Лекция 4: Критерий и алгоритм Бухбергера

(4.1) Свойства базисов Грёбнера

Алгоритм деления, описанный в лекции №2, зависит от порядка, в котором перечислены многочлены в наборе F. Увидим, что остаток от деления на базис Грёбнера определён однозначно.

Предложение 4.1: Пусть $G = \{g_1, \dots, g_t\}$ – базис Грёбнера идеала $I \lhd k[x_1, \dots, x_n]$, многочлен $f \in k[x_1, \dots, x_n]$. Тогда существует единственный мн-н $r \in k[x_1, \dots, x_n]$, для которого справедливо:

1°. ни один одночлен не делится ни на один $\operatorname{lt} g_1, \dots, \operatorname{lt} g_t$;

2°. существует $g \in I$, т.ч. $f = g + r$.

Доказательство: Существование многочлена r со свойствами 1°, 2° вытекает из теоремы 2.1 (алгоритм деления) согласно, которой
$$f = a_1 g_1 + \dots + a_t g_t + r,$$
где r удовлетворят 1°, а $a_1 g_1 + \dots + a_t g_t$ можно обозначить за g.

Докажем единственность, для этого предположим, что $f = g + r = g' + r'$ с выполнением 1° и 2°. Поскольку разность $r - r' = g' - g$ лежит в идеале I, то при условии, что $r \neq r'$ мы имеем бы включение $\operatorname{lt}(r' - r) \in \operatorname{lt}(I) = \langle \operatorname{lt} g_1, \dots, \operatorname{lt} g_t \rangle$. По лемме 3.1 $\operatorname{lt}(r' - r)$ делился бы на некоторый $\operatorname{lt} g_i$. Противоречие, т.к. ни один из одночленов в r и r' не делится ни на один из $\operatorname{lt} g_1, \dots, \operatorname{lt} g_t$. Следовательно, $r - r' = 0$. ◀

Часто остаток r от деления на базис Грёбнера G называют **нормальной формой** f (**относительно** $I = \langle G \rangle$).

Следствие: Пусть $G = \{g_1, \dots, g_t\}$ – базис Грёбнера идеала $I \lhd k[x_1, \dots, x_n]$. Тогда многочлен $f \in I$ в том и только том случае, когда остаток от деления f на G равен нулю.
(это свойство можно положить в основу определения базиса Грёбнера).

Определение 4.1: Пусть $f, g \in k[x_1, \dots, x_n]$ ненулевые. **S-многочленом** f и g называется
$$S(f, g) := \frac{\operatorname{lcm}(\operatorname{lm} f, \operatorname{lm} g)}{\operatorname{lt} f} f - \frac{\operatorname{lcm}(\operatorname{lm} f, \operatorname{lm} g)}{\operatorname{lt} g} g.$$

Пример 4.1: Зафиксируем на $\mathbb{R}[x, y]$ порядок deglex: $x > y$. Для многочленов $f = x^3y^2 - x^2y^3 + x$ и $g = 3x^4y + y^2$,
$$S(f, g) := \frac{x^4y^2}{x^3y^2} f - \frac{x^4y^2}{3x^4y} g = xf - \tfrac{1}{3} y g = -x^3y^3 + x^2 - \tfrac{1}{3} y^3.$$ ◀

Лемма 4.1: Пусть $f_i \in k[x_1, \dots, x_n]$, $i = 1, \dots, s$, т.ч. $\operatorname{mdeg} f_i = \delta \in \mathbb{Z}^n_{\geq 0}$ для всех i. Тогда, если для $c_i \in k$

$$(4.1) \qquad \operatorname{mdeg}\left(\sum_{i=1}^{s} c_i f_i\right) < \delta,$$

то $\sum_{i=1}^{s} c_i f_i$ является линейной комбинацией с коэффициентами в k S-многочленов $S(f_i, f_j)$, $1 \leq i, j \leq s$. Более того, все

$$\operatorname{mdeg} S(f_i, f_j) < \delta.$$

Доказательство: Обозначим $d_i = \operatorname{lc} f_i$, тогда в силу условия (4.1) имеем равенство

$$(4.2) \qquad \sum_{i=1}^{s} c_i d_i = 0.$$

Введём многочлены $p_i := \frac{f_i}{d_i}$, т.ч. $\operatorname{lc} p_i = 1$. Тогда

$$(4.3) \qquad \sum_{i=1}^{s} c_i f_i = \sum_{i=1}^{s} c_i d_i p_i = c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \dots$$
$$+ (c_1 d_1 + \dots + c_{s-1} d_{s-1})(p_{s-1} - p_s) + (c_1 d_1 + \dots + c_s d_s) p_s.$$

Очевидно, что $\operatorname{lcm}(\operatorname{lm} f_i, \operatorname{lm} f_j) = x^\delta$, где $\operatorname{lt} f_i = d_i x^\delta$ для всех i. Поэтому

$$S(f_i, f_j) = \frac{x^\delta}{\operatorname{lt} f_i} f_i - \frac{x^\delta}{\operatorname{lt} f_j} = \frac{x^\delta}{d_i x^\delta} f_i - \frac{x^\delta}{d_j x^\delta} f_j = p_i - p_j.$$

Тогда, принимая во внимание (4.2), из (4.3) получаем

$$\sum_{i=1}^{s} c_i f_i = c_1 d_1 S(f_1, f_2) + (c_1 d_1 + c_2 d_2) S(f_2, f_3) + \dots$$
$$+ (c_1 d_1 + \dots + c_{s-1} d_{s-1}) S(f_{s-1}, f_s)$$

Заметим, что в силу $\operatorname{lt} p_i = x^\delta$ для всех $i = \overline{1, s}$, поэтому

$$\operatorname{mdeg} S(f_i, f_j) = \operatorname{mdeg}(p_i - p_j) < \delta.$$ ◀

Теорема 4.1: (критерий Бухбергера) Пусть $I \subset k[x_1, \dots, x_n]$ — идеал. Тогда $G = \{g_1, \dots, g_t\}$ является базисом Грёбнера идеала I, если и только если для всех $i \neq j$ остаток от деления $S(g_i, g_j)$ на G равен нулю.

Доказательство: ($\Rightarrow$) Если G — базис Грёбнера, то остатки от деления $S(g_i, g_j)$ на G равны нулю по следствию из предложения 4.1, т.к. все $S(g_i, g_j) \in I$.

($\Leftarrow$) Пусть f — ненулевой многочлен из идеала $I = \langle g_1, \dots, g_t \rangle$. Достаточно д-ть что если все остатки от деления $S(g_i, g_j)$ на G равны нулю, то $\operatorname{lt} f \in \langle \operatorname{lt} g_1, \dots, \operatorname{lt} g_t \rangle$.

Поскольку $f \in I$, мы можем записать его в виде

$$f = \sum_{i=1}^{t} h_i g_i, \tag{4.4}$$

где $h_i \in k[x_1, \dots, x_n]$. Обозначим $m(i) := \operatorname{mdeg}(h_i g_i)$ и $\delta := \max\{m(1), \dots, m(t)\}$, тогда

$$\operatorname{mdeg} f \leqslant \delta.$$

Среди всех разложений (4.4) для f можно выбрать разложение с наименьшим δ, множество мономов вполне упорядочено относительно мономиального порядка.

Заметим, что если $\operatorname{mdeg} f = \delta$, то $\operatorname{lt} f$ делится на какой-то $\operatorname{lt} g_i$, т.е. $\operatorname{lt} f \in \langle \operatorname{lt} g_1, \dots, \operatorname{lt} g_t \rangle$ — набор G является базисом Грёбнера.

Предположим, что $\operatorname{mdeg} f < \delta$. Перепишем многочлен f в следующем виде

$$f = \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i = \sum_{m(i)=\delta} \operatorname{lt} h_i g_i + \sum_{m(i)=\delta} (h_i - \operatorname{lt} h_i) g_i + \sum_{m(i)<\delta} h_i g_i. \tag{4.5}$$

В силу $\operatorname{mdeg} f < \delta$ и $\operatorname{mdeg}\left(\sum_{m(i)=\delta} (h_i - \operatorname{lt} h_i) g_i\right) < \delta$, $\operatorname{mdeg}\left(\sum_{m(i)<\delta} h_i g_i\right) < \delta$ и мультистепень $\operatorname{mdeg}\left(\sum_{m(i)=\delta} h_i g_i\right) < \delta$.

Пусть $\operatorname{lt} h_i = c_i x^{\alpha(i)}$. Тогда первая сумма

$$\sum_{m(i)=\delta} \operatorname{lt} h_i g_i = \sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$$

попадает под условие леммы 4.1 с $f_i = x^{\alpha(i)} g_i$. Поэтому эта сумма является линейной комбинацией S-многочленов $S(x^{\alpha(i)} g_i, x^{\alpha(j)} g_j)$.
В свою очередь

$$S(x^{\alpha(i)} g_i, x^{\alpha(j)} g_j) = \frac{x^{\delta}}{x^{\alpha(i)} \operatorname{lt} g_i} x^{\alpha(i)} g_i - \frac{x^{\delta}}{x^{\alpha(j)} \operatorname{lt} g_j} x^{\alpha(j)} g_j = x^{\delta - \gamma_{ij}} S(g_i, g_j),$$

где $x^{\gamma_{ij}} = \operatorname{lcm}(\operatorname{lm} g_i, \operatorname{lm} g_j)$. Значит для некоторых констант $c_{ij} \in k$

$$\sum_{m(i)=\delta} \operatorname{lt} h_i g_i = \sum_{i,j} c_{ij} x^{\delta - \gamma_{ij}} S(g_i, g_j). \tag{4.6}$$

По условию все остатки от деления $S(g_i, g_j)$ на $G = \{g_1, \dots, g_t\}$ равны нулю, поэтому согласно алгоритму деления

$$S(g_i, g_j) = \sum_{k=1}^{t} a_{ijk} g_k,$$

где $a_{ijk} \in k[x_1, \dots, x_n]$, т.ч. $\operatorname{mdeg}(a_{ijk} g_k) \overset{(*)}{\leq} \operatorname{mdeg}(S(g_i, g_j))$. Тогда, положив $b_{ijk} = x^{\delta - \gamma_{ij}} a_{ijk}$, запишем

(4.7) $$x^{\delta - \gamma_{ij}} S(g_i; g_j) = \sum_{k=1}^{t} b_{ijk} g_k.$$

В силу леммы 4.1 справедлива самая правая оценка в цепочке

$$\operatorname{mdeg}(b_{ijk} g_k) \overset{(*)}{\leq} \operatorname{mdeg}(x^{\delta - \gamma_{ij}} S(g_i; g_j)) = \operatorname{mdeg}(S(x^{\alpha(i)} g_i,\ x^{\alpha(j)} g_j)) < \delta.$$

Если мы подставим выражение (4.7) в сумму (4.6), то получим

$$\sum_{m(i)=\delta} Uh_i\, g_i = \sum_{i,j} c_{ij} \left(\sum_k b_{ijk} g_k \right) = \sum_i \tilde{h}_i g_i,$$

где $\operatorname{mdeg}(\tilde{h}_i g_i) < \delta$. Теперь, подставляя $\sum_{m(i)=\delta} Uh_i g_i = \sum_i \tilde{h}_i g_i$ в (4.5), мы получим выражение для f, где каждый одночлен имеет мультистепень $< \delta$. Противоречие с выбором δ доказывает теорему. ◀

Пример 4.2: Рассмотрим идеал $I = \langle y - x^2; z - x^3 \rangle$ скрученной кубики в $\mathbb{R}^3$. Докажем, что $G = \{y - x^2;\ z - x^3\}$ — базис Грёбнера относительно lex: $y > z > x$.
Рассмотрим

$$S(y - x^2;\ z - x^3) = \frac{yz}{y}(y - x^2) - \frac{yz}{z}(z - x^3) = yx^3 - zx^2,$$

$$yx^3 - zx^2 \xrightarrow[g_1]{x^3} -zx^2 + x^5 \xrightarrow[g_2]{-x^2} 0 \quad \text{или}$$

$$yx^3 - zx^2 = x^3(y - x^2) - x^2(z - x^3) + 0. \quad ◀$$

4.2 Алгоритм Бухбергера

Пример 4.3: Критерий Бухбергера в полной мере даёт идею того как строить базис Грёбнера: нужно добавлять ненулевые остатки от деления S-многочленов в набор образующих.

Рассмотрим идеал $I = \langle \overbrace{x^3 - 2xy}^{f_1}, \overbrace{x^2y - 2y^2 + x}^{f_2} \rangle$ в кольце $k[x, y]$ с deglex: $x > y$.
Тогда $S(f_1, f_2) = yf_1 - xf_2 = -x^2$, и $S(f_1, f_2) \notin \langle Uf_1, Uf_2 \rangle = \langle x^3, x^2y \rangle$.
Следовательно, набор (f_1, f_2) не является базисом Грёбнера.

Добавим $f_3 = S(f_1, f_2)$ в набор (f_1, f_2, f_3). Тогда

$$S(f_1, f_2) \to 0,$$
$$S(f_1, f_3) = f_1 - (-x) f_3 = -2xy,$$

где многочлен $-2xy$ не даёт 0 в остатке от деления на (f_1, f_2, f_3). Поэтому мы и многочлен $f_4 = -2xy$ добавляем в набор образующих. Продолжая пополнять набор образующих ненулевыми остатками от деления S-многочленов, мы приходим к тому, что набор

$$G = \{x^3 - 2xy,\ x^2y - 2y^2 + x,\ -x^2, -2xy,\ -2y^2 + x\}$$

даёт базис Грёбнера идеала I. ◀

Теорема 5.2: Пусть $I = \langle f_1, .., f_s \rangle$ - ненулевой идеал в $k[x_1, ..., x_n]$.
Тогда базис Грёбнера идеала I строится за конечное число шагов алгоритмом

Вход: $F = (f_1, ..., f_s)$

Выход: Базис Грёбнера $G = (g_1, ..., g_t)$ для I, т.ч. $F \subset G$.

Инициализация: $G := F$

Повторять

$G' := G$

Для каждой пары $\{p, q\}$, $p \neq q$

$S :=$ остаток от деления $S(p, q)$ на G

Если $S \neq 0$

$G := G \cup \{S\}$

Пока $G \neq G'$

Доказательство: (см. Cox, Little & O'Shea, p. 90) ◀

Пусть $G = \{g_1, ..., g_t\}$ — базис Грёбнера идеала I. Если старший член $p \in G$ выражается через старшие члены других многочленов набора G, то очевидно набор $G - \{p\}$ тоже является базисом Грёбнера.

Определение 4.2: Минимальный базис Грёбнера идеала I — это базис Грёбнера G идеала I, т.ч.

1) $lc\,p = 1$ для всех $p \in G$.

2) Для всех $p \in G$ старший член $lt\,p \notin \langle lt(G - \{p\}) \rangle$.

Пример 4.4: Анализируя базис Грёбнера из примера 4.3, легко найти минимальный базис Грёбнера

$$\{x^2,\ xy,\ y^2 - \tfrac{1}{2}x\}.$$

Нетрудно проверить, что для всех $a \in k$ набор

$$\{x^2 + axy,\ xy,\ y^2 - \tfrac{1}{2}x\}$$

является минимальным базисом Грёбнера. ◀

Определение 4.3: **Редуцированный базис Грёбнера** идеала I — это минимальный базис Грёбнера G идеала I, т.ч. для всех $p \in G$ ни один моном многочлена p не лежит в $\langle LT(G - \{p\}) \rangle$.

Предложение 4.2: Пусть $I \subset k[x_1, \dots, x_n]$ - ненулевой идеал. Тогда для фиксированного мономиального порядка существует единственный редуцированный базис Грёбнера идеала I.

Доказательство: (см. Cox, Little & O'Shea, p. 92) ◀

Предложение 4.2 решает вопрос о равенстве идеалов, порождённых наборами $\{f_1, \dots, f_s\}$ и $\{g_1, \dots, g_t\}$: нужно зафиксировать мономиальный порядок и вычислить редуцированные базисы Грёбнера идеалов $\langle f_1, \dots, f_s \rangle$ и $\langle g_1, \dots, g_t \rangle$.