

7. Базис Грёбнера (Ширшова)

Исполнение: лексисп. сф. порядок
одночленов в $F[x_1, \dots, x_n]$, по которому старшим
члена. Старшим член произведения
= произведение старших членов в см. §5.4
из [ВЛМ].

Обозн: Если $f \in F[x_1, \dots, x_n]$, то f_c — его старший
член, а $f_n \in F[x_1, \dots, x_n] : f = f_c + f_n$. В этих
обозн. имеем $(fg)_c = f_c \cdot g_c$.

Зам. Существует и другие порядки на мн-ве
одночленов "условные" от-но членов.

Задача Вхожденья: Пусть задан $I \subseteq F[x_1, \dots, x_n]$

задан своим базисом $I = (f_1, \dots, f_m)$. Требуется найти алгоритм, который (за конечное число шагов) определит принадлежит ли элемент m -и $h \in F[x_1, \dots, x_n]$ идеалу I .

Примеры 1) $h = x_2 x_3^2 x_4 - x_1 x_3 x_4^2 \in I =$
 $= (x_1 + x_2, x_3 + x_4)$, т.к. $(x_1 + x_2) x_3^2 x_4 -$
 $- (x_3 + x_4) x_1 x_3 x_4$
2) $x + y^2 x + 3xy^3 \notin (x^2, y)$, т.к. $x \notin (x^2, y)$.

Как упростить решение задачи Вхожденья?

Операция резюми: Предположим, что $\exists i=1 \dots m$:

$f_i \in \mathcal{I} \mid h_c$, т.е. $h_c = f_i \cdot u$, где u — элемент из $F[x_1 \dots x_n]$. Положим $h_1 = h - u f_i = (h_c + h_m) - u(f_i + f_m) = h_m - u f_m$, т.е. $h_{1c} < h_c$.

При этом $h \in \mathcal{I} \Leftrightarrow h_1 \in \mathcal{I}$, так $h - h_1 = u f_i \in \mathcal{I}$.

Если h за конечное число резюмирований сводится к нулю, то $h \in \mathcal{I}$.

В примере 1: $h_c = -x_1 x_3 x_4^2 = f_{1c} \cdot u = x_1(-x_3 x_4^2)$

Ред 1: $h \rightarrow x_2 x_3^2 x_4 + x_2 x_3 x_4^2 = h_1$.

Теперь $h_{1c} = x_2 x_3^2 x_4 = f_{2c} \cdot u = x_3(x_2 x_3 x_4)$

Реш 2: $h_1 \rightarrow x_2 x_4^3 + x_2 x_3 x_4^2 = h_2$

$$h_{2c} = x_2 x_3 x_4^2 = f_{2c} \text{ и } u = x_3 (x_2 x_4^2)$$

Реш 3: $h_2 \rightarrow x_2 x_4^3 - x_2 x_4^3 = 0 \Rightarrow h \in (f_1, f_2)$.

Опр 1 Базис f_1, \dots, f_m идеала $I = (f_1, \dots, f_m)$

называется **базисом Грёбнера (-Липцова)** этого идеала (относительно данного порядка перемножения), если каждый $h \in I$ сводится к нулю при помощи f_1, \dots, f_m .

Предл. 1 Набор мн-ч $f_1, \dots, f_m \in I = (f_1, \dots, f_m)$

— б.г. $\Leftrightarrow \forall h \in I \exists i \in \{1, \dots, m\} : f_i c \mid h_c$.

Δ -во: Упр 1

Предп 2 Если $f_1, \dots, f_m \in I$ и $\forall h \in I$

$\exists i \in 1 \dots m$: $f_i \mid h$, то $I = (f_1, \dots, f_m)$, в частности,
 $f_1, \dots, f_m \in \Gamma$. Δ -во: Упр 2

Т.1 Для любого $I \subseteq F[x_1, \dots, x_n]$ существует Γ .

Δ -во: Выводят из 7. Теоремы Гильберта о базисе
и предп. 2. Ино, если $I = (f_i \mid f_i \in I)$,
то по 7. Теореме существуют кан. базис этого
идеала $\Gamma = (u_1, \dots, u_m)$. Но тогда $I = (f_1, \dots, f_m)$,
где $f_i \mid u_i$, $i = 1 - m$. ~~■~~

Упр 3 x, y — б.т. идеала $I = (x, y) \triangleleft F[x, y]$.

Пример 2 $I = (x^2 - y, x^2 - z) \triangleleft F[x, y, z]$

$f_1 = x^2 - y, f_2 = x^2 - z$. У нас $z - y = f_1 - f_2 \in I$.

Но $(z - y)_c = -y$ не генер. идеала $I_c = I_c = x^2$
 $\Rightarrow f_1, f_2$ не явл-ся б.т.

Покажем, что если б.т. идеала I дан, то
задача нахождения алгоритмически разрешима,
Вопрос в том, как найти базис Грёбнера.

Далее, пусть $f_1 \dots f_m$ — базис идеала
 $I \triangleleft F[x_1 \dots x_n]$.

Опр 2 Мк-нн f_i и f_j имеют **ЗАГЛУШЕНИЕ**,
если \exists означен w , отличный от констант,
такой, что w делит f_i и f_j .

Если f_i и f_j имеют ЗАГЛУШЕНИЕ, то $f_i c = w u_i$
 $f_j c = w u_j$, где $w = \text{НОД}(f_i c, f_j c)$. Положим
 $F_{ij} = S(f_i, f_j) = f_i u_j - f_j u_i$ — сизига (срезка)
мк-нов f_i и f_j . Редуцируем F_{ij} с помощью
 $f_1 \dots f_m$ пока это возможно. Т.к. в конце
попытки не редуцируются мк-н \widetilde{F}_{ij} .

Опр 3 Задаваемые f_i и f_j **РАЗРЕШИМО** (иногда говорят, тривиально), если $\tilde{F}_{ij} = 0$.

Если задаваемые f_i и f_j **НЕРАЗРЕШИМО**?, то добавим к базису f_1, \dots, f_m и к $f_{m+1} = \tilde{F}_{ij}$.

Предл 3 В базисе f_1, \dots, f_m, f_{m+1} задаваемые f_i и f_j **РАЗРЕШИМО**. Д-во: очевидно.

В примере 2 Имеем задаваемые $f_1 = x^2 - y$ и $f_2 = x^2 - z$, тк. КОЯ $(f_1, f_2) = x^2$. Имеем

$F_{1,2} = -y \cdot 1 + z \cdot 1 = z - y$. Положим $f_3 = y - z$.

Других задаваемых в базисе f_1, f_2, f_3 нет.

Т.2 Для любых $f_1, \dots, f_n \in F[x_1, \dots, x_n]$ после reductions конечного числа заглажений получится набор $f_1, \dots, f_m, f_{m+1}, \dots, f_n$, в котором каждое заглавление разрешимо

Лемма Презп. о противнот, что сущ. бескон. много неразр. мн-ов F_{ij} . Р-м идеал J , порожд. их старшими членами. Выберем в нём кан. базис (т. Гильберта). Тогда у любого мн-ва из беск. мн-ва F_{ij} старший член делится на старший член одного из "базисных" мн-ов \Rightarrow его можно редуц. Противоречие.

T.3 (Diamond Lemma) базис f_1, \dots, f_n удовлетворяет

т.е. базисом Треубера \Leftrightarrow когда в нем нет заглаженных или конечное заглаженных разностей.

Δ -ВО: \Rightarrow) Если f_1, \dots, f_n - б.т. $\Rightarrow f_{ij} \in I$ и, значит, сводится к нулю.

\Leftarrow) Лемма Пусть даны g_1, \dots, g_s такие что $g_{i\ell} = \alpha_i x_1^{k_1} \dots x_n^{k_n}$. Если $f = \sum \lambda_i g_i$ и $f \in \langle x_1^{k_1} \dots x_n^{k_n} \rangle$, то $f = \sum_{i=1}^{s-1} \delta_i S(g_i, g_{i+1})$, $\delta_i \in F$.

Δ -ВО: $S(g_i, g_{i+1}) = g_i/\alpha_i - g_{i+1}/\alpha_{i+1}$ и $\lambda_1 \alpha_1 + \dots + \lambda_s \alpha_s = 0 \Rightarrow$

$$\begin{aligned}
 f &= \sum_{i=1}^s \lambda_i g_i = \lambda_1 \alpha_1 \left(\frac{g_1}{\alpha_1} - \frac{g_2}{\alpha_2} \right) + (\lambda_1 \alpha_1 + \lambda_2 \alpha_2) \left(\frac{g_2}{\alpha_2} - \frac{g_3}{\alpha_3} \right) + \\
 &+ \dots + (\lambda_1 \alpha_1 + \dots + \lambda_{s-1} \alpha_{s-1}) \left(\frac{g_{s-1}}{\alpha_{s-1}} - \frac{g_s}{\alpha_s} \right) + (\lambda_1 \alpha_1 + \dots + \lambda_s \alpha_s) \frac{g_s}{\alpha_s} \\
 &= \sum_{i=1}^{s-1} \delta_i S(g_i, g_{i+1}) \quad \blacksquare
 \end{aligned}$$

Нам нужно показать, что $f = \sum h_i f_i \quad \forall f \in I$,
 где $f_c = (h_i f_i)_c$ для некоторого $i \in 1 \dots m$. Если
 это не так, то выберем из всех представлений
 $f = \sum h_i f_i$ такое, что наиб. из $(h_i f_i)_c$ равно
 нулю. Из возможности, но при этом $f_c < (h_i f_i)_c$.
 Умень $f = \sum_{i=1}^s (h_{i,c} f_i + h_{i,m} f_i) + \sum_{i=s+1}^m h_i f_i$, где
 $(h_{i,c} f_i)_c = \alpha_i x_1^{k_i} \dots x_n^{k_n}$ — наиб. старший член для $i=1 \dots s$.

По предположению старшие члены в
сумме $F = \sum_{i=1}^s h_{ic} f_i$ уничтожаются. Тогда
по лемме $F = \sum_{i=1}^s \delta_i S(h_{ic} f_i, h_{i+1c} f_{i+1})$.

Т.к. h_{ic} и h_{i+1c} — однородны, то $S(h_{ic} f_i, h_{i+1c} f_{i+1})$
делится на $S(f_i, f_{i+1})$ (проверьте!). $\forall i = 1 \dots s-1$.

По условию все $S(f_i, f_{i+1})$ делятся

на f_1 при помощи f_2, \dots, f_m . Поэтому

$\forall i = 1 \dots s-1 \quad S(f_i, f_{i+1}) = \sum g_{el} f_l$, где ст. многочлен
срезки совпадает с $(g_{el} f_l)_c$ где $l \leq m$.

ко тогда F и, зная, f имеют представление
в виде комбинации $\sum d_j f_j$, у которого
наибольший из старших членов мн-ов
 $d_j f_j$ строго меньше, чем у исходной комбинации,
противоречие.

Осталось р-т считать, когда задан предельный не-
воображ. Это вытекает из след. предложения

Предл. 4 Если $(f_c, g_c) = 1$, то $S(f, g)$ рас-
щепляется к нулю с помощью f и g .

Упр 4 д.п. предл. 4

из т. 2 и 3 вытекает существование эфф. алгоритма для построения базиса Грёбнера из а.г.

Алгоритм Бухбергера

Вход: базис f_1, \dots, f_m идеала $I \subseteq F[x_1, \dots, x_n]$

Выход: базис Грёбнера идеала I .

- 1) Проверим нет ли в наборе зауждений. Если нет, то выходим, если есть пер. к шагу 2
- 2) По зауждению f_i и f_j строим \widetilde{F}_{ij} и результируем его к не резу. форме \widetilde{F}_{ij} . Если $\widetilde{F}_{ij} \neq 0$, то идеал I идеал I , если $\widetilde{F}_{ij} = 0$, то I идеал I .

3) Добавляем к набору мн-н $f_{k+1} = \widetilde{f_{ij}} \neq 0$
с $\text{цгс} 2$ и переходим к $\text{цгс} 4$

4) В импозитиве набора $\{f_i\}$ ищем нераск-
ренное р-ие z и переходим
на $\text{цгс} 2$. Если больше z не существует,
Выходим.

Т. 4 Алгоритм Бухбергера ищет базис
Гребнера идеала I за $10n$ число цгс ов.

В примере 2 f_1, f_2, f_3 — базис Гребнера!

Пусть f_1, \dots, f_m — в. Грёбнера $I \subseteq F[x_1, \dots, x_n]$.

Можно ли это упростить?

Упрощение 1: Пусть $f_i \in \mathbb{C} \mid f_j \in \mathbb{C}$. Удалим f_i .

Предл 5 базис, состоящий из в. Г с помощью
это упрощения слов в. Г.

Опр 4 базис Грёбнера называется **минималным**,
если $f_i \nmid f_j \in \mathbb{C} \forall i, j : i \neq j$.

Зам Минимализация является частью работы к
базису Грёбнера! (рассмотрите $I = (x, x+y)$!)

Упрощение 2 Предп, что несобравшийся сгруппирован
и мн-н f_i сводятся к f_j , где $i \neq j$.

Резуцируем и с помощью f_j и затем свеем
результат в f_i внесем и.

Предп 6 После упрощения 2 в Γ остается в Γ .

Опр 5 Базис Гребнера $\{f_1, \dots, f_m\}$ наз-ся

редуцированными, если ни один из членов
мн-н f_i не сводится к старшему члену f_j
 $\forall i, j \in \{1 \dots m\}, i \neq j$.

Т.5 Редуцированный базис Гребнера идеала $I \triangleleft F[x_1, \dots, x_n]$ определен однозначно (считается, что все коэффициенты свободных членов $= 1$), т.е. не зависит от выбора исходного базиса идеала I и от последовательности операций.

Зам Но этот базис, конечно, зависит от упорядочения переменных!

В примере 2 $f_1 = x^2 - y$, $f_2 = x^2 - z$, $f_3 = y - z$
 $\rightarrow f_2, f_3$ - редуцированный базис (а f_1, f_3 - нет почему?)

Применение к РСШемлю системы алгебр. ур-я
из алг. зам. поля F .

Т. 6 Система S несовместна \Leftrightarrow базис Грёбнера
идеала $I(S)$ содержит константу.

Д-во: $1 \in I(S)$ в силу т. Грёбнера означ
 $\Rightarrow \exists i: f_i \mid 1 \Rightarrow f_i$ - константа. \square

Т. 7 Число решений системы S об n переменных конечно
 \Leftrightarrow базис Грёбнера идеала $I(S)$ содержит

м-м $f_1, \dots, f_n: f_i = x_i^{k_i}$ для переменных
 x_1, \dots, x_n . Д-во: см Т. 7.4.3 из [ПСП, часть II].

Зам. В базисе Гр. может быть больше м-м!

Как проверить, что система эк-нн?

Из Т-мн Гамбурга о нулях $\Rightarrow S_1 = \{f_i = 0\} \sim S_2 = \{g_j = 0\} \Leftrightarrow \forall i f_i \in \Gamma(I(S_2)) \text{ и } \forall j g_j \in \Gamma(I(S_1))$.

Т.8 Пусть F - произв. поле, $I = (f_1, \dots, f_m) \subseteq F[x_1, \dots, x_n]$.

$f \in F[x_1, \dots, x_n]$. Тогда $f \in \Gamma(I) \Leftrightarrow \exists$ конст

$F[x_1, \dots, x_n, y]$ и деля $I_f = (f_1, \dots, f_m, 1 - yf) = F[x_1, \dots, x_n, y]$.

Из Т.8 \Rightarrow существует алгоритм, определяющий (кажд ли дан конст), удовлетворяет ли f разложению и деля (f_1, \dots, f_m) , а значит, возв. решить задачу об эк-нн систем. Упр 5* Δ -в Т.8.