БАЗИСЫ ГРЕБНЕРА И АЛГОРИТМ БУХБЕРГЕРА

ОПР.

НЕПУСТОЕ ПОДМНОЖЕСТВО I КОЛЬЦА R НАЗЫВАЕТСЯ ИДЕАЛОМ В R ($I \triangleleft R$), ЕСЛИ: 1) $\forall a, b \in I$ ВЫПОЛНЯЕТСЯ $a - b \in I$

2) $\forall a \in I$; $c \in ac \in I$

ПРИМЕР: $2\mathbb{Z}$

ОПР.

ИДЕАЛ КОЛЬЦА НАЗЫВАЕТСЯ ГЛАВНЫМ, ЕСЛИ $\exists a \in I$ | I ПОРОЖДАЕТСЯ ЭЛЕМЕНТОМ a. В ЭТОМ СЛУЧАЕ a - ПОРОЖДАЮЩИЙ ЭЛЕМЕНТ.

ОПР.

КОЛЬЦО R НАЗ-СЯ КОЛЬЦОМ ГЛАВНЫХ ИДЕАЛОВ, ЕСЛИ КАЖДЫЙ ИДЕАЛ ЯВЛЯЕТСЯ ГЛАВНЫМ.

УТВ.

$\exists a_1; \dots; a_k \in R$, ТОГДА $\{a_1; \dots; a_k\} = \{a_1 r_1 + \dots + a_k r_k;\ r_1, r_2, \dots, r_k \in R\} \subset R$ - ИДЕАЛ КОЛЬЦА R.

ОПР.

ЭЛЕМЕНТЫ $a_1; \dots; a_k$ СОСТАВЛЯЮТ БАЗИС ИДЕАЛА $I = \{a_1; \dots; a_k\}$. ГОВОРЯТ, ЧТО $I \triangleleft R$ ДОПУСКАЕТ КОНЕЧНЫЙ БАЗИС, ЕСЛИ В НЁМ НАЙДУТСЯ ТАКИЕ $a_1; \dots; a_k$, ЧТО $I = \{a_1; \dots; a_k\}$

ТЕОРЕМА ГИЛЬБЕРТА О БАЗИСЕ

КАЖДЫЙ ИДЕАЛ $I \triangleleft K[x_1; \dots; x_n]$ ДОПУСКАЕТ КОНЕЧНЫЙ БАЗИС, ТО ЕСТЬ $\exists$ $f_1(x_1; \dots; x_n)$ $f_k(x_1; \dots; x_n)$ | $I = \{f_1 r_1 + \dots + f_k r_k,\ r_1; \dots; r_k \in K[x_1; \dots; x_n]\}$

Со всякой системой алгебраических уравнений можно связать идеал I, порождённый многочленами, отвечающими уравнениям системы.

$$\text{САУ}\begin{cases} P_1(x_1;\dots;x_n)=0 \\ P_2(x_1;\dots;x_n)=0 \\ \end{cases} \longleftrightarrow I=\{P_1(x_1,\dots;x_n);P_2(x_1,\dots;x_n)\dots$$

Утв.

Если $(P_1;\dots;P_m)$ и $(\bar{P}_1;\dots;\bar{P}_k)$ два базиса одного идеала I, тогда САУ $\begin{cases} P_1(x_1;\dots;x_n)=0 \\ P_m(x_1;\dots;x_n)=0 \end{cases}$ и $\begin{cases} \bar{P}_1(x_1;\dots;x_n)=0 \\ \bar{P}_k(x_1;\dots;x_n)=0 \end{cases}$ эквивалентны

Опр.

Многочлен, состоящий из одночлена $P=a x_1^{k_1}\dots x_n^{k_n}$, $a\in\mathbb{K}$ называют одночленом или мономом.

$\exists\ P=\sum a_{i_1\dots i_n} x_1^{i_1}\cdot\ldots\cdot x_n^{i_n}$. Каждому такому одночлену входящему в P можно сопоставить набор $\{i_1,\dots;i_n\}$ целых неотрицательных чисел, который называют набором степеней.

Пример:

$5\cdot x_2^2 x_5 \to (0;2;0;0;1)$

Опр.

Будем говорить, что $(i_1\dots i_n)$ больше $(j_1;\dots;j_n)$, если $k\le n \mid i_1=j_1 \quad i_{k-1}=j_{k-1} \quad i_k>j_k$

ПРИМЕР:

$(2;3;0;7) < (4;0;0;0)$

ОПР.

СТАРШИМ ЧЛЕНОМ МНОГОЧЛЕНА P НАЗЫВАЕТСЯ МОНОМ, НАБОР СТЕПЕНЕЙ КОТОРОГО БОЛЬШЕ НАБОРОВ СТЕПЕНЕЙ ЛЮБОГО ДРУГОГО МОНОМА, ВХОДЯЩЕГО В P.

ЛЕММА О СТАРШЕМ ЧЛЕНЕ

СТАРШИЙ ЧЛЕН ПРОИЗВЕДЕНИЯ ДВУХ МНОГОЧЛЕНОВ = ПРОИЗВЕДЕНИЮ СТАРШИХ ЧЛЕНОВ ЭТИХ МНОГОЧЛЕНОВ.

ЗАМЕЧАНИЕ

СУЩЕСТВУЮТ ДРУГИЕ СПОСОБЫ УПОРЯДОЧЕНИЯ МНОГОЧЛЕНОВ. ИСПОЛЬЗУЕМЫЙ СЕЙЧАС НОСИТ НАЗВАНИЕ „ПРЯМОЕ ЛЕКСИКОГРАФИЧЕСКОЕ УПОРЯДОЧЕНИЕ"

] $P = \underset{\substack{\nearrow \\ \text{старший член}}}{P_c} + P_M \leftarrow$ СУММА ОСТАЛЬНЫХ ЧЛЕНОВ

] СТАРШИЙ ЧЛЕН (h_c) МНОГОЧЛЕНА h ДЕЛИТСЯ НА СТАРШИЙ ЧЛЕН (f_{ic}) НЕКОТОРОГО ИЗ f_i, ТО ЕСТЬ $h_c = f_{ic} \cdot Q$, ГДЕ Q - ОДНОЧЛЕН. ТОГДА ПОЛОЖИМ $h_1 = h - Qf_i = Q(-f_{im}) + h_m$.

ПРИ ЭТОМ $h_{1c} < h_c$. ПРИМЕНЁННАЯ ОПЕРАЦИЯ НОСИТ НАЗВАНИЕ „ОПЕРАЦИЯ РЕДУКЦИИ".

ЗАДАЧА ВХОЖДЕНИЯ

] $I \triangleleft \mathbb{K}[x_1; \dots; x_n]$ ЗАДАН СВОИМ БАЗИСОМ $I = (f_1; \dots; f_m)$. ТРЕБУЕТСЯ НАЙТИ АЛГОРИТМ, ПОЗВОЛЯЮЩИЙ ЗА КОНЕЧНОЕ ЧИСЛО ШАГОВ ОПРЕДЕЛИТЬ ПРИНАДЛЕЖНОСТЬ h ИДЕАЛУ I, ТО ЕСТЬ ВОЗМОЖНОСТЬ ЕГО РАЗЛОЖЕНИЯ В СУММУ: $h = f_1 r_1 + \dots + f_m r_m$

r_i - многочлен $i \in \overline{1;m}$

ОПРЕДЕЛЕНИЕ:

$f_1;\dots;f_m$ называют базисом Грёбнера идеала, если $I=(f_1;\dots;f_m)$, если $\forall h \in I$ редуцируется к 0 при помощи $(f_1;\dots;f_m)$.
или иначе h_c делится на один из f_{ic} $i\in\overline{1;m}$

] $I \triangleleft K[x_1;\dots;x_n]$ - идеал $f_1;\dots;f_m$ - его базис

ОПРЕДЕЛЕНИЕ

говорят, что многочлены f_i и f_j имеют зацепление, если их старшие члены f_{ic} и f_{jc} делятся одновременно на некоторый одночлен w, отличный от константы.

Если f_i и f_j имеют зацепление, то есть $f_{ic}=wq_1$, $f_{jc}=wq_2$, где w - наибольший общий делитель f_{ic} и f_{jc}, то рассмотрим многочлен $F_{ij}=f_iq_2-f_jq_1 \in I$.

Его принято называть S-многочленом пары $f_i;f_j$ и обозначать $S(f_i;f_j)$ или $S(i;j)$. Редуцируем многочлен F_{ij} с помощью базиса $f_1;\dots;f_m$ до тех пор, пока это возможно. В результате получим нередуцированный многочлен $\widetilde{F_{ij}}$. Если $\widetilde{F_{ij}}\equiv 0$, то будем говорить, что зацепление разрешимо. Иначе добавим $\widetilde{F_{ij}}$ к базису идеала $I: f_{m+1}=\widetilde{F_{ij}}$.

В НОВОМ БАЗИСЕ $f_1; \dots; f_{m+1}$ БУДЕМ ИСКАТЬ ВОЗМОЖНЫЕ ЗАЦЕПЛЕНИЯ И РЕДУЦИРОВАТЬ СООТВЕТСТВУЮЩИЕ МНОГОЧЛЕНЫ F_{ij}.

ТЕОРЕМА

$\forall f_1; \dots; f_m \in K[x_1; \dots; x_n]$ ПОСЛЕ РЕДУЦИРОВАНИЯ КОНЕЧНОГО ЧИСЛА ЗАЦЕПЛЕНИЙ МЫ ПОЛУЧИМ $f_1, \dots, f_m, f_{m+1}, \dots, f_M$, В КОТОРОМ КАЖДОЕ ЗАЦЕПЛЕНИЕ РАЗРЕШИМО.

ТЕОРЕМА

БАЗИС $f_1; \dots; f_m$ ИДЕАЛА I ЯВЛЯЕТСЯ БАЗИСОМ ГРЁБНЕРА $\Leftrightarrow$ В НЁМ НЕТ ЗАЦЕПЛЕНИЙ ИЛИ КАЖДОЕ ЗАЦЕПЛЕНИЕ РАЗРЕШИМО.

АЛГОРИТМ БУХБЕРГЕРА

1) ПРОВЕРИМ, ЕСТЬ ЛИ В НАБОРЕ ЗАЦЕПЛЕНИЯ. ЕСЛИ ЗАЦЕПЛЕНИЙ НЕТ, ТО НАБОР ЯВЛЯЕТСЯ БАЗИСОМ ГРЕБНЕРА ИДЕАЛА I, ИНАЧЕ ПЕРЕХОДИМ К ПУНКТУ 2.

2) ПО НАЙДЕННОМУ ЗАЦЕПЛЕНИЮ $(i; j)$ МНОГОЧЛЕНОВ f_i И f_j ПОЛОЖИМ $f_{ic} = wq_1$; $f_{jc} = wq_2$, И СОСТАВИМ МНОГОЧЛЕН $F_{i,j} = f_i q_2 - f_j q_1$. РЕДУЦИРУЕМ МНОГОЧЛЕН F_{ij} РЕДУЦИРОВАЛСЯ К НЕНУЛЕВОМУ МНОГОЧЛЕНУ f, ТО ПЕРЕХОДИМ К П.3, ИНАЧЕ К П.4. (РЕДУЦИРУЕМОСТЬ И ВИД МН-НА f ВООБЩЕ ГОВОРЯ ЗАВИСЯТ ОТ ПУТИ ПРИМЕНЯЕМЫХ РЕДУКЦИЙ). В АЛГОРИТМЕ РАССМАТРИВАЕТСЯ $\forall$ ПРИМЕНИМАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ РЕДУКЦИЙ И, ПОЛУЧИВ НЕРЕДУЦИРУЕМЫЙ МНОГОЧЛЕН f, ПЕРЕХОДИМ К ПУНКТУ 3, БОЛЕЕ НИКОГДА ЗАЦЕПЛЕНИЕ (i, j) НЕ РАССМАТРИВАЯ.

3) ДОБАВЛЯЕМ МНОГОЧЛЕН f К НАБОРУ $f_1; \dots; f_k$ В

КАЧЕСТВЕ f_{k+1} И К П.Ч.

4) В ПОСТРОЕННОМ К НАСТОЯЩЕМУ МОМЕНТУ МН-ВО МНОГОЧЛЕНОВ $\{f_i\}$ РАССМАТРИВАЕТСЯ ЗАЦЕПЛЕНИЕ, КОТ. НЕ БЫЛО РАССМОТРЕНО РАНЕЕ И ПЕРЕХОДИМ К П.2. ЕСЛИ ВСЕ ИМЕЮЩИЕСЯ ЗАЦЕПЛЕНИЯ РАНЕЕ РАССМОТРЕНЫ АЛГОРИТМ ЗАВЕРШЁН.

ОПР.

БАЗИС ГРЁБНЕРА НАЗЫВАЕТСЯ МИНИМАЛЬНЫМ, ЕСЛИ f_{ic} НЕ ДЕЛИТСЯ НА f_{jc} ПРИ $i \neq j$.

ЗАМЕЧАНИЕ:

$\forall$ БАЗИС ГРЁБНЕРА СВОДИТСЯ К МИНИМАЛЬНОМУ ПУТЁМ „ОТБРАСЫВАНИЯ ЛИШНИХ" МНОГОЧЛЕНОВ.

ОПР.

БАЗИС ГРЁБНЕРА НАЗЫВАЕТСЯ РЕДУЦИРОВАННЫМ, ЕСЛИ НИ ОДИН ЧЛЕН МНОГОЧЛЕНА f_i НЕ ДЕЛИТСЯ НА СТАРШИЙ ЧЛЕН МН-НА f_j ДЛЯ ВСЕХ $i, j = 1, \ldots, m$ $i \neq j$.

ТЕОРЕМА:

МИНИМАЛЬНЫЙ РЕДУЦИРОВАННЫЙ БАЗИС ГРЁБНЕРА ОПРЕДЕЛЁН ОДНОЗНАЧНО.

$\triangleright$ ДОКАЗАТЕЛЬСТВО:

1) $\exists$ $f_1, \ldots, f_s$ И $g_1, \ldots, g_t$ – ДВА min БАЗИСА ГРЁБНЕРА ИДЕАЛА I. ПОКАЖЕМ $s = t$ И СТАРШИЕ ЧЛЕНЫ СОВПАДАЮТ С ТОЧНОСТЬЮ ДО ПЕРЕСТАНОВКИ. ТАКЖЕ $\forall$ МНОГОЧЛЕНА КОЭФФИЦИЕНТ ПРИ СТАРШЕМ

ЧЛЕНЕ
СТАРШИЙ
ЧЛЕН
СИЛУ
ДАЛЕ
ВОЗНИ
2)
$\exists$ f_i
НО
ИЗ
ПРО

ЧЛЕНЕ РАВЕН 1. ПО ОПРЕДЕЛЕНИЮ БАЗИСА ГРЁБНЕРА, СТАРШИЙ ЧЛЕН МНОГОЧЛЕНА f_i ДЕЛИТСЯ НА СТАРШИЙ ЧЛЕН g_i ДЕЛИТСЯ НА СТАРШИЙ ЧЛЕН НЕКОТОРОГО f_j. В СИЛУ МИНИМАЛЬНОСТИ $f_1, \dots, f_s$ ИМЕЕМ $j = 1 \Rightarrow f_{ic} = g_{ic}$ ДАЛЕЕ ПРОЦЕСС ПРОДОЛЖАЕТСЯ ПО ИНДУКЦИИ И ПАРЫ ВОЗНИКАЮТ ОДНОВРЕМЕННО $\Rightarrow s = t$.

2)] $f_1, \dots, f_s$ И $g_1, \dots, g_s$ ЯВЛЯЕТСЯ РЕДУЦИРОВАННЫМ.] $f_i - g_i \neq 0$ ДЛЯ НЕКОТОРОГО $i \Rightarrow (f_i - g_i)_c \in I$ ~~ДЕЛИТСЯ~~Я ДЕЛИТСЯ НА g_j ДЛЯ НЕКОТОРОГО $j \neq i$, НО $(f_i - g_i)_c$ ЯВЛЯЕТСЯ НЕСТАРШИМ ЧЛЕНОМ ОДНОГО ИЗ МНОГОЧЛЕНОВ f_i ИЛИ g_i, НО ЭТО ПРИВЕДЁТ К ПРОТИВОРЕЧИЮ С РЕДУЦИРОВАННОСТЬЮ БАЗИСА $\triangleleft$.