Введение. Базис Грёбнера.

Определение базиса Грёбнера.

В докладе используется техника базисов Грёбнера, поэтому вспомним некоторые основные понятия и алгоритмы.

Пусть k — поле и $k[X] := k[X_1, \ldots, X_n]$ — свободная алгебра над k. Обознаим через T множество мономов $k[X]$. Пусть $<$ — полный порядок на T. Назовем его допустимым, если $1 < t$ для любого $t \in T, t \neq 1$ и для любых $t_1, t_2, t \in T$ из $t_1 < t_2$ следует, что $tt_1 < tt_2$. Можно считать порядок $<$ определённцым на $k[X]$.

Пусть $0 \neq f \in k[X]$, тогда $f = \sum_{t \in T} c_t t$. Наибольший элемент t, такой что $c_t \neq 0$ назовём главным членом и обозначим $l_t(f)$, а соответствующий ему коэффициент назовём главным и обозначим $l_c(f)$. Для $f = 0$ положим $l_t(0) = 0$ и $l_c(0) = 0$.

Определение 1. *Пусть $G \subset k[X]$ — конечное подмножество и $0 \neq f \in k[X]$. Назовем f редуцируемым по модулю G, если существует моном t в f, что $t = s \cdot l_t(g)$ для $s \in T, g \in G$.*

Определение 2. *Пусть I ненулевой идеал $k[X]$, а $<$ допустимый порядок и $G \subset I$ — конечное подмножество.*

1. *G называется базисом Гребнера I (относительно порядка $<$), если для любого $f \in I$ существуют $s \in T$ и $g \in G$, что $l_t(f) = s \cdot l_t(g)$.*

2. *Базис Грёбнера G идеала I минимальный, если для любого $g \in G$ множество $G \setminus \{g\}$ не является базисом Грёбнера идеала I.*

3. *Базис Грёбнера G идеала I называется редуцированным, если для любого $g \in G$ элемент g нельзя редуцировать по модулю $G \setminus \{g\}$ и $l_c(g) = 1$.*

Таким образом, базис Грёбнера G идеала I является идеалом в том смысле, что G порождает идеал I. С другой стороны, существуют алгоритмы, позволяющие по конечному набору порождающих идеала построить его базис Грёбнера (в том числе редуцированный). Например алгоритм Бухбергера решает эту задачу.

Нормальная форма.

Пусть I — ненулевой идеал $k[X]$ и $<$ — допустимый порядок на $k[X]$, а G базис Грёбнера I относительно порядка $<$.

Предположим, что $f = \sum_{t \in T} c_t t$ содержит редуцируемые члены по модулю G. Пусть t_1 —наибольший из таких членов, редуцируется элементом $g \in G$, тогда положим $f_1 = f - (c_{t_1}/l_c(g))sg \in I$. Если у f_1 имееются редуцируемые члены, продолжим процесс. Пусть процесс не закончится, тогда мы получим бесконечную последовательность $t_1 > t_2 > \ldots$, что невозможно для допустимого порядка. Назовём последний элемент последовательности $f_1, f_2, \ldots$ нормальной формой f и обозначим его f_+. Очевидно $f - f_+ \in I$ и f_+ не редуцируется по модулю G.

Алгоритм отношения.

Пусть $F_1, \ldots, F_m \in k[X]$ и I — идеал в $k[X]$, порожденный $Q_1, \ldots, Q_s$. Пусть $J = \{P(Y) \in k[Y] \mid P(F_1, \ldots, F_m) \in I\}$. Если $\prec$ — такой допустимый порядок на мономах $k[X, Y]$, что $X_i \succ Y_1^{\alpha_1} \ldots Y_m^{\alpha_m}$ для всех $i, \alpha_1, \ldots, \alpha_m \in \mathbb{N}$, G — базис Гребнера идеала

$$(Y_1 - F_1(X), \ldots, Y_m - F_m(X), Q_1, \ldots, Q_s)$$

, то $G \cap k[Y]$ — базис Гребнера идела J относительно порядка $\prec$.

Алгоритм проверки членства.

Пусть на $k[X, Y]$ задан допустимый порядок $\prec$, такой что $X_i \succ Y_1^{\alpha_1} \ldots Y_m^{\alpha_m}$ для всех $i, \alpha_1, \ldots, \alpha_m \in \mathbb{N}$. И пусть $f_1, \ldots, f_m, g \in k[X]$, а G — базис Грёбнера идеала

$$J = (Y_1 - f_1(X), \ldots, Y_m - f_m(X), Q_1, \ldots, Q_s)\,,$$

тогда $g(X) \in k[f_1, \ldots, f_m]$ тогда и только тогда, когда $g_+(X) \in k[Y]$, где g_+ — нормальная форма g по модулю G. Более того, если $g+(X) = P(Y)$, то $g(X) = P(f_1, \ldots, f_m)$.

Алгоритм вычисления ядра ЛНД.

Пусть k — поле характеристики 0, $A = k[a_1, \ldots, a_n]$ — конечно порожденная k–алгебра без делителей нуля, а D — не нулевое локально нильпотентное дифференцирование.

Определение 3. *Отображение Диксилье для любого локального слайса r — это $\pi_r \colon A \to A$,*

$$\pi_r(f) = \sum_{i \geq 0} \frac{(-1)^i}{i!} D^i f \frac{r^i}{(Dr)^i}.$$

Пусть $A^D = \ker D$ тоже конечно порожден. Пусть $p \in A$ — локальный слайс (то есть $D^2 p = 0, Dp \neq 0$). Тогда $\tilde{A} = A[d^{-1}] = A_d$ — локализация A, а элемент $s = p/d$ — слайс (то есть $D^2 s = 1$), где $d = Dp$.

Обозначим через b_i образ a_i при отображениии Диксилье. Тогда по теореме о слайсе получаем $\tilde{A}^D = k[b_1, \ldots, b_n][d^{-1}]$ ($D(d^{-1}) = 0$, значит $\pi_r(d^{-1}) = d^{-1}$). Более того $\tilde{A}^D = A^D[d^{-1}]$, так как

$$0 = D(\frac{a}{d^k}) = \frac{D(a)}{d^k} \Leftrightarrow D(a) = 0.$$

Значит для всех b_i существуют такие минимальные $e_i \geq 0$, что $c_i = d^{e_i} b_i \in C \stackrel{\text{def}}{:=} A^D$.

Положим $C_0 = k[c_1, \ldots, c_n, d]$, тогда $C_0 \subseteq C \subseteq C_0[d^{-1}]$. Теперь определим $C_m, m \geq 1$ как подалгебру A порожденную такими элементами $h \in A$, что $dh \in C_{m-1}$. Так как $d \in C_0$, то $C_0 \subset C_1 \subset \cdots \subset C_m \subset C$ для любого $m \geq 1$. Покажем, что $C_m \in C$. Для $m = 0$ утверждение верно, докажем по индукции. Пусть $C_{m-1} \in C, h \in C_m$, тогда $0 = D(dh) = D(d)h + dD(h) = dD(h)$, значит $D(h) = 0$, что и требовалось доказать.

Утверждение 4.

1. *Для любого $m \geq 0$ C_m — конечно порожденная подалгебра C.*

2. *Если C — конечно порождена, то $C = C_r$.*

3. *Если $C_r = C_{r+1}$, то $C = C_r$ и конечно порождена.*

Доказательство.

1. Пусть $m \geq 1$, $C_{m-1} = k[f_1, \ldots, f_l]$. Обозначим через $J = \{P \in k[Y_1, \ldots, Y_l] \mid P(f_1, \ldots, f_l \in Ad)\} \lhd k[Y]$. По теореме Гильберта о базисе J конечно порожден, пусть $P_1, \ldots, P_s$ — порождающие J. Тогда $P_i(f_1, \ldots, f_l) = g_i d$, где $g_i \in A$, значит $g_i \in C_m$.

Докажем, что $C_m[f_1, \ldots, f_l, g_1, \ldots, g_s]$. Включение $\subset$ очевидно, покажем $\supset$. Положим $h \in C_m, dh \in C_{m-1}$, тогда $dh = P(f_1, \ldots, f_l)$ для некоторого P. Получаем, что $P(Y) = \sum_{i=1}^{s} a_i(Y) P_i(Y)$, тогда $P(f) = \sum_{i=1}^{s} a_i(f) P_i(f)$. Значит $dh = d \sum_{i=1}^{s} a_i(f) g_i$, что завершает индукцию.

2. Пусть C — конечно пораженная алгебра, $C = k[I_1, \ldots, I_n]$. Так как $C \subset C_0[d^{-1}]$, то существует такое r, что для всех $j : d^r I_j \in C_0$, значит $I_j \in C_r$. Таким образом $C_r \subset C \subset C_r$, то есть $C = C_r$.

3. По определению C, получаем $C = \cup_{m \geq 0} C_m = C = \cup_{m=0}^{r} C_m = C_r$ — конечно порождена по первому пункту. □

Алгоритм выглядит следующим образом:

1. Строим C_0.

2. Строим C_m по C_{m-1}. Для этого надо построить $g_1, \ldots, g_s$ из первого пункта. Положим $\bar{A} \stackrel{\text{def}}{:=} A/Ad$, тогда положим

$$J = \{P \in k[Y_1, \ldots, Y_l] \mid P(\bar{f}_1, \ldots, \bar{f}_l) = 0 \text{ в } \bar{A}\}, \text{ где } \bar{f}_j = f_j + Ad.$$

Применяя алгоритм отношения находим $P_1, \ldots, P_s$. Получаем, что $P_i(f) = dg_i$. Пусть $A = k[X_1, \ldots, X_n]/I$, где $I \triangleleft k[X], I = (H_1, \ldots, H_t)$. Пусть $f_i = F_i + I, d = d^* + I$ для $F_i, d^* \in k[X]$. Значит

$$P_i(f) \in dA \Leftrightarrow P_i(F) = B_i d^* + \sum_{j=1}^{t} G_{j,i} H_j, \text{ для } B_i, G_{i,j} \in k[X].$$

Найти B_i можно с помощью базиса Грёбнера $\{S_1, \ldots, S_p\}$ идеала $(d^*, H_1, \ldots, H_t)$, где $S_1, \ldots, S_p$ — выражаются через $d^*, H_1, \ldots, H_j$. Имеем $P_i(F) = \sum_{j=1}^{p} L_{i,j} S_j$, $L_{i,j} \in k[X]$, откуда находим B_i, то есть $g_i = B_i + I$.

3. Проверяем $C_m = C_{m+1}$ с помощью алгоритма проверки членства.

Алгоритм вычисления образа ЛНД.

Пусть $0 \neq a \in A$, значит существует такое m, что $D^m(a) \neq 0$, $D^{m+1}(a) = 0$. Попробуем найти, такой элемент $b \in A$, что $Db = a$. Пусть $A^D = k[f_1, \ldots, f_l]$. Положим

$$b' = \sum_{i=0}^{m} \frac{(-1)^i}{(i+1)!} D^i(a) s^{i+1}, \text{тогда } D(b') = a.$$

Если слайс $s \in A$, то алгоритм завершен.

Получаем $g \stackrel{\text{def}}{:=} d^{m+1} b' \in A$. Пусть $a = a^* + I$, $d = d^* + I$, $g = G + I$, $f_i = F_i + I$, где $a^*, d^*, G, F_i \in k[X]$. И пусть

$$J = (Y_1 - F_1, \ldots, Y_l - F_l, d^{*m+1}, H_1, \ldots, H_t) \triangleleft k[X, Y].$$

Введём порядок $\prec$ на $k[X, Y]$, такой что $X_i \succ Y_1^{\alpha_1} \ldots Y_m^{\alpha_m}$ для всех $i, \alpha_1, \ldots, \alpha_m \in \mathbb{N}$. Рассмотрим нормальную форму G_+.

Утверждение 5. *$a \in D(A) \Leftrightarrow G_+ \in k[Y]$. Более того, если $G_+ \in k[Y]$, то $b = (g - G_+(f))/d^{m+1} \in A$ и $D(b) = a$.*

Доказательство. 1. Пусть $a = D(b)$ для некоторого $b \in A$. Тогда $D(b - b') = 0$, то есть $g - d^{m+1}b \in A^D$. Получаем, что $g - d^{m+1}b = H(f_1, \ldots, f_l)$ для $H(Y) \in k[Y]$. Пусть $b = b^* + I$, тогда

$$G - d^{*m+1}b - H(F_1, \ldots, F_l) \in I,$$

значит $G(Y) - H(Y) \equiv 0 \mod J$. Тогда $l_t(G_+) \preceq l_t(H)$, откуда $G_+ \in k[Y]$.

2. Обратно, пусть для $a_i, c_j, e \in k[X, Y]$ выполнено

$$G = G_+ + \sum_i a_i(X, Y)(Y_i - F_i) + \sum_j c_j(X, Y)H_j + e(X, Y)d^{*m+1}.$$

То есть $g \equiv G_+(f_1, \ldots, f_l) + bd^{m+1} \mod I$, где $b = e(X, F) + I$ в A/I. Получаем $b = (g - G_+(f_1, \ldots, f_l))/(d^{m+1})$, так как $D(G_+(f_1, \ldots, f_l) \in A^D$, то $d^m + 1D(b') = D(b)d^{m+1}$, значит $D(b') = a = D(b)$. □