$
$$g_3 = x^2 y^2 - z$$

Нужно рассмотреть следующие S – полиномы:

$S (g_1 , g_2)$, $S (g_1 , g_3)$, $S (g_2 , g_3)$

Старшие члены полиномов g_2 и g_3 суть $x y^2 z$ и $x^2 y^2$. Их НОК равен $x^2 y^2 z$. Поэтому

$S (g_2 , g_3) = x g_2 - z g_3 = - x^2 y z + z^2$

Этот полином ненулевой и редуцирован относительно G,
поэтому базис G – не стандартный.
Значит, можно добавить к G этот полином (или противоположный ему: g_4).

Алгоритм Бухбергера

Пример построения стандартного базиса – 2

Теперь G состоит из следующих полиномов:

$$g_1 = x^3 y z - x z^2$$
$$g_2 = x y^2 z - x y z$$
$$g_3 = x^2 y^2 - z$$
$$g_4 = x^2 y z - z^2$$

Нужно рассмотреть обновлённый состав S – полиномов:

$S(g_1, g_2)$, $S(g_1, g_3)$, $S(g_1, g_4)$, $S(g_2, g_4)$, $S(g_3, g_4)$

Заметив, что $g_1 = x g_4$, можно выполнить упрощение (удалив g_1).
При этом идеал, порождённым множеством G , не изменится.

После такого упрощения для рассмотрения остаются только два S – полинома:
$S(g_2, g_4)$ и $S(g_3, g_4)$

Алгоритм Бухбергера

Пример построения стандартного базиса – 3

Далее получим:
$S(g_2, g_4) = x g_2 - y g_4 = -x^2 y z + y z^2$

Получившийся полином можно упростить (добавив g_4), что приводит к $y z^2 - z^2$

Т.к. это не нуль, то базис нестандартный и поэтому необходимо расширить G , добавив новую образующую – g_5 .

Теперь G состоит из следующих полиномов:

$g_2 = x y^2 z - x y z$
$g_3 = x^2 y^2 - z$
$g_4 = x^2 y z - z^2$
$g_5 = y z^2 - z^2$

Нужно рассмотреть обновлённый состав S – полиномов:
$S(g_3, g_4)$, $S(g_2, g_5)$, $S(g_3, g_5)$, $S(g_4, g_5)$

Алгоритм Бухбергера

Пример построения стандартного базиса – 4

Далее получим:

$S(g_3, g_4) = z g_3 - y g_4 = -z^2 + y z^2$

Полученный полином можно редуцировать к нулю (добавив g_5).

Относительно других S – полиномов имеем:

$S(g_2, g_5) = z g_2 - x y g_5 = -x y z^2 + x y z^2 = 0$

$S(g_4, g_5) = z g_4 - x^2 g_5 = -z^3 + x^2 z^2 = x^2 z^2 - z^3$

(заметим, что при последнем переписывании

мономы упорядочиваются по убыванию <)

Полином $S(g_4, g_5)$ уже редуцирован относительно G ,

поэтому G не является стандартным базисом

и необходимо добавить к G этот новый полином (обозначим его g_6).

Алгоритм Бухбергера

Пример построения стандартного базиса – 5

Теперь множество G состоит из следующих полиномов:

$g_2 = x y^2 z - x y z$

$g_3 = x^2 y^2 - z$

$g_4 = x^2 y z - z^2$

$g_5 = y z^2 - z^2$

$g_6 = x^2 z^2 - z^3$

Нужно рассмотреть обновлённый состав S – полиномов:

$S(g_3, g_5)$, $S(g_2, g_6)$, $S(g_3, g_6)$, $S(g_4, g_6)$, $S(g_5, g_6)$

Нетрудно проверить, что G редуцирует все эти S – полиномы к нулю.

Таким образом, $G = \{g_2, g_3, g_4, g_5, g_6\}$
является стандартным базисом данного идеала.

Алгоритм Бухбергера

Критерий Бухбергера

Рассмотренный пример наглядно показывает,
что отыскание стандартного базиса может быть весьма трудоёмко.

Поэтому полезно применять те или иные методы оптимизации алгоритма.

Бухбергер определил критерий
исключающий некоторые S – полиномы из рассмотрения.

Критерий Бухбергера. Если имеется элемент h базиса G ,
такой, что его старший моном делит НОК старших мономов полиномов f и g ,
и, если мы уже рассмотрели S – полиномы S (f , h) и S (h , g) ,
то не обязательно рассматривать S – полином S (f , g) ,
т.к. он будет редуцирован к нулю.

Алгоритм Бухбергера

Выбор S – полиномов

Пока остаётся открытым ещё один важный вопрос –
о наиболее рациональном порядке рассмотрения S – полиномов
для полиномов множества G и о сложности таких вычислений.

В общем случае существует несколько S – полиномов,
которые нужно рассмотреть даже после применения критерия Бухбергера

При любом выборе алгоритм даст один и тот же результат,
но время счёта может быть различным.

Утверждение (Бухбергер). Выбор S – полинома,
НОК старших мономов которого имеет минимальную суммарную степень
(среди всех S – полиномов, которые нужно рассмотреть)
успешно согласуется с критерием Бухбергера.

Алгоритм Бухбергера

Сложность алгоритма – 1

Наличие алгоритма не означает, что легко решить любую задачу.

Доказав конечность предложенного им алгоритма построения стандартного базиса, Бухбергер не оценил:

(1) границ времени счёта;
(2) числа полиномов в стандартном базисе.

Впоследствии было показано, что вычисление стандартного базиса требует в общем случае объёма памяти, **экспоненциально** зависящего от числа переменных n .

Далее проанализируем некоторые оценки сложности алгоритма Бухбергера, которые были получены при $n = 1$, $n = 2$ и $n > 2$.

Алгоритм Бухбергера

Сложность алгоритма – 2

Случай одной переменной ($n = 1$) тривиален.

Замечание. В случае одной переменной и двух полиномов
алгоритм Бухбергера эквивалентен алгоритму Евклида отыскания НОД
этих двух полиномов.

Для **случая двух переменных** ($n = 2$) показано,
что если все данные имеют общую степень, ограниченную числом d ,
то общая степень элементов стандартного базиса ограничена числом ($2d - 1$),
если используется порядок «общей степени» (степенно-лексикографический),
и всегда ограничена числом d^2 .

Более того, число элементов в стандартном базисе ограничено числом ($k + 1$),
где k – минимум общих степеней старших мономов всех данных.

Замечание. Вышеуказанные границы являются лучшими из возможных.

Алгоритм Бухбергера

Сложность алгоритма – 3

Замечание. Для случая нескольких переменных и линейных полиномов алгоритм Бухбергера соответствует методу Гаусса: исключение переменных, приводящее матрицу системы уравнений к треугольному виду.

Т.к. $S(f_1, f_2)$ – линейная комбинация (с постоянными коэффициентами) полиномов f_1 и f_2 , исключающая старшую переменную (здесь следует считать, что $S(f_1, f_2) = 0$, если f_1 и f_2 не содержат одну и ту же старшую переменную).

Полином f_2 редуцируется к нулю относительно f_1 и $S(f_1, f_2)$ и потому он исключается (т.е. может быть отброшен).
Таким образом, переменная исключается из всех уравнений.

Затем вычисления продолжаются со следующей переменной, пока не получим треугольную матрицу.

Замечание. Оценки сложности алгоритма для **случая**, когда **число переменных больше двух** ($n > 2$) не получены.

Алгоритм Бухбергера

Метод повторного исключения

Альтернативой алгоритму Бухбергера
является **метод повторного исключения** (**Джоэль Мозес**, 1966)

Однако (в отличие от алгоритма Бухбергера)
в общем случае могут быть получены не только истинные решения,
но и некоторые **паразитические решения**,
т.е. решения редуцированной системы,
не являющиеся решениями исходной системы.

Замечание. В некоторых случаях исключение может дать
даже несовместные результаты, зависящие от порядка исключения.
Чтобы сделать исключение корректным, необходимо проверить,
что все решения удовлетворяют всем данным уравнениям.
Если уравнения не удовлетворяются, то ещё остаётся возможность,
что истинно некоторое подмножество решения.

Спасибо за внимание !

Вопросы ?