О БАЗИСАХ ГРЕБНЕРА

Хабибова Амира Улугбековна

Самаркандский государственный университет, факультет математики

магистрант

Annotatsiya: Ushbu maqolada polinomial ideallar uchun algoritmli masalalarni yechishga imkoniyat yaratadigan Gryobner bazislari ko‘rilmoqda. Gryobner bazislar usuli ko‘p kuchli kompyuter tizimlarida amalga oshirilgan bo‘lib, amaliy masalalarda paydo bo‘ladigan polinomial ideallarni o‘rganish uchun qo‘llaniladi.

Kalit so‘zlar: Groyber bazisi, polinomial ideallar, Gilbert teoremasi, S-polinom, EKUK.

ABOUT GROEBNER BASIS

Abstract: In this article considered Groebner basis that allow to solve algorithmically problems about polynomial ideals. The method of Groebner basis is realized in all powerful enough systems of computer algebra and is used for the study of polynomial ideals arising up in the applied problems.

Key words: Groebner basis, polynomial ideals, Hilbert’s theorem, S-polynom, LCM.

Метод базисов Грёбнера реализован во всех достаточно мощных системах компьютерной алгебры и применяется для изучения полиномиальных идеалов, возникающих в прикладных задачах и успешно решены следующие: задача о принадлежности идеалу; задача решения полиномиальных уравнений; задача нахождения базиса Грёбнера над общими полями.

Рассмотрим решение *задачи описания идеала.* Для этого нам будет необходимо определить базисы с «хорошими» (по отношению к алгоритму деления) свойствами. Ключевая идея состоит в том, что как только задано

мономиальное упорядочение, то однозначно определен старший член каждого полинома $f \in k[x_1,\ldots,x_n]$. Тогда для каждого идеала I мы можем определить его *идеал старших членов* следующим образом.

Определение. Пусть $I \subset k[x_1,\ldots,x_n]$- ненулевой идеал.

а) Обозначим через LT(I) множество старших членов элементов из I, т.е. LT(I)={ cx^α : существует $f \in I$ и LT(f)=cx^α }.

б) Обозначим через <LT(I)> идеал, порожденный элементами из LT(I).

Пусть I конечно порожден, $I = < f_1, f_2,..., f_s >$. Тогда

< LT(f_1),…,LT(f_s) > и < LT(I) > могут быть *разными* идеалами.

LT(f_i) $\in$ LT(I) $\subset$ < LT(I) >; поэтому < LT(f_1),…,LT(f_s) > $\subset$ < LT(I) >. Однако < LT(I) > может быть строго больше.

< LT(I) > - мономиальный идеал. В частности, это означает, что < LT(I) > порожден конечным множеством старших членов.

Пусть $I \subset k[x_1,...,x_n]$ - некоторый идеал, и пусть < LT(I) > - его идеал старших членов. Мы считаем, что заданно некоторое мономиальное упорядочение, используемое в алгоритме деления.

Теорема. (теорема Гильберта о базисе [2]) Каждый идеал $I \subset k[x_1,...,x_n]$ является конечно порожденным, т.е. $I =< g_1,...,g_s >$, *где* $g_1,...,g_s \in$ I.

Базис $\{g_1,...,g_s\}$ из теоремы не только дает описание идеала, он обладает еще и специальным свойством < LT(I) > = < LT(g_1),…,LT(g_s) > .

Определение. Пусть задано мономиальное упорядочение. Конечное подмножество G = $\{g_1,...,g_s\}$ элементов идеала I называется его базисом Гребнера (или стандартным базисом), если < LT(g_1),…,LT(g_s)> = < LT(I) >.

Следствие. Пусть задано некоторое мономиальное упорядочение. Тогда любой ненулевой идеал $I \subset k[x_1,...,x_n]$ обладает базисом Грёбнера. Более того, базис Грёбнера идеала I является его базисом.

Предложение. Пусть G = $\{g_1,..., g_s\}$ - базис Грёбнера идеала I$\subset k[x_1,..., x_n]$, *и* пусть $f \in k[x_1,\ldots,x_n]$. Тогда существует единственный полином $r \in k[x_1,\ldots,x_n]$, который обладает следующими двумя свойствами:

а) ни один член полинома r не делится ни на один из старших членов <LT(g_1),…,LT(g_s)>;

б) существует $g \in I$, такой, что $f = g + r$. *То* есть является остатком от деления f на G, не зависящим от порядка делителей в G.

Остаток r называется нормальной формой полинома f. Фактически базисы Грёбнера могут быть охарактеризованы требованием единственности остатка.

Хотя единственность остатка и имеет место, но «частные» a_i, вычисляемые алгоритмом деления $f = a_1g_1 + a_2g_2 + \ldots + a_sg_s + r$, зависят от порядка делителей даже в том случае, когда G – базис Грёбнера.

Следствие. Пусть G=$\{g_1,..., g_s\}$ - базис Грёбнера идеала $I \subset k[x_1,..., x_n]$, *и пусть* $f \in k[x_1,\ldots,x_n]$. Тогда f$\in I$ в том и только в том случае, когда остаток от деления f на G равен нулю.

Свойство, сформулированное в следствии, иногда используется как определение базиса Грёбнера: можно доказать, что G обладает этим свойством в том и только в том случае, когда является базисом Грёбнера.

Остаток от деления полинома f на упорядоченный S-набор F=($f_1,..., f_s$) будет обозначаться $\overline{f}^F$. Если F является базисом Грёбнера идеала $< f_1,..., f_s >$, то его можно рассматривать как (неупорядоченное) множество.

«Препятствием» к тому, чтобы набор $\{ f_1,..., f_s\}$ был базисом Грёбнера, является существование такой полиномиальной комбинации полиномов f_i, что ее старший член не принадлежит идеалу < LT(f_1),…,LT(f_s)>. Это может произойти, например, в том случае, когда в некоторой комбинации $ax^\alpha f_i - bx^\beta f_j$ старшие члены полиномов $ax^\alpha f_i$ и $bx^\beta f_j$ *сокращаются.* Но $ax^\alpha f_i - bx^\beta f_j \in I$,

так что старший член этой комбинации принадлежит <LT(*I*)>. Для изучения сокращений мы определим специальные комбинации.

Определение. Пусть $f, g \in k[x_1,\ldots,x_n]$– ненулевые полиномы.

а) Пусть multideg(*f*)= α и multideg(*g*)= β .Положим $\gamma = (\gamma_1,...,\gamma_n) = \max(\alpha_i, \beta_i)$ для любого *i*. Тогда x^γ называется *наименьшим общим кратным* мономов LM(*f*) и LM(*g*), x^γ = LCM(LM(*f*), LM(*g*)).LCM- аббревиатура английского термина least common multiple.

б) S –*полиномом* от f и g называется комбинация S(*f*, *g*)= $\frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g$.

S-полином S(*f*, *g*) специально «сконструирован» для сокращения старших членов.

Теорема. Пусть I – некоторый полиномиальный идеал. Тогда базис G= $\{g_1,..., g_s\}$ идеала I является базисом Грёбнера в том и только в том случае, когда для всех пар $i \neq j$ остаток от деления $S(g_i, g_j)$ на G (в любом порядке) равен нулю.

Теперь будет решаться следующая задача: как построить базис Грёбнера заданного идеала $I \subset k[x_1,..., x_n]$?

Теорема. Пусть дан некоторый ненулевой полиномиальный идеал $I =< f_1,..., f_s >$. Тогда базис Грёбнера для I может быть построен за конечное число шагов с помощью следующего алгоритма:

Вход: F=($f_1,..., f_s$)

Выход: базис Грёбнера G= $\{g_1,..., g_s\}$ идеала *I*, где $f \subset$ G

G:= F

REPEAT

$G' =$ G

FOR каждой пары {*p*, *q*}, в G' DO

S:= $\overline{S(p,q)}^{G'}$

IF S $\neq 0$ THEN G: =G $\cup \{S\}$

UNTIL G = G'

Базисы Грёбнера, построенные с помощью алгоритма этой теоремы, часто оказываюся избыточными – большими, чем необходимо. Мы можем исключить лишние образующие, используя следующий факт.

Лемма. Пусть G – базис Грёбнера полиномиального идеала I, и пусть $p \in$ LT(p) $\in <$ LT(G-{p}) >. Тогда G - {p} также является базисом Грёбнера для I.

Подберем константы и сделаем все старшие коэффициенты единицами, а также исключим из G все p, такие что LT(p) $\in <$ LT(G - {p}) >.. В результате мы получим *минимальный* базис Грёбнера.

Определение. *Минимальным базисом Грёбнера* полиномиального идеала *I* называется его базис Грёбнера G, такой, что

а) LC(p) = 1 для всех $p \in$ G; б) LT(p) $\notin <$ LT(G-{p}) > для всех $p \in$ G.

Во многих системах компьютерной алгебры реализован алгоритм Бухбергера для вычисления базисов Грёбнера. Эти системы, как правило, находят базис, элементы которого отличаются от элементов редуцированного базиса постоянным множителем. Это означает, что базисы, вычисляемые разными системами, по существу совпадают. Таким образом, полученные результаты легко проверить, переходя от одной системы к другой.

Список литературы:

1. Давенпорт Дж., Сире Й., Турнье Е. Компьютерная алгебра. – М.: Мир,1991.

2. Кокс Д., Литтл Дж., О'Ши Д. Идеалы, многообразия и алгоритмы. – М.:Мир,2000.