Преобразование базиса Грёбнера нульмерного идеала к иному мономиальноальному упорядочению.

Федоров Глеб M33351

Октябрь 2020

1 Оглавление

1.1 Постановка проблемы

1.2 Дополнительная теория

1.3 Алгоритм FGLM

1.4 Примерная архитектура программы

1.5 Используемая литература

2 Постановка проблемы

Дан базис Грёбнера нульмерного идеала, построенный на мономиальном упорядочении m_1. Привести данный базис к иному мономиальному упорядочению m_2.

3 Дополнительная теория

3.1 Исключающий идеал

Определение: Пусть дан $I =< f_1, \dots, f_n >\in F[x_1, \dots, x_n]$. Тогда l-м исключающим идеалом I_l называется идеал в $F[x_{l+1}, \dots, x_n]$, равный $I \cup F[x_{l+1}, \dots, x_n]$.

Теорема(об исключении): Пусть $I \subset F[x_1, x_2, \dots, x_s]$ - идеал и G - его базис Грёбнера по отношению к lex-упорядочению с $x_1 > x_2 > \dots > x_n$. Тогда $\forall l : 0 \leq l \leq n$ множество

$$G_l = G \cap F[x_1, x_2, \dots, x_s]$$

является базисом Грёбнера l-го исключающего идеала I_l.

Доказательство: Зафиксируем l в интервале $(0, n)$. Так как $G_l \in I_l$ по построению, достаточно показать, что

$$< LT(I_l) >=< LT(G_l) >$$

(по определению базиса Грёбнера). Включение в одну сторону очевидно($< LT(G_l) >\in< LT(I_l) >$ по построению). Докажем, что $< LT(I_l) >\in< LT(G_l) >$. Для этого достаточно показать что $LT(f)$, где $f \in I_l$, делится на некоторый $g \in G_l$. Заметим, что $f \in I$, то есть $LT(f)$ делится на $LT(g)$ для некоторго g(т.к. G является базисом Грёбнера иделала I). Так как $f \in I_l$, то $LT(g)$ содержит только переменные $x_{l+1}, \dots, x_n$. Так как используется lex-упорядочении с $x_1 > x_2 > \dots > x_n$, то любой моном, содержащий хотя бы одну из переменных $x_1, \dots, x_l$, больше всех мономов из $F[x_{x+1}, \dots, x_n$. Значит $g \in G_l$, что и требовалось доказать.

3.2 Соответсвие иделала и многообразия

Определение: Пусть $I \in F[x_1, \dots, x_n]$ - некоторый идеал. Положим

$$V(I) = (a_1, \dots, a_n) \in F^n : f(a_1, \dots, a_n) = 0 \forall f \in I$$

Теорема: $V(I)$ является аффинным многообразием. В частности, если $I =< f_1, \dots, f_n >$, то $V(I) = V(f_1, \dots, f_n)$

Доказательство: По теореме Гильберта о базисе идеал I конечно порождён, $I =< f_1, \dots, f_n >$. Покажем, что $V(I) = V(f_1, \dots, f_n)$. Если $f(a_1, \dots, a_n) = 0$ для всех полиномов $f \in I$, то $f_i(a_1, \dots, a_n) = 0$ (так как $f_i \in I$). Следовательно, $V(I) \in V(f_1, \dots, f_n)$. С другой стороны, пусть $(a_1, \dots, a_n) \in V(f_1, \dots, f_n)$, и пусть $f \in I$. Так как $I =< f_1, \dots, f_n >$, то

$$f = \sum_{i=1}^{s} h_i f_i$$

для некоторых $h_i \in F[x_1, \dots, x_n]$. Но тогда

$$f(a_1, \dots, a_n) = \sum_{i=1}^{s} h_i(a_1, \dots, a_n) f_i(a_1, \dots, a_n) = \sum_{i=1}^{s} h_i(a_1, \dots, a_n) * 0 = 0$$

Следовательно, $V(f_1, \dots, f_n) \in V(I)$, а значит эти два идеала равны.

Следствие: Многообразия определены идеалами.

3.3 Нульмерный идеал

Теорема: Пусть поле F алгебраически замкнуто и $I \in F[x_1, x_2, \dots, x_n]$. Тогда следующие условия эквивалентны:

1. Алгебра $A = F[x_1, x_2, \dots, x_n]$ - I конечномерна над F.
2. $V(I) \subset F^n$ конечно.
3. Если G - базис Грёбнера идеала I, то
$$\forall i \exists m_i \geq 0 : x_i^{m_i} = LM(g)$$
для некоторого $g \in G$.
4. Для каждой переменной x_i исключающий идеал $I \cap F[x_1, x_2, \dots, x_n]$ является ненулевым.

Доказательство: Идеал, удовлетворяюзий данной теореме называется нульмерным

4 Алгоритм FGLM

5 Используемая литература

1. http://halgebra.math.msu.su/groebner.pdf

2. Кокс Д., Литтл Дж., О'Ши Д. Идеалы, многообразия, кольца. Стр. 108. Стр. 153.

3. https://www.math.lsu.edu/system/files/Groeb$_presentation_final.pdf$