

Преобразование базиса Грёбнера нульмерного идеала к иному мономиальноальному упорядочению.

Федоров Глеб М33351

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 $I = \langle f_1, \dots, f_n \rangle \in F[x_1, \dots, x_n]$. 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 лех-упорядочению с $x_1 \rangle x_2 \rangle \dots \rangle x_n$. 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

$$\langle LT(I_l) \rangle = \langle LT(G_l) \rangle$$

Включение в одну сторону очевидно ($\langle LT(G_l) \rangle \in \langle LT(I_l) \rangle$ по построению). Докажем, что $\langle LT(I_l) \rangle \in \langle LT(G_l) \rangle$. 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 некоторого g (т.к. G является базисом Грёбнера идеала I). Так как $f \in I_l$, то $LT(g)$ содержит только переменные x_{l+1}, \dots, x_n . Так как используется лех-упорядочение с $x_1 \rangle x_2 \rangle \dots \rangle x_n$, то любой моном, содержащий хотя бы одну из переменных x_1, \dots, x_l , больше всех мономов из $F[x_{l+1}, \dots, x_n]$. Значит $g \in G_l$, что и требовалось доказать.

3.2 Соответствие идеала 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 $I = \langle f_1, \dots, f_n \rangle$, то $V(I) = V(f_1, \dots, f_n)$

Доказательство: По теореме Гильберта о базисе идеал I конечно порождён, $I = \langle f_1, \dots, f_n \rangle$. 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, $V(I) \subseteq V(f_1, \dots, f_n)$. С другой стороны, пусть $(a_1, \dots, a_n) \in V(f_1, \dots, f_n)$, и пусть $f \in I$. Так как $I = \langle f_1, \dots, f_n \rangle$, 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, $V(f_1, \dots, f_n) \subseteq V(I)$, 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, удовлетворяющий данной теореме называется нульмерным

!!!Определение: Пусть нульмерный идеал I над $F[x_1, \dots, x_n]$ и G - его редуцированный базис Грёбнера. Натуральным базисом, определяемым G K -векторного пространства R/I , назовем базис $B(G)$, элементами которого являются приведенные мономы относительно G .

!!!Определение: Пусть $B(G)$ - натуральный базис для R/I . Тогда положим, что

$$M(G) = \{x_i b \mid b \in B(G), 1 \leq i \leq n, x_i b \notin B(G)\}$$

граница G .

Теорема: Пусть I - нульмерный идеал и G - редуцированный базис Грёбнера данного идеала, и $B(G)$ - натуральный базис Грёбнера для R/I , тогда $\forall m \in M(G)$ выполнено одно из данных условий:

1. $\forall x_i : x_i | m, m/x_i \in B(G)$, если m - это старший моном элементов G .
2. $m = x_j m_j$ для некоторых j и $m_j \in M(G)$

Доказательство:

1. Следует из определения редуцированного базиса Грёбнера и определения $B(G)$
2. Пусть x_j делит m и $m/x_j \notin B(G)$, тогда $m_j = m/x_j \in M(G)$.

Следствие: Пусть k число образующих редуцированного базиса Грёбнера для нульмерного идеала. Тогда $k \leq nD(I)$

4 Алгоритм FGLM

4.1 Вычисление нормальной формы

4.2 Смена упорядочения

5 Используемая литература

1. Faugère, J.C., Gianni, P., Lazard, D., Mora, T. Efficient computation of zero-dimensional gröbner bases by change of ordering (1993) Journal of Symbolic Computation, 16 (4), pp. 329-344.
2. <http://halgebra.math.msu.su/groebner.pdf>
3. Кокс Д., Литтл Дж., О'Ши Д. Идеалы, многообразия, кольца. Стр. 108. Стр. 153.
4. https://www.math.lsu.edu/system/files/Groeb_presentation_final.pdf