Введение

Кольцо многочленов $F[x]$ над полем F от одной переменной x обладает рядом хороших свойств. В нём есть алгоритм деления с остатком и алгоритм Евклида. Все идеалы в этом кольце главные. В этом смысле оно очень похоже на кольцо целых чисел $\mathbb{Z}$. Задача принадлежности многочлена f идеалу I в таком кольце решается тривиально с помощью деления с остатком на образующий элемент идеала I. Вычисления в факторкольце приводят к арифметике остатков по модулю образующего многочлена. Если переменных становится хотя бы две, то таких хороших свойств уже нет. Например, непонятно, что значит «разделить x на y с остатком». Идеалы в кольце $F[x, y]$ уже не обязательно главные. Системы полиномиальных уравнений от двух и более переменных, вообще говоря, уже не эквивалентны одному уравнению. Наша ближайшая цель — научиться исследовать системы нелинейных полиномиальных уравнений над полем. В частности, мы хотим научиться отвечать на следующие вопросы:

— всякая ли система может быть задана конечным набором уравнений?
— как проверить, совместна ли система?
— как узнать, конечно ли множество решений системы (над $\bar{F}$)?
— как проверить принадлежность многочлена f идеалу I?
— как проводить вычисления в факторалгебре $F[x_1, \ldots, x_n]/I$?
— как исключить заданные неизвестные из системы?

Заметим, что для линейных систем ответы на эти вопросы легко получить с помощью приведения системы к ступенчатому виду методом Гаусса.

1. Свойства конечности полугруппы $\mathbb{Z}^n_{\geqslant 0}$

Мы будем работать в кольце многочленов $F[x_1, \dots, x_n]$. Договоримся называть *мономом* выражение $x_1^{a_1} \dots x_n^{a_n}$, где a_i — неотрицательные целые числа. *Термом* будем называть одночлен, то есть, моном с коэффициентом. Моноид мономов изоморфен моноиду $\mathbb{Z}^n_{\geqslant 0}$. Иногда нам будет удобнее говорить о мономах в аддитивном смысле именно как об элементах $\mathbb{Z}^n_{\geqslant 0}$. Следуя книге [1], рассмотрим «свойство конечности» этой полугруппы.

Определение 1.1. *Идеалом* полугруппы $\mathbb{Z}^n_{\geqslant 0}$ называется всякое ее подмножество, содержащее вместе с каждой точкой α и точку $\alpha + \gamma \ \forall\, \gamma \in \mathbb{Z}^n_{\geqslant 0}$.

Определение 1.2. *Октантом* $O(\alpha)$ с центром в точке α называется множество $\{\alpha + \gamma \,|\, \gamma \in \mathbb{Z}^n_{\geqslant 0}\}$.

Ясно, что октант является идеалом, и что идеал вместе с каждой своей точкой содержит весь октант с центром в ней.

Теорема 1.3 (Свойство конечности полугруппы $\mathbb{Z}^n_{\geqslant 0}$)**.** *Всякий идеал в $\mathbb{Z}^n_{\geqslant 0}$ является объединением конечного числа октантов.*

Доказательство. □

Определение 1.4. Подмножество $\mathbb{Z}^n_{\geqslant 0}$ называется *коидеалом*, если его дополнение — идеал.

Следствие 1.5. *Всякий мономиальный идеал в $F[x_1, \dots, x_n]$ конечно порожден.*

Следствие 1.6 (Лемма Диксона)**.** *Пусть $M_1, \dots, M_s, \dots$ — бесконечная последовательность мономов. Тогда обязательно найдутся два монома M_i и M_j, такие, что $M_i \mid M_j$.*

Предложение 1.7. *Моном M принадлежит мономиальному идеалу $(M_1, \dots, M_s)$ тогда и только тогда, когда $M_i \mid M$ для некоторого i.*

Далее нам понадобится понятие допустимого упорядочения на мономах, чтобы можно было выбирать «старший моном» в многочленах.

Определение 1.8. *(Допустимым) мономиальным упорядочением* $\prec$ на $\mathbb{M}_n$ называется линейный порядок, удовлетворяющий свойствам:

(1) $M \prec N \implies MP \prec NP \quad \forall\, M, N, P \in \mathbb{M}_n$;
(2) $1 \preccurlyeq M \quad \forall\, M \in \mathbb{M}_n$.

Определение 1.9. Пусть $a = (a_1, \dots, a_n)$, $b = (b_1, \dots, b_n) \in \mathbb{R}^n$. Вектор a *лексикографически младше* вектора b ($a \prec_{\text{lex}} b$), если существует такое k, $0 \leqslant k < n$, что $a_i = b_i$ для всех натуральных $i \leqslant k$, но $a_{k+1} < b_{k+1}$. Аналогично будем сравнивать векторы-столбцы.

Примеры. Зафиксируем порядок на переменных (положив, например, $x_1 \prec x_2 \prec \dots \prec x_n$). Пусть $M = x_1^{a_1} \dots x_n^{a_n}$ и $N = x_1^{b_1} \dots x_n^{b_n}$ — произвольные мономы из $\mathbb{M}_n$. Следующие бинарные отношения на $\mathbb{M}_n$ являются мономиальными упорядочениями:

(1) *Лексикографическое* упорядочение (lex):
$$M \prec_{\text{lex}} N \iff (a_1, \dots, a_n) \prec_{\text{lex}} (b_1, \dots, b_n).$$
(2) *Сначала по степени, затем лексикографическое* упорядочение (deglex):
$$M \prec_{\text{deglex}} N \iff (\deg M, a_1, \dots, a_n) \prec_{\text{lex}} (\deg N, b_1, \dots, b_n).$$
(3) *Сначала по степени, затем обратное лексикографическое* упорядочение (degrevlex):
$$M \prec_{\text{degrevlex}} N \iff (\deg M, b_n, \dots, b_1) \prec_{\text{lex}} (\deg N, a_n, \dots, a_1).$$

Предложение 1.10. *Любое мономиальное упорядочение вполне упорядочивает множество $\mathbb{M}_n$ (то есть, любая убывающая цепочка мономов обрывается).*

Зафиксируем некоторое упорядочение на мономах. Будем обозначать через $\mathrm{LM}\, f$ старший моном ненулевого многочлена f, а через $\mathrm{LM}\, I$ множество старших мономов ненулевых элементов из I.

Теорема 1.11. *Пусть I — идеал в $F[x_1, \ldots, x_n]$. Рассмотрим его как векторное пространство над F. Пусть подпространство L порождено всеми мономами, не принадлежащими $\mathrm{LM}\, I$. Тогда справедливо разложение векторных пространств*

$$F[x_1, \ldots, x_n] = I \oplus L.$$

Доказательство. □

Определение 1.12. Система образующих G идеала I называется его *базисом Грёбнера*, если $(\mathrm{LM}\, G) = (\mathrm{LM}\, I)$.

Следствие 1.5 показывает, что у каждого идеала существует конечный базис Грёбнера. Действительно, достаточно взять многочлены $g_1, \ldots, g_s \in I$, такие, что $\mathrm{LM}\, g_1, \ldots, \mathrm{LM}\, g_s$ порождают мономиальный идеал $(\mathrm{LM}\, I)$.

Следствие 1.13 (Теорема Гильберта о базисе)**.** *Кольцо многочленов $F[x_1, \ldots, x_n]$ нётерово, то есть, всякий идеал в нем конечно порожден.*

Задача 1.1. Для всякого подмножества $I \subset \{1, \ldots, n\}$ можно рассмотреть подполугруппу

$$\mathbb{Z}^n_{\geqslant 0}(I) := \{(a_1, \ldots, a_n) \in \mathbb{Z}^n_{\geqslant 0} \,|\, a_i = 0 \,\forall\, i \in I\}.$$

Сдвинутой координатной подполугруппой называется множество вида $\alpha + \mathbb{Z}^n_{\geqslant 0}(I)$, где $\alpha \in \mathbb{Z}^n_{\geqslant 0}$. Докажите, что всякий коидеал в $\mathbb{Z}^n_{\geqslant 0}$ является объединением конечного числа сдвинутых координатных подполугрупп.

Задача 1.2. Докажите, что из любой бесконечной последовательности мономов можно выбрать подпоследовательность, в которой каждый следующий моном делится на предыдущий.

Задача 1.3. Покажите, что в $F[x, y]$ упорядочения deglex и degrevlex совпадают.

Задача 1.4. Покажите, что на множестве мономов из $F[x, y]$ существует континуум различных упорядочений.

Задача 1.5. Зафиксируем лексикографический порядок с $x \succ y \succ z$. Верно ли, что множество $\{x - z^2, y - z^3\}$ является базисом Грёбнера идеала, порожденного этими двумя многочленами?

Задача 1.6. Приведите пример ассоциативного коммутативного кольца с единицей, не являющегося нётеровым.

2. Матричное задание мономиальных упорядочений

Обозначим через $\mathbb{M}_n$ множество мономов от n переменных $x_1, \ldots, x_n$. Пусть дана матрица $\mathcal{M} \in M_{m,n}(\mathbb{R})$ размера $m \times n$ (при некотором $m \geqslant 1$) с нулевым ядром над $\mathbb{Q}$ и лексикографически положительными столбцами. Тогда можно задать мономиальное упорядочение на $\mathbb{M}_n$ следующим образом:

$$x_1^{\alpha_1} \ldots x_n^{\alpha_n} \prec x_1^{\beta_1} \ldots x_n^{\beta_n} \iff \mathcal{M} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \prec_{\text{lex}} \mathcal{M} \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}.$$

Матрицы с указанными свойствами мы будем называть *мономиальными*. Допуская вольность записи, мы будем писать $\mathcal{M} \cdot P$, подразумевая здесь под P вектор-столбец из степеней переменных монома P. Итак, если матрица $\mathcal{M}$ задает упорядочение $\prec$, то

$$P \prec Q \iff \mathcal{M} \cdot P \prec_{\text{lex}} \mathcal{M} \cdot Q.$$

Произведение первой строки мономиальной матрицы на вектор-столбец степеней монома M мы будем называть *весом* M относительно этой строки.

По определению единичная матрица задает лексикографическое упорядочение. Разумеется, одно и то же упорядочение может быть задано разными матрицами. Так, можно доказать, что лексикографическое упорядочение задается произвольными нижнетреугольными матрицами с положительными элементами на диагонали. Кроме того, можно доказать, что если две мономиальные матрицы задают одно и то же упорядочение и имеют рациональные коэффициенты, то одна получается из другой умножением слева на нижнетреугольную матрицу с положительными элементами на диагонали.

Пример 2.1. Упорядочение deglex с $x_1 \succ x_2 \succ \ldots \succ x_n$ задается матрицей $n \times n$

$$\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 & 1 & 1 \\ 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & & & \\ & & & \ldots & & & \\ & & & & 1 & & \\ & & & & & 1 & \end{pmatrix}.$$

Пример 2.2. Упорядочение degrevlex с $x_1 \prec x_2 \prec \ldots \prec x_n$ можно задать матрицей $n \times n$

$$\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 & 1 & 1 \\ & & & & & & -1 \\ & & & & & -1 & \\ & & & & -1 & & \\ & & & \ldots & & & \\ & & -1 & & & & \\ & -1 & & & & & \end{pmatrix}.$$

или матрицей

$$\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 & 1 & 1 \\ 1 & 1 & 1 & \ldots & 1 & 1 & \\ 1 & 1 & 1 & \ldots & 1 & & \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & & & & & \\ 1 & & & & & & \end{pmatrix}.$$

Мы докажем обратное утверждение:

Теорема 2.1. *Каждое мономиальное упорядочение на $\mathbb{M}_n$ можно задать матрицей $\mathcal{M} \in M_{m,n}(\mathbb{R})$ размера $m \times n$ (при некотором $m \geqslant 1$) с нулевым ядром над $\mathbb{Q}$ и лексикографически положительными столбцами*

Доказательство этого факта было известно давно [7], но в контексте базисов Гребнера было впервые опубликовано в 1986 Лоренцо Робьяно [5, 6]. Робьяно впоследствии развил эти идеи, которые привели к построению так называемых вееров Гребнера (Gröbner Fan) и алгоритму маршрута Гребнера (Gröbner Walk). Мы приведем более простое доказательство, принадлежащее Хуну Хонгу и Фолькеру Вайспфеннингу [3].

Лемма 2.2. *Пусть $\prec$ — допустимый порядок на $\mathbb{Q}^n$ и U — ненулевое подпространство в евклидовом пространстве $\mathbb{Q}^n$. Тогда существует единственная строка $A \in \langle U\rangle_{\mathbb{R}}$, такая, что $\|A\| = 1$ и для любого вектора-столбца $x \in U$ неравенство $A \cdot x > 0$ влечет $x \succ 0$.*

Доказательство. Докажем **существование** такой строки A. Пусть $v_1, \ldots, v_s$ — ортогональный базис пространства $U \subset \mathbb{Q}^n$. Его всегда можно выбрать с условием $v_i \succ 0$. Пусть v_k — максимальный базисный вектор. Положим

$$\beta = \sum_{i=1}^{s} \gamma_i \frac{v_i^T}{\|v_i\|^2},$$

где

$$\gamma_i = \inf\{q \in \mathbb{Q} \mid qv_k \succ v_i\}.$$

Заметим, что $\gamma_i \leqslant 1$ и, вообще говоря, $\gamma_i \in \mathbb{R}$. Положим $A = \frac{\beta}{|\beta|}$.

Пусть $A \cdot x > 0$ для некоторого вектора $x \in U$. Разложим вектор x по базису $v_1, \ldots, v_s$:

$$x = \sum_{i=1}^{s} x_i' v_i, \quad x_i' \in \mathbb{Q}.$$

Тогда, ввиду ортогональности базиса $v_1, \ldots, v_n$, получаем

$$\beta \cdot x = \sum_{i=1}^{s} \gamma_i x_i' > 0.$$

Слегка «пошевелив» γ_i, мы можем выбрать такие рациональные числа γ_i', что по прежнему будет выполняться неравенство

$$\sum_{i=1}^{s} \gamma_i' x_i' > 0,$$

причем

$$\gamma_i' < \gamma_i \text{ при } x_i' > 0,$$
$$\gamma_i' > \gamma_i \text{ при } x_i' < 0$$
$$\text{и } \gamma_i' = 0 \text{ при } x_i' = 0.$$

Тогда $\gamma_i' x_i' < \gamma_i x_i'$ и $\gamma_i' x_i' v_k \prec x_i' v_i$ в силу выбора γ_i. Осталось заметить, что

$$0 = 0v_k \prec \left(\sum_{i=1}^{s} \gamma_i' x_i'\right) v_k \prec \sum_{i=1}^{s} x_i' v_i = x.$$

Теперь докажем **единственность** строки A. Пусть имеются две разные строки A и A' с указанным свойством. По условию $\|A\| = \|A'\| = 1$. Тогда множество

$$S = \{x \in \langle U\rangle_{\mathbb{R}} \mid Ax > 0,\ A'x < 0\}$$

которое есть пересечение двух полупространств в $\langle U\rangle_{\mathbb{R}}$, является непустым и открытым. Значит, в нем существует точка x с рациональными координатами. Тогда $x \in U$, причем $Ax > 0$ и $A'(-x) > 0$, откуда $x \succ 0$ и $-x \succ 0$. Складывая два последних неравенства, получаем противоречие: $0 \succ 0$. □

Доказательсто теоремы. Будем строить искомую матрицу индуктивно. Выберем в качестве ее первой строки A_1 строку, которая существует по доказанной лемме для пространства $U_0 = \mathbb{Q}^n$. Пусть построено k строк $A_1, \ldots, A_k$ этой матрицы. Обозначим за $U_k \subset \mathbb{Q}^n$ подпространство всех рациональных векторов, ортогональных каждой из этих строк, и построим строку A_{k+1} по лемме для этого подпространства U_k. На некотором шаге m мы получим $U_m = \{0\}$, так как размерности пространств U_k уменьшаются на каждом шаге. Таким образом, мы построим требуемую матрицу размера $m \times n$. □

Заметим, что в построенной матрице норма каждой строки равна единице, а сами строки ортогональны друг другу. Матрица мономиального упорядочения с таким свойством будет единственной (а потому ее можно назвать *канонической матрицей* данного мономиального упорядочения). В самом деле, каждая очередная строка этой матрицы по доказанной лемме определяется единственным образом.

Теорема Бухбергера

Зафиксируем допустимое мономиальное упорядочение $\prec$ на множестве мономов.

Определение 2.3. Пусть f и g — ненулевые многочлены, а M — наименьшее общее кратное мономов $\operatorname{LM} f$ и $\operatorname{LM} g$. Построим так называемый *S-полином*

$$S(f,g) := \operatorname{LC} g \frac{M}{\operatorname{LM} f} f - \operatorname{LC} f \frac{M}{\operatorname{LM} g} g.$$

Другими словами, мы домножаем многочлены f и g на мономы минимально возможной степени и берем их линейную комбинацию с тем расчётом, чтобы старшие мономы сократились.

Определение 2.4. Пусть G — множество многочленов. Многочлен $f \in (G)$ *имеет стандартное G-представление*, если f можно записать в виде

$$f = \sum_{g_\alpha \in G} p_\alpha g_\alpha, \tag{1}$$

где $p_\alpha \in F[x_1, \ldots, x_n]$ и $\operatorname{LM} p_\alpha g_\alpha \preccurlyeq \operatorname{LM} f$ для всех α..

Заметим, что всякий многочлен из идеала (G) можно записать в виде (1), но, вообще говоря, требование $\operatorname{LM} p_\alpha g_\alpha \preccurlyeq \operatorname{LM} f$ не будет выполняться.

Теорема 2.5 (Бухбергер)**.** *Следующие условия эквивалентны:*

(1) *Множество G является базисом Грёбнера идеала (G);*
(2) *Всякий многочлен из (G) имеет стандартное G-представление;*
(3) *Для любых двух многочленов из G их S-полином имеет стандартное G-представление;*

Доказательство.
(1) → (2). От противного. Пусть $f \in (G)$ — многочлен с минимальным старшим мономом, не имеющий стандартного G-представления. По предположению $\operatorname{LM} f$ делится на $\operatorname{LM} g$ для некоторого $g \in G$. Тогда можно записать f в виде

$$f = cMg + f',$$

где $\operatorname{LM} cMg = \operatorname{LM} f$, а $\operatorname{LM} f' \prec \operatorname{LM} f$, то есть, для f' существует стандартное G-представление. Поэтому и для f можно построить такое представление. Противоречие.
(2) → (1): очевидно.
(2) → (3): очевидно.
(3) → (2). Снова от противного. Среди всех многочленов $f \in (G)$, не имеющих стандартного G-представления, выберем такой, у которого имеется представление (1) с минимальным мономом $M = \max \operatorname{LM} p_\alpha g_\alpha$, а среди всех таких представлений — то, где количество

слагаемых $p_\alpha g_\alpha$ со старшим мономом M минимально. Тогда $\mathrm{LM}\, f \prec M$, поэтому в правой части есть по крайней мере два слагаемых со страршим мономом M, так как этот моном справа должен сократиться. Пусть это $p_1 g_1$ и $p_2 g_2$. Тогда M делится на $\mathrm{НОК}(\mathrm{LM}\, g_1, \mathrm{LM}\, g_2)$, и линейную комбинацию $p_1 g_1$ и $p_2 g_2$ можно переписать в виде полиномиальной комбинации $S(g_1, g_2)$ и g_2. Старший моном $S(g_1, g_2)$ меньше M, и у этого S-полинома есть стандартное G-представление. Поэтому исходное представление для f можно переписать, уменьшив число слагаемых со старшим мономом M. Противоречие. □

Зафиксируем какой-нибудь алгоритм редукции многочлена по множеству других многоченов, который каким-либо образом разрешает неоднозначности в выборе очередного слагаемого для редукции и в выборе самого редуктора.

Следствие 2.6. *Множество G является базисом Грёбнера идеала (G) тогда и только тогда, когда все S-полиномы пар многочленов из G редуцируются относительно G к нулю.*

Доказательство. □

Задача 2.1. Постройте канонические матрицы упорядочений deglex и degrevlex.

Задача 2.2 (Первый критерий Бухбергера)**.** Пусть все старшие мономы элементов множества G взаимно просты. Докажите, что тогда G является базисом Грёбнера идеала (G).

Задача 2.3. Зависит ли $S(f, g)$ от выбранного мономиального упорядочения?

Задача 2.4. Докажите, что если G — базис Грёбнера идеала (G), то остаток от редукции любого многочлена относительно G определён однозначно. Покажите, что если G — не базис Грёбнера, то разные способы редукции могут приводить к разным остаткам.

Задача 2.5. Пусть G — базис Грёбнера, и в процессе редукции многочлена f относительно G получено разложение

$$f = q_1 g_1 + \ldots + q_s g_s + r,$$

где $g_i \in G$, а r — остаток. Однозначно ли определены «частные» q_i?

Задача 2.6. Определите, являются ли следующие множества базисами Грёбнера порождаемых ими идеалов:

а) $G = \{x^2 - y, x^3 - z\}$, упорядочение degrevlex, $x \succ y \succ z$;
б) $G = \{xy^2 - xz + y, xy - z^2, x - yz^4\}$, упорядочение lex, $x \succ y \succ z$.

3. Отношение редукции и условия слияния

Пусть зафиксирован допустимый мономиальный порядок, и $G = \{g_1, \dots, g_s\}$ — конечное множество многочленов. Пусть f — произвольный многочлен и $g \in G$. Мы будем писать $f \xrightarrow{g} f'$, если найдутся коэффициент $c \in F$ и моном M, такие, что $f' = f - cMg$, причем $\mathrm{LM}\, Mg$ не встречается в f'. Транзитивное замыкание отношений $\xrightarrow{g_1}, \dots, \xrightarrow{g_s}$ будем обозначать через $\xrightarrow{G}$. Отношение эквивалентности, порожденное $\xrightarrow{G}$, будем обозначать через $\xleftrightarrow{G}$.

Предложение 3.1. *Справедливы следующие свойства построенных отношений:*

(1) *Если* $f_1 \xrightarrow{G} f_2$ *и* $f_2 \xrightarrow{G} f_1$, *то* $f_1 = f_2$.
(2) *Если* $f_1 \xrightarrow{G} f_2$, *то для любого монома* M *выполнено* $Mf_1 \xrightarrow{G} Mf_2$.
(3) *Всякая цепочка* $f_1 \xrightarrow{G} f_2 \xrightarrow{G} \dots$ *стабилизируется.*
(4) *Если* $f_1 \xrightarrow{g_i} f_2$, *то для любого многочлена* f_3 *существует* f_4, *такой, что* $f_1 + f_3 \xrightarrow{G} f_4$ *и* $f_2 + f_3 \xrightarrow{G} f_4$.
(5) *Если* $f_1 \xleftrightarrow{G} f_2$ *и* $f_3 \xleftrightarrow{G} f_4$, *то* $f_1 + f_3 \xleftrightarrow{G} f_2 + f_4$.
(6) *Если* $f_1 \xleftrightarrow{G} f_2$, *то для любого многочлена* f *выполнено* $ff_1 \xleftrightarrow{g} ff_2$.
(7) $f \xleftrightarrow{G} 0$ *тогда и только тогда, когда* $f \in (G)$.
(8) $f_1 \xleftrightarrow{G} f_2$ *тогда и только тогда, когда* $f_1 - f_2 \in (G)$.

Теорема 3.2. *Следующие условия на отношение* $\xrightarrow{G}$ *эквивалентны:*

(1) *Для всякого многочлена* f *отношение* $f \xrightarrow{G} 0$ *выполняется тогда и только тогда, когда* $f \in (G)$.
(2) *Если* $f \in (G)$ *не редуцируется относительно* G, *то* $f = 0$.
(3) *Для всякого многочлена* f_1 *существует единственный* f_2, *такой, что* $f_1 \xrightarrow{G} f_2$ *и* f_2 *не редуцируется относительно* $\xrightarrow{G}$.
(4) *Если* $f_1 \xrightarrow{G} f_2$ *и* $f_1 \xrightarrow{G} f_3$, *то существует* f_4, *такой, что* $f_2 \xrightarrow{G} f_4$ *и* $f_3 \xrightarrow{G} f_4$.

Говорят, что в таком случае отношение $\xrightarrow{G}$ *удовлетворяет условиям слияния.*

Предложение 3.3. *Отношение* $\xrightarrow{G}$ *удовлетворяет условиям слияния тогда и только тогда, когда* G *— базис Грёбнера идеала* G.

Алгоритм Бухбергера

Вход: допустимое упорядочение $\prec$, многочлены $f_1, \dots, f_m$;
Выход: базис Грёбнера идеала $(f_1, \dots, f_m)$.

$G := \{f_1, \dots, f_m\}$
$P := \{(g_i, g_j) \mid i < j\}$
while $P \neq \varnothing$ **do**
    выберем $(g_i, g_j) \in P$
    $P := P \setminus \{(g_i, g_j)\}$
    пусть r — остаток от редукции $S(g_i, g_j)$ относительно G
    if $r \neq 0$ **then**
        $P := P \cup \{(g, r) \mid g \in G\}$
        $G := G \cup \{r\}$
return G

Теорема 3.4. *Алгоритм Бухбергера корректен и останавливается за конечное число шагов.*

Заметим, что теперь мы можем алгоритмически решать проблему принадлежности многочлена идеалу: $f \in I$ тогда и только тогда, когда остаток от редукции f относительно базиса Грёбнера идеала I равен нулю.

Определение 3.5. Базис Грёбнера G идеала (G) называется *редуцированным*, если
— для всех $g \in G$ ни один моном в g не делится на старшие мономы $G \setminus \{g\}$;
— старшие коэффициенты всех многочленов из G равны 1.

Задача 3.1. Докажите, что редуцированный базис Грёбнера данного идеала единственен (то есть, он определяется только идеалом и выбранным допустимым упорядочением).

Задача 3.2. Докажите, что два идеала равны тогда и только тогда, когда их редуцированные базисы Грёбнера (при одном и том же упорядочении) совпадают.

Задача 3.3. Предложите алгоритм для построения редуцированного базиса Грёбнера.

Задача 3.4. Предложите алгоритм проверки вложения одного идеала в другой.

Задача 3.5. Определите, принадлежит ли многочлен $xy^3 - z^2 + y^5 - z^3$ идеалу $(-x^3 + y, x^2y - z)$.

Задача 3.6. Пусть числа a, b, c удовлетворяют уравнениям

$$a + b + c = 3,$$
$$a^2 + b^2 + c^2 = 5,$$
$$a^3 + b^3 + c^3 = 7.$$

Докажите, что $a^4 + b^4 + c^4 = 9$. Чему равны суммы $a^5 + b^5 + c^5$ и $a^6 + b^6 + c^6$?

4. Сизигии старших членов

Пусть $G = (g_1, \ldots, g_s)$ — набор многочленов из $F[x_1, \ldots, x_n]$. Многочлены $h_1, \ldots, h_s$ образуют *сизигию* элементов из G, если

$$\sum_{i=1}^{s} h_i g_i = 0.$$

Заметим, что множество всех сизигий $S(G)$ является подмодулем в свободном модуле $F[x_1, \ldots, x_n]^s$.

Мы будем рассматривать *сизигии старших членов* $S(\operatorname{LT} G)$, то есть, наборы $(h_1, \ldots, h_s)$, такие, что

$$\sum_{i=1}^{s} h_i \operatorname{LT} g_i = 0.$$

Сизигия называется *однородной мультистепени* $\alpha = (\alpha_1, \ldots, \alpha_n)$, если $\operatorname{LM} h_i g_i = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$ для всех i.

Заметим, что с каждым S-полиномом $S(g_i, g_j)$, $i < j$, связана однородная сизигия старших членов.

Предложение 4.1. *Множество $\{S_{ij}\}$ образует однородный базис подмодуля сизигий старших членов.*

Пусть $s_1, \ldots, s_k$ — какой-либо однородный базис подмодуля сизигий старших членов набора G. Будем через $s_i \cdot G$ обозначать многочлен

$$\sum_{j=1}^{s} s_{ij} g_j.$$

Теорема 4.2. *Следующие условия эквивалентны:*

(1) *множество G является базисом Грёбнера идеала (G);*
(2) *все многочлены $s_i \cdot G$ имеют стандартное G-представление.*

Эта теорема обобщает теорему Бухбергера (в которой в качестве базиса был выбран базис из сизигий, соответствующих S-полиномам).

Предложение 4.3. *Пусть g_i, g_j и g_k таковы, что $\operatorname{LM} g_k \mid HOK(\operatorname{LM} g_i, \operatorname{LM} g_j)$. Пусть S — однородный базис подмодуля сизигий страших членов. Тогда если $S_{i,k} \in S$ и $S_{j,k} \in S$, то $S \setminus \{S_{i,j}\}$ — тоже базис.*

Это предложение позволяет оптимизировать алгоритм Бухбергера: если пары (g_i, g_k) и (g_j, g_k) уже рассмотрены и $\operatorname{LM} g_k \mid \operatorname{HOK}(\operatorname{LM} g_i, \operatorname{LM} g_j)$, то пару (g_i, g_j) можно не рассматривать.

Исключение неизвестных из систем алгебраических уравнений

Пусть $I \lhd F[x_1, \ldots, x_n]$. Рассмотрим лексикографическое упорядочение с $x_1 \succ \ldots \succ x_n$. Пусть G — базис Грёбнера идеала I, а $I_l = I \cap F[x_{l+1}, \ldots, x_n]$ — идеал в $F[x_{l+1}, \ldots, x_n]$ (*l-й исключающий идеал*).

Теорема 4.4 (Об исключении)**.** *Множество $G \cap F[x_{l+1}, \ldots, x_n]$ является базисом Грёбнера идеала I_l.*

Заметим, что для исключения переменной x_1 на самом деле от упорядочения нам требовалось лишь следующее свойство: *любой моном, содержащий x_1, больше любого монома, зависящего лишь от остальных переменных.* При этом мономы от $x_2, \ldots, x_n$ могли сравниваться друг с другом как угодно. Это позволяет вместо лексикографического порядка рассматривать другие порядки, которые ведут себя «как лексикографический» только по

отношению к исключаемым переменным. Будем называть упорядочение *l-м исключающим*, если для данного l при этом упорядочении справедлива теорема об исключении.

Теорема 4.5 (О продолжении)**.** *Пусть F алгебраически замкнуто. Пусть $I = (f_1, \dots, f_s) \lhd \mathbb{F}[x_1, \dots, x_n]$, и пусть I_1 — первый исключающий идеал. Запишем каждый многочлен f_i в виде*

$$f_i = g_i(x_2, \dots, x_n)x_1^{N_i} + \text{ члены, содержащие } x_1 \text{ в степени } < N_i,$$

где $N_i \geqslant 1$, а g_i — ненулевые многочлены. Пусть $(a_2, \dots, a_n) \in \mathbf{V}(I_1)$ — частичное решение. Тогда если $(a_2, \dots, a_n) \notin \mathbf{V}(g_1, \dots, g_s)$, то существует $a_1 \in \mathbb{F}$, такое, что $(a_1, a_2, \dots, a_n) \in \mathbf{V}(I)$.

Доказательство этой теоремы будет приведено на следующей лекции.

Задача 4.1. Пусть идеал I порождается *биномами* $f_1, \dots, f_s$, то есть, многочленами из двух слагаемых. Покажите, что при любом упорядочении редуцированный базис Грёбнера идеала I тоже состоит из биномов. Покажите также, что остаток от редукции любого одночлена относительно базиса Грёбнера такого идеала снова является одночленом (или нулём).

Задача 4.2. Рассмотрим систему уравнений над полем $F \supset \mathbb{Q}$:

$$x^2 + 2y^2 = 3,$$
$$x^2 + xy + y^2 = 3.$$

Пусть I — соответствующий идеал. Найдите базисы идеалов $I \cap F[x]$ и $I \cap F[y]$. Найдите все решения этой системы. Какие из них рациональны? Найдите наименьшее поле $F \supset \mathbb{Q}$, такое, что все решения принадлежат F^2.

Задача 4.3. Опишите общий вид матрицы l-го исключающего упорядочения.

Задача 4.4. Пусть M — матрица размера $n \times (n+1)$, элементы которой — различные независимые переменные. Пусть G — все миноры размера $n \times n$. Опишите подмодуль сизигий $S(G)$.

Задача 4.5. С помощью базисов Грёбнера, системы компьютерной алгебры и метода множителей Лагранжа найдите точку s на поверхности $x^4 + y^2 + z^2 - 1 = 0$, ближайшую к точке $(1, 1, 1)$ в $\mathbb{R}^3$.

Задача 4.6. Пусть задано семейство алгебраических кривых (например, парабол $4py_0 - x_0^2 = 0$) и задан параметр $r > 0$. Задача — описать геометрическое место точек, равноудаленных от заданной кривой на расстояние r. Такие точки образуют *эквидистанту*. Обычно эквидистанту можно описать алгебраическим уравнением от x, y, r и параметров исходного семейства (в нашем примере — p). Предложите алгоритм, который бы по заданному семейству кривых вычислял бы уравнение эквидистанты с помощью базисов Грёбнера и исключения неизвестных.

5. Результанты, теорема о продолжении и теорема Гильберта о нулях

Напомним, что *результантом* $\mathrm{Res}(f,g)$ двух многочленов

$$f = a_l x^l + \ldots + a_0$$

и

$$g = b_m x^m + \ldots + b_0$$

из $F[x]$ называется определитель матрицы Сильвестра размера $(l+m)\times(l+m)$

$$\begin{pmatrix} a_l & a_{l-1} & \cdots & \cdots & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_l & \cdots & \cdots & \cdots & a_1 & a_0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_0 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & b_m & \cdots & b_1 & b_0 & \cdots & \cdots & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & b_0 \end{pmatrix}.$$

Напомним некоторые свойства результантов.

(1) $\mathrm{Res}(f,g)$ является целочисленным многочленом от коэффициентов многочленов f и g;
(2) $\mathrm{Res}(f,g) = 0$ тогда и только тогда, когда f и g имеют общий множитель положительной степени в $F[x]$, или, что то же самое, когда f и g имеют общий корень в $\bar{F}$;
(3) Существуют такие $u, v \in F[x]$, что $\mathrm{Res}(f,g) = uf + vg$;

Для многочленов от нескольких переменных можно рассматривать результанты $\mathrm{Res}(f,g,x_i)$ по каждой из переменных x_i, считая другие переменные коэффициентами. Заметим, что $\mathrm{Res}(f,g,x_1)$ принадлежит исключающему идеалу $(f,g)_1$.

Пусть поле F алгебраически замкнуто. Напомним, что через $\mathbf{V}(I)$ мы обозначаем *многообразие* идеала I, а через $\mathbf{I}(V)$ — идеал, состоящий из всех многочленов, зануляющихся на многообразии V.

Предложение 5.1. *Пусть* $f, g \in F[x_1, \ldots, x_n]$,

$$f = a_0 x_1^l + \ldots + a_l,\ a_0 \neq 0$$
$$g = b_0 x_1^m + \ldots + b_m,\ b_0 \neq 0,$$

где $a_i, b_j \in F[x_2, \ldots, x_n]$. *Если* $\mathrm{Res}(f,g,x_1) \in F[x_2, \ldots, x_n]$ *равен нулю в точке* $(c_2, \ldots, c_n) \in F^{n-1}$, *то либо* a_0 *или* b_0 *равно нулю в этой точке, либо* $\exists c_1 \in F$, *такое, что* f *и* g *равны нулю в* $(c_1, \ldots, c_n) \in F^n$.

Теорема 5.2 (теорема о продолжении для двух многочленов)**.** *Пусть* $I = (f,g) \subset F[x_1, \ldots, x_n]$, *и пусть* a_0 *и* b_0 *определены как и раньше. Предположим, что* $(c_2, \ldots, c_n) \in \mathbf{V}(I_1)$ *— частичное решение. Тогда если* $(c_2, \ldots, c_n) \notin \mathbf{V}(a_0, b_0)$, *то существует* $c_1 \in F$, *такое, что* $(c_1, \ldots, c_n) \in \mathbf{V}(I)$.

Теорема 5.3 (О продолжении, общая версия)**.** *Пусть* $I = (f_1, \ldots, f_s) \lhd F[x_1, \ldots, x_n]$, *и пусть* I_1 *— первый исключающий идеал. Запишем каждый многочлен* f_i *в виде*

$$f_i = g_i(x_2, \ldots, x_n) x_1^{N_i} + \text{ члены, содержащие } x_1 \text{ в степени} < N_i,$$

где $N_i \geqslant 1$, *а* g_i *— ненулевые многочлены. Пусть* $(c_2, \ldots, c_n) \in \mathbf{V}(I_1)$ *— частичное решение. Тогда если* $(c_2, \ldots, c_n) \notin \mathbf{V}(g_1, \ldots, g_s)$, *то существует* $c_1 \in F$, *такое, что* $(c_1, c_2, \ldots, c_n) \in \mathbf{V}(I)$.

Общая версия теоремы сводится к версии для двух многочленов с помощью так называемого *мультирезультанта*

$$\mathrm{Res}(f_1, u_2 f_2 + \ldots + u_s f_s) = \sum_\alpha h_\alpha(x_2, \ldots, x_n) u^\alpha,$$

где $u_2, \ldots, u_s$ — формальные новые переменные.

Теорема 5.4 (Слабая теорема Гильберта о нулях)**.** *Пусть F алгебраически замкнуто. Пусть $I \subset F[x_1, \ldots, x_n]$ — идеал, такой, что $\mathbf{V}(I) = \varnothing$. Тогда $I = (1)$.*

Теорема 5.5 (Теорема Гильберта о нулях)**.** *Пусть F алгебраически замкнуто и $I \subset F[x_1, \ldots, x_n]$ — идеал. Тогда $f \in \mathbf{I}(\mathbf{V}(I))$ в том и только том случае, когда $\exists m : f^m \in I$.*

Задача 5.1. Пусть $f, g \in F[x]$. Найдите связь между $\mathrm{Res}(f, g)$ и $\mathrm{Res}(g, f)$.

Задача 5.2. Пусть $f, g \in F[x]$. Разделим f на g с остатком: $f = qg + r$, где $\deg r < \deg g$. Докажите, что

$$\mathrm{Res}(f, g) = (-1)^{m(l - \deg r)} b_0^{l - \deg r} \mathrm{Res}(r, g).$$

Задача 5.3. Используя результаты предыдущих задач, предложите алгоритм для вычисления результанта $\mathrm{Res}(f, g)$, аналогичный алгоритму Евклида.

Задача 5.4. Пусть $f, g \in F[x_1, x_2]$. Верно ли, что $\mathrm{Res}(f, g, x_1)$ порождает исключающий идеал $(f, g)_1$?

Задача 5.5. Пусть f, g — многочлены положительной степени из $\mathbb{C}[x]$.

(1) Что можно сказать о корнях многочлена $\mathrm{Res}(f(x), g(y - x), x)$?
(2) Пусть $f(0) \neq 0$. Постройте многочлен, корнями которого будут в точности произведения корней f и g.

Задача 5.6. Докажите, что если поле не является алгебраически замкнутым, то любое многообразие можно задать одним уравнением.

Задача 5.7. Пусть F — произвольное поле. Пусть S — множество многочленов из $F[x_1, \ldots, x_n]$, не равных нулю ни в одной точке. Пусть I — идеал, такой, что $I \cap S = \varnothing$. Докажите, что $\mathbf{V}(I) \neq \varnothing$.

6. Другое доказательство теоремы о продолжении

Мы приведем альтернативное доказательство теоремы о продолжении, не использующее результанты, а опирающееся только на теорию базисов Грёбнера. Это доказательство было опубликовано Петером Шауенбургом в 2007 году [**?**].

Для этого нам потребуется определить базис Грёбнера в кольце многочленов $R[x_1, \dots, x_n]$, где R — произвольное коммутативное кольцо. Возьмем определение в духе теоремы Бухбергера: множество G (не содержащее нуля) будем называть базисом Грёбнера при данном упорядочении, если для всякого S-полинома его элементов имеется стандартное представление.

Пусть R — кольцо многочленов $F[z_1, \dots, z_t]$ над полем F. Тогда $R[x_1, \dots, x_n]$ можно рассматривать как кольцо многочленов от $x_1, \dots, x_n, z_1, \dots, z_t$ над F. Рассмотрим блочное упорядочение, исключающее переменные $z_1, \dots, z_t$. Тогда базис Грёбнера над F будет и базисом Грёбнера над R (докажите это!).

Предложение 6.1. *Пусть G — базис Грёбнера идеала $I \lhd R[x]$, а $\sigma : R \to F$ — гомоморфизм. Предположим, что G содержит многочлен, старший коэффициент которого не лежит в ядре σ. Пусть g — многочлен из G минимальной степени с таким свойством. Тогда $\sigma(I) = (\sigma(g))$.*

Доказательство. Пусть $D = \deg g$. Пусть $h \in G$ и $\deg h = d < D$. Покажем, что тогда $\sigma(h) = 0$. Для этого докажем, что для любого $\delta \in \mathbb{N}$ выполнено $\deg \sigma(h) \leqslant \deg h - \delta$. Для $\delta = 1$ это так, потому что из минимальности g следует, что $\sigma(\mathrm{LC}_R(g)) = 0$. Для шага индукции возьмем S-полином

$$S(h, g) = \mathrm{LC}_R(g) h x^{D-d} - \mathrm{LC}_R(h) g,$$

запишем его стандартное представление $\sum_{j \in G} f_j j$, где $\deg f_j j < D$, и воспользуемся предположением индукции для j:

$$\deg \sigma(f_j j) = \deg \sigma(f_j) + \deg \sigma(j) \leqslant \deg f_j + \deg j - \delta < D - \delta,$$

откуда

$$\deg \sigma(S(h, g)) = \deg \sigma(h) + D - d < D - \delta,$$

так что $\deg \sigma(h) \leqslant d - (\delta + 1)$.

Пусть теперь $h \in G$ и $d = \deg h \geqslant D$. Покажем, что $\sigma(h) \in (\sigma(g))$. Снова рассмотрим S-полином

$$S(h, g) = \mathrm{LC}_R(g) h - \mathrm{LC}_R(h) g x^{d-D}$$

и его стандартное представление $\sum_{j \in G} f_j j$, где $\deg f_j j < d$, откуда $\deg j < d$. Будем считать, что для j уже доказано, что $\sigma(j) \in (\sigma(g))$. Отсюда

$$\mathrm{LC}_R(g) h = S(h, g) + \mathrm{LC}_R(h) g x^{d-D} = \sum_{j \in G} f_j j + \mathrm{LC}_R(h) g x^{d-D}.$$

Так как $\sigma(\mathrm{LC}_R(g)) \neq 0$, то

$$\sigma(h) \in (\sigma(j) | f_j \neq 0) + (\sigma(g)) \subset (\sigma(g)).$$

□

Теорема 6.2 (О продолжении)**.** *Пусть F алгебраически замкнуто, $I \lhd F[x_1, \dots, x_n]$, I_1 — первый исключающий идеал и $(c_2, \dots, c_n) \in \mathbf{V}(I_1)$. Предположим, что в I имеется многочлен*

$$f = f_N(x_2, \dots, x_n) x_1^N + \text{ члены, содержащие } x_1 \text{ в степени } < N,$$

где $N \geqslant 1$ и $f_N(c_2, \dots, c_n) \neq 0$. Тогда существует $c_1 \in F$, такое, что $(c_1, c_2, \dots, c_n) \in \mathbf{V}(I)$.

Доказательство. Пусть $R = F[x_2, \ldots, x_n]$, а $\sigma : R \to F$ — гомоморфизм вычисления в точке $(c_2, \ldots, c_n)$. Пусть G — базис Гребнера I в $R[x_1]$ (например, базис Грёбнера I в $F[x_1, \ldots, x_n]$ при подходящем блочном упорядочении). Запишем стандартное представление для f:

$$f = \sum_{g \in G} f_g g,$$

где $\deg_{x_1} f_g g \leqslant \deg_{x_1} f$. Тогда $f_N = \mathrm{LC}_R f \in (\mathrm{LC}_R(g) | g \in G)$. Значит, не все $\mathrm{LC}_R(g)$ обращаются в 0 в точке $(c_2, \ldots, c_n)$. По предыдущему предложению существует $g \in G$, такой, что $\sigma(I) = (\sigma(g))$. Теперь в качестве c_1 можно выбрать корень $\sigma(g)$ в $F[x_1]$. □

Можно ли обобщить эти результаты на случай, когда исключается более одной переменной? Оказывается, да, но только теперь придется потребовать, чтобы *все* старшие коэффициенты элементов базиса Грёбнера не обращались в ноль.

Для этого нам понадобится следующая лемма, показывающая, когда базис Грёбнера остаётся базисом Грёбнера при специализации.

Лемма 6.3. *Пусть G — базис Грёбнера в кольце $R[x_1, \ldots, x_n]$, а $\sigma : R \to F$ — гомоморфизм. Предположим, что для всех $g \in G$, таких, что $\sigma(\mathrm{LC}(g)) = 0$, выполнено $\sigma(g) = 0$. Тогда $\sigma(G)$ — базис Грёбнера в $F[x]$.*

Доказательство. Возьмём $g, h \in G$, такие, что $\mathrm{LC}(g), \mathrm{LC}(h) \notin \operatorname{Ker} \sigma$. Рассмотрим S-полином

$$S(g,h) = \frac{\mathrm{LT}(g)h - \mathrm{LT}(h)g}{\gcd(\mathrm{LM}(g), \mathrm{LM}(h))} \in (G).$$

По построению $\mathrm{LM}(S(g,h)) \prec m := \mathrm{HOK}(\mathrm{LM}(g), \mathrm{LM}(h))$. Итак, в стандартном представлении $S(g,h) = \sum_{j \in G} f_j j$ должно быть $\mathrm{LM}(f_j)\,\mathrm{LM}(j) \prec m$, если $f_j \neq 0$. Применим σ:

$$\sigma(S(g,h)) = \sum_{j \in G} \sigma(f_j)\sigma(j).$$

Заметим, что это выражение отличается лишь множителем от $S(\sigma(g), \sigma(h))$, и что по предположению $m = \mathrm{HOK}(\mathrm{LM}(\sigma(g)), \mathrm{LM}(\sigma(h)))$, так что $\sigma(G)$ — базис Грёбнера в $F[x_1, \ldots, x_n]$. □

Следствие 6.4. *Пусть F алгебраически замкнуто. Пусть $I \lhd F[x_1, \ldots, x_n]$, и $\mathbf{b} \in \mathbf{V}(I_l)$ — частичное решение. Пусть G — базис Грёбнера идеала I относительно упорядочения, исключающего первые l переменных. Пусть $R = F[x_{l+1}, \ldots, x_n]$. Если $\mathbf{b}$ не зануляет ни один элемент множества $\mathrm{LC}_R(G \setminus R)$, то частичное решение $\mathbf{b}$ продолжается до полного решения.*

Доказательство. Пусть $\sigma : R \to F$ — гомоморфизм вычисления в точке $\mathbf{b}$. По предположению, если $\mathrm{LC}_R(g)(\mathbf{b}) = 0$ для $g \in G$, то $g \in R$, а значит, $g \in I_l$, то есть, $\sigma(g) = 0$. По предыдущей лемме $\sigma(G) \setminus \{0\} = \sigma(G \setminus R)$ — базис Грёбнера $\sigma(I)$, причем его элементы не являются константами. Поэтому $\mathbf{V}(\sigma(I)) \neq \varnothing$. Но $\mathbf{V}(\sigma(I)) \times \{\mathbf{b}\} \subset \mathbf{V}(I)$. □

Пусть $\pi_l : F^n \to F^{n-l}$ — проекция на последние $n - l$ координат.

Теорема 6.5 (Теорема о замыкании)**.** *Пусть F алгебраически замкнуто. Пусть $I \lhd F[x_1, \ldots, x_n]$ и $1 \leqslant l < n$. Существует идеал $J \lhd F[x_{l+1}, \ldots, x_n]$, такой, что*

(1) $I_l \subset J$;
(2) $\pi_l(\mathbf{V}(I)) \cup \mathbf{V}(J) = \mathbf{V}(I_l)$;
(3) $\overline{\mathbf{V}(I_l) \setminus \mathbf{V}(J)} = \mathbf{V}(I_l)$.

Задача 6.1. Докажите утверждение, сформулированное в начале лекции (о том, что базис Грёбнера над F при подходящем блочном упорядочении будет базисом Грёбнера и над R).

Задача 6.2. На примере идеала $(x^2+y^2+z^2+2, 3x^2+4y^2+4z^2+5)$ докажите, что теорема о замыкании не справедлива для поля $\mathbb{R}$.

Задача 6.3. Рассмотрим идеал

$$((x_2-x_3)x_1^2+x_1x_2-1, (x_2-x_3)x_1^2+x_1x_3-1) \lhd \mathbb{C}[x_1,x_2,x_3].$$

Пусть $l=1$. Найдите многообразие J из теоремы о замыкании для этого идеала.

7. Алгебро-геометрический словарь

Доказательства утверждений этой лекции можно найти в главе 4 книги [2].

Пусть, как и раньше, F — алгебраически замкнутое поле, $\mathbf{V}(I)$ — многообразие, соответствующее идеалу, а $\mathbf{I}(S)$ — идеал, состоящий из всех многочленов, обнуляющихся на точках множества $S \subset F^n$.

Теорема Гильберта о нулях утверждает, что $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$.

Теорема 7.1 (соответствие идеал – многообразие)**.**

(1) *Отображения*

$$\textit{аффинные многообразия} \xrightarrow{\mathbf{I}} \textit{идеалы}$$

и

$$\textit{идеалы} \xrightarrow{\mathbf{V}} \textit{аффинные многообразия}$$

обращают включение. Кроме того, отображение $\mathbf{I}$ *взаимно однозначно, то есть равенство*

$$\mathbf{V}(\mathbf{I}(V)) = V$$

справедливо для любого многообразия V*.*

(2) *Если* F *алгебраически замкнуто и мы ограничиваемся радикальными идеалами, то отображения*

$$\textit{аффинные многообразия} \xrightarrow{\mathbf{I}} \textit{радикальные идеалы}$$

и

$$\textit{радикальные идеалы} \xrightarrow{\mathbf{V}} \textit{аффинные многообразия}$$

являются взаимно обратными биекциями, которые обращают включения.

Естественным образом возникают три алгоритмических вопроса:

(1) Существует ли алгоритм вычисления образующих радикала данного идеала?
(2) Существует ли алгоритм проверки радикальности данного идеала?
(3) Возможно ли проверить принадлежность конкретного многочлена f радикалу заданного идеала I?

Ответы на все три вопроса положительный, хотя в общем виде алгоритмы решения первых двух задач достаточно сложны. Мы отдельно рассмотрим их в нульмерном случае. Понятно, что на третий вопрос можно ответить, решив первый. Однако мы приведем более простое решение.

Предложение 7.2. *Пусть* $I = (f_1, \dots, f_m) \lhd F[x_1, \dots, x_n]$*. Тогда* $f \in \sqrt{I}$ *тогда и только тогда, когда* $1 \in (f_1, \dots, f_m, 1 - tf) \lhd F[x_1, \dots, x_n, t]$*.*

Пусть $I, J \lhd F[x_1, \dots, x_m]$. *Суммой* идеалов $I + J$ называется множество

$$I + J = \{f + g \mid f \in I, g \in J\}.$$

Теорема 7.3.

(1) $I + J$ *— наименьший идеал, содержащий* I *и* J*.*
(2) *Если* $I = (f_1, \dots, f_r)$ *и* $J = (g_1, \dots, g_s)$*, то* $I + J = (f_1, \dots, f_r, g_1 \dots, g_s)$*.*
(3) $\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J)$*.*

Произведением идеалов $I \cdot J$ называется идеал, порожденный всеми полиномами fg, где $f \in I$ и $g \in J$.

Теорема 7.4.

(1) *Если* $I = (f_1, \dots, f_r)$ *и* $J = (g_1, \dots, g_s)$*, то* $I \cdot J = (f_i g_j \mid 1 \leqslant i \leqslant r; 1 \leqslant j \leqslant s)$*.*
(2) $\mathbf{V}(I \cdot J) = \mathbf{V}(I) \cup \mathbf{V}(J)$*.*

Пересечением идеалов $I \cap J$ называется их теоретико-множественное пересечение.

Теорема 7.5.

(1) $I \cap J$ — *тоже идеал, причем* $IJ \subset I \cap J$;
(2) $I \cap J = (tI + (1-t)J) \cap F[x_1, \ldots, x_n]$;
(3) $\mathbf{V}(I \cap J) = \mathbf{V}(I) \cup \mathbf{V}(J)$;
(4) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$;
(5) *Если* $I = (f)$ *и* $J = (g)$ — *главные идеалы, то* $I \cap J$ — *тоже главный идеал, порожденный* $НОК(f, g)$.

Эта теорема, в частности, позволяет находить НОД многочленов от нескольких переменных.

Предложение 7.6. *Пусть* $S \subset F^n$. *Тогда* $\mathbf{V}(\mathbf{I}(S))$ — *наименьшее многообразие, содержащее* S.

Замыканием Зарисского подмножества $S \subset F^n$ называется наименьшее многообразие, содержащее это множество. Оно обозначается через $\bar{S}$ и равно $\mathbf{V}(\mathbf{I}(S))$.

Пусть $I, J \lhd F[x_1, \ldots, x_n]$. *Частным* этих идеалов называется множество

$$I : J = \{f \in F[x_1, \ldots, x_n] \mid fg \in I \, \forall g \in J\}.$$

Теорема 7.7.

(1) $I : J$ — *идеал, причем* $I \subset I : J$;
(2) $\mathbf{V}(I : J) \supset \overline{\mathbf{V}(I) \setminus \mathbf{V}(J)}$;
(3) *Если* F *алгебраически замкнуто, а* I *радикален, то* $\mathbf{V}(I : J) = \overline{\mathbf{V}(I) \setminus \mathbf{V}(J)}$;
(4) *Если* V *и* W — *многообразия, то* $\mathbf{I}(V) : \mathbf{I}(W) = \mathbf{I}(V \setminus W)$;
(5) *Если* $I \cap (g) = (h_1, \ldots, h_s)$, *то* $I : (g) = (h_1/g, \ldots, h_s/g)$.

Задача 7.1. Докажите, что $h = \gcd(f, g)$ тогда и только тогда, когда h порождает наименьший главный идеал, содержащий f и g.

Задача 7.2. Предложите алгоритм для вычисления образующих идеала $\sqrt{(f)}$, где $f \in F[x_1, \ldots, x_n]$.

Задача 7.3. Приведите пример, показывающий, что равенство $\sqrt{IJ} = \sqrt{I}\sqrt{J}$ может не выполняться.

Задача 7.4. Имея алгоритм вычисления пересечения двух идеалов, можно построить алгоритм пересечения произвольного количества идеалов, однако он не будет эффективным. Покажите, что для нахождения пересечения нескольких идеалов достаточно обойтись одним вычислением базиса Грёбнера:

$$I_1 \cap I_2 \cap \ldots \cap I_s = (t_1 I_1 + \ldots + t_s I_s + (t_1 + \ldots + t_s - 1)) \cap F[x_1, \ldots, x_n],$$

где $t_1, \ldots, t_s$ — новые переменные.

Задача 7.5. Два идеала I и J называются *комаксимальными*, если $I + J = (1)$.

(1) Докажите, что если F алгебраически замкнуто, то I и J комаксимальны тогда и только тогда, когда $\mathbf{V}(I) \cap \mathbf{V}(J) = \varnothing$. Верно ли это для произвольного поля?
(2) Докажите, что если I и J комаксимальны, то $IJ = I \cap J$. Верно ли обратное утверждение?
(3) Пусть I и J комаксимальны. Докажите, что I^r и J^s комаксимальны для любых натуральных r и s.

Задача 7.6. Докажите следующие равенства:

(1) $I : F[x_1, \ldots, x_n] = I$;
(2) $IJ \subset K$ в том и только том случае, когда $I \subset K : J$;
(3) $J \subset I$ в том и только том случае, когда $I : J = F[x_1, \ldots x_n]$;
(4) $(\cap_{i=1}^r I_i) : J = \cap_{i=1}^r (I_i : J)$;
(5) $I : (\sum_{i=1}^r J_i) = \cap_{i=1}^r (I : J_i)$;
(6) $(I : J) : K = I : JK$;

8. Нульмерный случай

Теорема 8.1. *Пусть поле F алгебраически замкнуто и $I \triangleleft F[x_1, \ldots, x_n]$. Следующие условия эквивалентны:*

(1) *Алгебра $A = F[x_1, \ldots, x_n]/I$ конечномерна над F;*
(2) $\mathbf{V}(I) \subset F^n$ *конечно;*
(3) *Если G — базис Грёбнера идеала I, то для каждой переменной x_i найдётся $m_i \geqslant 0$, такое, что $x_i^{m_i} = \mathrm{LM}\, g$ для некоторого $g \in G$;*
(4) *Для каждой переменной x_i исключающий идеал $I \cap F[x_i]$ является ненулевым.*

Идеалы, удовлетворяющие этой теореме, называются *нульмерными*.

Чтобы найти образующие главных идеалов $I \cap F[x_i]$ можно было бы вычислить базис Грёбнера при лексикографическом упорядочении, в котором x_i — самая младшая переменная. Однако этот метод крайне неэффективен. Гораздо эффективнее найти линейную зависимость между образами степеней x_i

$$\{1, [x_i], [x_i]^2, \ldots\}$$

в алгебре A.

Предложение 8.2. *Пусть I — нульмерный идеал. Пусть p_i — образующие элементы идеалов $I \cap F[x_i]$ со старшим коэффициентом* 1*, и пусть $p_{i,red}$ — результат освобождения p_i от кратных корней. Тогда*

$$\sqrt{I} = I + (p_{1,red}, \ldots, p_{n,red})\,.$$

Теорема 8.3. *Пусть F алгебраически замкнуто, I — нульмерный идеал в $F[x_1, \ldots, x_n]$ и $A = F[x_1, \ldots, x_n]/I$. Тогда $\dim_F A$ не меньше числа точек в $\mathbf{V}(I)$, причем равенство имеет место тогда и только тогда, когда идеал I радикален.*

Далее мы рассмотрим задачу преобразования базис Грёбнера G, построенного для какого-либо упорядочения, к лексикографическому базису Грёбнера. В нульмерном случае эту задачу решает алгоритм FGLM (по первым буквам фамилий его создателей — Faugère, Gianni, Lazard и Mora). Алгоритм перебирает мономы в порядке лексикографического возрастания. На каждом шаге алгоритма поддерживается список G_{lex}, который изначально является пустым, и в котором в конце концов оказывается ответ, а также список B_{lex}, состоящий из лексикографически нестарших мономов идеала (образы которых порождают A). Для каждого рассматриваемого монома x^α (начиная с 1) алгоритм выполняет следующие шаги:

(1) Основной цикл. Вычисляем $\overline{x^\alpha}$ (остаток относительно G).
   a) Если этот моном линейно зависим с остатками элементов из B_{lex}, то существует линейная зависимость
   $$\overline{x^\alpha} - \sum_j c_j \overline{x^{\alpha_j}} = 0,$$
   где $x^{\alpha_j} \in B_{\mathrm{lex}}$ и $c_j \in F$. Тогда
   $$g = x^\alpha - \sum_j c_j x^{\alpha_j} \in I.$$
   Мы добавляем этот многочлен g в конец списка G_{lex}. Заметим, что его старшим термом является именно x^α. Если x^α — это степень самой старшей переменной x_1, то алгоритм заканчивается, и мы возвращаем G_{lex} в качестве ответа.
   b) Если $\overline{x^\alpha}$ линейно независим с остатками элементов из B_{lex}, мы добавляем x^α в конец списка B_{lex}.
(2) Заменяем x^α на лексикографически следующий моном, не делящийся ни на один из мономов множества $\mathrm{LM}_{\mathrm{lex}} G_{\mathrm{lex}}$ и продолжаем цикл.

Задача 8.1. Покажите, как можно было бы реализовать функцию NextMonomial, возвращающую в алгоритме FGLM следующий в лексикографическом порядке моном, не делящийся ни на один из мономов данного конечного множества.

Задача 8.2. Используя идеи алгоритма FGLM, предложите алгоритм, вычисляющий лексикографический базис Грёбнера идеала $\mathbf{I}(p_1, \ldots, p_m)$, где p_i — точки из F^n.

Задача 8.3. Пусть I — нульмерный идеал в $F[x_1, \ldots, x_n]$. Пусть $m_{x_i} : A \to A$ — оператор умножения на образ переменной x_i в алгебре $A = F[x_1, \ldots, x_n]/I$. Покажите, что идеал I радикален тогда и только тогда, когда все операторы m_{x_i} диагонализируемы.

Задача 8.4 («Лемма о форме»)**.** Пусть I — нульмерный радикальный идеал в $F[x_1, \ldots, x_n]$, причем x_n-координаты всех точек из $\mathbf{V}(I)$ различны. Пусть G — редуцированный лексикографический базис Грёбнера (где переменная x_n является младшей). Покажите, что G состоит из n многочленов

$$g_1 = x_1 + h_1(x_n),$$
$$\ldots$$
$$g_{n-1} = x_{n-1} + h_{n-1}(x_n),$$
$$g_n = x_n^m + h_n(x_n),$$

где $m = |\mathbf{V}(I)|$, а степени всех многочленов h_i строго меньше m.

Задача 8.5. Покажите, что неравенство $|\mathbf{V}(I)| \leqslant \dim_F F[x_1, \ldots, x_n]/\sqrt{I}$ может быть строгим, если поле не является алгебраически замкнутым.

9. Алгоритм F4

Алгоритм F4 был предложен Ж.-Ш. Фожером в 1999 г. Этот алгоритм вычисляет базис Грёбнера идеала в кольце многочленов с помощью серии стандартных линейноалгебраических процедур: приведений матриц к ступечатому виду. Он является одним из самых быстрых на сегодняшний день.

Пусть есть некоторое конечное множество многочленов F. По этому множеству строится большая разреженная матрица, строки которой соответствуют многочленам из F, а столбцы — мономам. В матрице записаны коэффициенты многочленов при соответствующих мономах. Столбцы матрицы отсортированы согласно выбранному мономиальному упорядочению (старший моном соответствует первому столбцу). Приведение такой матрицы к ступенчатому виду позволяет узнать базис линейной оболочки многочленов из F в пространстве многочленов.

Пусть в классическом алгоритме Бухбергера требуется провести шаг редукции многочлена f относительно g, и при этом g должен быть домножен на моном M. В алгоритме F4 в матрицу будут специально помещены f и Mg. Утверждается, что можно заранее подготовить множество всех потенциальных домноженных редукторов, которые могут потребоваться, и поместить их заранее в матрицу.

Более общо, пусть нам требуется отредуцировать многочлен f относительно множества F. Для этого мы

(1) добавляем f в матрицу;
(2) строим носитель $\mathcal{M}$ многочлена f (множество мономов);
(3) если $\mathcal{M}$ пусто, то заканчиваем процедуру;
(4) выбираем максимальный моном M в $\mathcal{M}$ (и выкидываем его из $\mathcal{M}$);
(5) если M не делится ни на один старший моном элементов F, то переходим к шагу (3);
(6) иначе выбираем редуктор $r \in F$ (и дополнительный множитель t): тогда $M = \mathrm{LM}\, tr$;
(7) добавляем tr в матрицу;
(8) добавляем мономы многочлена tr (кроме старшего M) ко множеству $\mathcal{M}$;
(9) переходим к шагу (3).

Эта процедура пополнения матрицы домноженными редукторами называется *символьным препроцессингом*.

Кроме того, вместо S-полиномов можно поместить в матрицу их левые и правые части (при редукции одной строки по другой автоматически получится S-полином). Наконец, третьим отличием от алгоритма Бухбергера является то, что в алгоритме F4 разрешается поместить в одну матрицу части сразу нескольких S-полиномов, выбранных согласно какой-либо стратегии. Так, если на каждом шаге выбирается один S-полином, то он повторяет классический алгоритм Бухбергера. Другая крайность — когда на очередном шаге редуцируется множество всех имеющихся S-полиномов. Это тоже не очень эффективно из-за больших размеров матриц. Автор алгоритма Ж.-Ш. Фожер предложил *нормальную стратегию* выбора S-полиномов для редукции, согласно которой выбираются S-полиномы с наименьшей степенью левых и правых частей. Она дает хорошие эмпирические результаты для упорядочения DegRevLex и ее выбор является естественным для однородных идеалов.

В алгоритм можно внести несколько естественных усовершенствований. Как и в классическом алгоритме вычисления базиса Грёбнера, можно применять критерии Бухбергера для отсеивания заведомо ненужных S-полиномов.

Псевдокод алгоритма F4 можно найти в работах [9, 10].

Алгоритм F5

Алгоритм F5 вычисления базиса Грёбнера был предложен Ж.-Ш. Фожером в 2002 году. Мы рассмотрим его матричную версию (в духе алгоритма F4), работающую для однородных многочленов. Основная процедура этого алгоритма вычисляет d-базис Грёбнера, то есть, подмножество базиса Грёбнера, относительно которого редуцируются к нулю все многочлены из идеала степени не выше, чем d.

В алгоритме F5 каждому полученному многочлену сопоставляется *сигнатура* (пара из монома и номера образующей), кодирующая информацию о происхождении этого многочлена. Основная идея — не включать по возможности в матрицы те строки, которые заведомо будут линейно зависимы с остальными (то есть, будут редуцироваться к нулю.) Для этого редукции ограничиваются такими, которые не изменяют сигнатуру элементов, а также среди очередных обрабатываемых многочленов рассматриваются лишь те, моном сигнатуры которых не делится ни на один старший моном уже найденных элементов базиса.

Последовательность элементов коммутативного кольца называется *регулярной*, если первый ее элемент — не ноль, а каждый следующий не является делителем нуля по модулю предыдущего. Гарантируется, что матрицы, генерируемые в ходе работы алгоритма F5, будут заведомо полного ранга (то есть, не будет происходить редукций к нулю), если исходная последовательность многочленов регулярна.

Пусть $f_1, \ldots, f_m$ — однородные многочлены степеней $d_1 \leqslant d_2 \leqslant \ldots \leqslant d_m$ соответственно. Пусть $I = (f_1, \ldots, f_m)$. Очевидно, что если $f \in I$ — однородный многочлен степени d, то f лежит в подпространстве

$$\langle M f_i \mid 1 \leqslant i \leqslant m,\ M \in \mathbb{M},\ \deg M = d - d_i \rangle$$

идеала I. Поэтому для поиска d-базиса Грёбнера идеала I достаточно просто взять ступенчатый базис подпространства

$$I_{\leqslant d} = \langle M f_i \mid 1 \leqslant i \leqslant m,\ M \in \mathbb{M},\ \deg M \leqslant d - d_i \rangle.$$

и выбрать из него элементы с минимальными в смысле отношения делимости старшими мономами (это делается так же, как и в алгоритме F4). Для поиска обычного базиса Грёбнера можно последовательно вычислять d-базисы Грёбнера для очередных значений d и проверять, что полученная система действительно является базисом Грёбнера исходного идеала.

Однако образующих $M f_i$ подпространства $I_{\leqslant d}$ слишком много, и между ними могут быть линейные зависимости. Хочется по возможности

(1) не использовать образующие, заведомо линейно выражающиеся через другие образующие;
(2) учитывать соотношения между образующими, полученные на предыдущих шагах (при меньших d).

Будем перебирать образующие вида $M f_i$ сначала по возрастанию номера i, а затем — по моному M (относительно выбранного упорядочения). Заметим, что если прибавить к текущей образующей произвольную линейную комбинацию предыдущих образующих (то есть, сделать «треугольную» замену), то линейная оболочка $I_{\leqslant d}$ не изменится. Мы будем делать такие замены, но для каждой новой образующей

$$M f_k + \sum_{i=1}^{k} p_i f_i, \quad p_i \in F[x_1, \ldots, x_n],$$

где либо $p_k = 0$, либо $\mathrm{LM}\, p_k \prec M$, мы будем запоминать исходную образующую $M f_k$, из которой она была получена треугольной заменой. Будем говорить, что пара (k, M) является *сигнатурой* такой образующей. Сигнатуру следует воспринимать как специальную «метку», приписанную многочлену, полученному в ходе вычислений. Наши правила

преобразования базиса разрешают прибавлять к многочлену лишь комбинации многочленов с меньшими сигнатурами (и в ходе приведения матрицы к ступенчатому виду тоже разрешаются лишь такие преобразования первого типа).

Предложение 9.1 (Критерий F5)**.** *Пусть (k, M) — сигнатура очередной рассматриваемой образующей h. Если $M \in \mathrm{LM}(f_1, \ldots, f_{k-1})$, то h линейно выражается через образующие с меньшими сигнатурами (и, следовательно, h можно не учитывать).*

Доказательство. Запишем h в виде

$$h = Mf_k + \sum_{i=1}^{k} p_i f_i, \quad p_i \in F[x_1, \ldots, x_n],$$

где либо $p_k = 0$, либо $\mathrm{LM}\, p_k \prec M$. По предположению $\exists g \in (f_1, \ldots, f_{k-1})$, такой, что $\mathrm{LM}\, g = M$. Можем считать, что $\mathrm{LC}\, g = 1$. Пусть

$$g = \sum_{j=1}^{k-1} q_j f_j = M + t,$$

где $\mathrm{LM}\, t \prec \mathrm{LM}\, g = M$. Тогда

$$h = (g - t)f_k + \sum_{i=1}^{k} p_i f_i = \sum_{j=1}^{k-1} q_j f_k f_j - tf_k + \sum_{i=1}^{k} p_i f_i =$$
$$= \sum_{i=1}^{k-1} (q_i f_k + p_i) f_i + (p_k - t) f_k,$$

и при этом либо $p_k - t = 0$, либо $\mathrm{LM}(p_k - t) \prec M$. Таким образом, h можно записать в виде линейной комбинации образующих с меньшей сигнатурой. □

Заметим, что в этом утверждении использовалось знание о «тривиальных» сизигиях $f_j f_k - f_k f_j = 0$ между образующими идеала. Если бы нам была бы дополнительно известна информация о еще каких-либо сизигиях, мы тоже могли бы ее использовать.

Перейдем теперь к пункту (2) наших пожеланий. Будем строить образующие для подпространства $I_{\leqslant d}$ исходя из ступенчатого базиса подпространства $I_{\leqslant d-1}$. Пусть h — элемент ступенчатого базиса $I_{\leqslant d-1}$ с сигнатурой (k, M). Пусть x_s — старшая переменная монома M. Рассмотрим многочлены $hx_s, hx_{s+1}, \ldots, hx_n$ с сигнатурами $(k, x_s M), (k, x_{s+1} M), \ldots, (k, x_n M)$ соответственно. Выберем те из них, которые не отбрасываются критерием F5 и добавим к списку образующих подпространства $I_{\leqslant d}$. Такой выбор дополнительных множителей-переменных гарантирует, что мы рассмотрим все возможные мономы сигнатуры, причем ровно по одному разу (конечно, кроме тех, которые отбрасываются критерием F5).

Предложение 9.2. *Если исходная последовательность многочленов $f_1, \ldots, f_m$ регулярна, то на каждом шаге d все построенные образующие пространства $I_{\leqslant d}$ линейно независимы, то есть, образуют базис. Другими словами, для регулярных однородных многочленов матричный алгоритм F5 исключает все редукции к нулю.*

Доказательство. Пусть h — рассматриваемая образующая с сигнатурой (k, M). Если эта образующая линейно зависима с предыдущими, то имеет место равенство

$$\sum_{j=1}^{k} q_j f_j = 0,$$

где $\mathrm{LM}\, q_k = M$. Но эта образующая не была отброшена критерием F5. Это значит, что $M = \mathrm{LM}\, q_k$ не принадлежит $\mathrm{LM}(f_1, \ldots, f_{k-1})$. В частности, $q_k \notin (f_1, \ldots, f_{k-1})$. Но тогда f_k — делитель нуля по модулю $(f_1, \ldots, f_{k-1})$, что противоречит регулярности. □

Псевдокод матричного алгоритма F5 можно найти в статье [12, стр. 10]. Хороший обзор матричного F5 и других «сигнатурных» алгоритмов построения базисов Грёбнера дан в [].

Задача 9.1. Докажите, что процедура символьного препроцессинга останавливается за конечное число шагов.

Задача 9.2. Предложите алгоритм для проверки регулярности последовательности многочленов $f_1, \ldots, f_n$.

Задача 9.3. Покажите, что если многочлены $f_1, \ldots, f_n$ не являются однородными, то регулярность последовательности $f_1, \ldots, f_n$, вообще говоря, зависит от порядка многочленов в последовательности.

Задача 9.4. Докажите, что последовательность однородных многочленов $f_1, \ldots, f_n$ является регулярной тогда и только тогда, когда модуль сизигий $\mathrm{Syz}(f_1, \ldots, f_n)$ порожден тривиальными сизигиями $f_i f_j - f_j f_i = 0$.

10. Универсальный базис Грёбнера. Веер Грёбнера.

Большую часть этой лекции можно найти в §8.4 книги [8].

У одного и того же идеала есть, вообще говоря, много базисов Грёбнера (даже редуцированных) в зависимости от выбранного мономиального упорядочения. Целью данной лекции будет доказать конечность этого множества и ввести на множестве возможных упорядочений определенную структуру.

Лемма 10.1. *Пусть многочлены $f_1, \dots, f_k$ являются базисом Грёбнера для идеала $(f_1, \dots, f_k)$ относительно упорядочения $<_1$. Пусть также для некоторого упорядочения $<_2$ выполнено $\mathrm{LM}_{<_1} f_i = \mathrm{LM}_{<_2} f_i$ для всех i. Тогда $f_1, \dots, f_k$ — базис Грёбнера относительно $<_2$.*

Доказательство. Предположим противное. Тогда существует многочлен $f \in (f_1, \dots, f_k)$, не редуцируемый к нулю при помощи $f_1, \dots, f_k$ относительно $<_2$. Рассмотрим результат редукции $f = q_1 f_1 + \ldots + q_k f_k + r$, где ни один из мономов r не делится ни на один из старших мономов $f_1, \dots, f_k$. Тогда $r \in (f_1, \dots, f_k)$, но он не редуцируетс к нулю и относительно $<_1$. Противоречие. □

Фиксируем идеал $I \subset k[x_1, \dots, x_n]$. С каждым мономиальным упорядочением $<$ связан мономиальный идеал старших членов $\mathrm{LM}_< I$. Обозначим множество таких идеалов через $\mathrm{Mon}(I)$.

Теорема 10.2. *Для всякого идеала I множество идеалов $\mathbb{M}(I)$ конечно.*

Доказательство. Предположим противное. Пусть $<_1, <_2, \dots$ — мономиальные упорядочения такие, что для любых $i \neq j$ выполнено $\mathrm{LM}_{<_i} I \neq \mathrm{LM}_{<_j} I$. Обозначим множество этих упорядочений через Σ.

Пусть $I = (f_1, \dots, f_k)$. Так как всего есть лишь конечное число способов упорядочить мономы многочленов $f_1, \dots, f_k$, найдется бесконечное подмножество $\Sigma_1 \subset \Sigma$, такое, что все порядки из Σ_1 при ограничении на мономы $f_1, \dots, f_k$ совпадают. Если хотя бы для одного из них $f_1, \dots, f_k$ были базисом Грёбнера, то, согласно предыдущей лемме, они были бы таковыми и для всех остальных элементов множества Σ_1. Это противоречило бы тому, что эти упорядочения задают различные идеалы старших членов.

Пусть $<_1 \in \Sigma_1$. Существует $f_{k+1} \in I$, такой, что $\mathrm{LM}_{<_1} f_{k+1} \notin N_0 = (\mathrm{LM}_{<_1} f_1, \dots, \mathrm{LM}_{<_1} f_k)$. Более того, можно считать, что ни один моном f_{k+1} не лежит в N. Тогда добавим его к набору порождающих и повторим операцию. То есть выберем бесконечное подмножество $\Sigma_2 \subset \Sigma_1$, которое бы одинаково упорядочивало бы мономы f_{k+1}. Пусть $<_2 \in \Sigma_2$. Так как $f_1, \dots, f_{k+1}$ опять не являются базисом Грёбнера, существует $f_{k+2} \in I$, такой, что $\mathrm{LM}_{<_2} f_{k+2} \notin N_1 = (\mathrm{LM}_{<_2} f_1, \dots, \mathrm{LM}_{<_2} f_{k+1})$.

Таким образом будет построена бесконечноая цепочка возрастающих мономиальных идеалов $N_0 \subset N_1 \subset N_2 \subset \dots$, чего не может быть. □

Доказательство теоремы, использующее компактность множества всех упорядочений относительно определенной топологии можно прочесть в [14].

В связи с тем, что один и тот же набор многочленов может рассматриваться относительно разных упорядочений, введем понятие *отмеченного базис Грёбнера*. Набор многочленов $f_1, \dots, f_k$, где в каждом многочлене один из мономов является выделенным, если набор $(f_1, \dots, f_k)$ является базисом Грёбнера идеала $(f_1, \dots, f_k)$ относительно некоторого упорядочения, причем отмеченные мономы являются старшими.

Следствие 10.3. *Множество $\mathrm{Mon}(I)$ находится во взаимнооднозначном соответствии с множеством всех редуцированных отмеченных базисов Грёбнера.*

Доказательство. По отмеченному базису Грёбнера мономиальный идеал старших членов строится однозначно.

Пусть два отмеченных редуцированных базиса $f_1, \ldots, f_k$ и $g_1, \ldots, g_l$ задают один и тот же идеал старших членов. Обозначим его через N. Так как $\operatorname{LM} f_1 \in N$, найдется i, такое, что $\operatorname{LM} g_i | \operatorname{LM} f_1$. В свою очередь, существует j, такое, что $\operatorname{LM} f_j | \operatorname{LM} g_i$. Значит $\operatorname{LM} f_j | \operatorname{LM} f_1$. В силу редуцированности отсюда следует, что $j = 1$ и $\operatorname{LM} g_i = \operatorname{LM} f_1$.

Значит множества $\{\operatorname{LM} g_1, \ldots, \operatorname{LM} g_l\}$ и $\{\operatorname{LM} f_1, \ldots, \operatorname{LM} f_k\}$ совпадают. Тогда можно считать, что $k = l$ и $\operatorname{LM} g_i = \operatorname{LM} f_i$ для всех i. В силу редуцированности ни один моном $f_i - g_i$ не лежит в N. Но тогда $f_i - g_i$ равен нулю, так как должен редуцироваться к нулю с помощью $f_1, \ldots, f_k$. Что и требовалось.

□

Следствие 10.4. *Для всякого идеала $I \subset k[x_1, \ldots, x_n]$ существует такой набор многочленов $f_1, \ldots, f_k$, что этот набор является базисом Грёбнера идеала I относительно любого упорядочения. Такой набор называется универсальным базисом Грёбнера.*

Выпуклым конусом называется такое подмножество $C \subset \mathbb{R}^n$, что для любых $a, b \in C$ и любых $\alpha, \beta \in \mathbb{R}_{\geqslant}$ выполнено $\alpha a + \beta b \in C$. Рассмотрим редуцированный отмеченный базис Грёбнера $F = \{f_1, \ldots, f_k\}$ для идеала $I \subset k[x_1, \ldots, x_n]$. Запишем f_i в виде $x^{\alpha_i} + \sum c_{i,j} x^{\beta_{i,j}}$, где $\alpha_i, \beta_{i,j} \in \mathbb{Z}^n_{\geqslant}$ и моном x^{α_i} является старшим в f_i. Рассмотрим конус:

$$C_F = \left\{ w \in \mathbb{R}^n_{\geqslant} \colon \forall i, j (\alpha_i, w) \geqslant (\beta_{i,j}, w) \right\}$$

Этот конус примечателен тем, что для любого упорядочения $<_M$ заданного матрицей M, относительно которого F является базисом Грёбнера, первая строка M лежит в C_F. Обратное, вообще говоря, неверно.

Теорема 10.5. *Пусть F — редуцированный отмеченный базис идеала I.*

1. *внутренность $\operatorname{Int}(C_F)$ является открытым непустым подмножеством в $\mathbb{R}^n$;*
2. *пусть $<_M$ — упорядочение заданное матрицей M. Если первая строка M лежит в $\operatorname{Int}(C_F)$, то F является базисом Грёбнера относительно $<_M$;*
3. *пусть F' — другой редуцированный отмеченный базис Грёбнера. Тогда пересечение $C_F \cap C_{F'}$ содержится в грани C_F;*
4. *объединение всех C_F, где F пробегает всевозможные отмеченные базисы Грёбнера идеала I, равно $\mathbb{R}^n_{\geqslant}$.*

Доказательство. Пусть F является базисом Грёбнера относиетльно упорядочения $<_M$ заданного матрицей M. Обозначим её строки через $w_1, \ldots, w_m$. Несложно понять, что $w_1 + w_2\varepsilon + w_3\varepsilon^2 + \ldots + w_m\varepsilon^{m-1} \in C_F$ для достаточно малых $\varepsilon > 0$. Так как вектора $w_1, \ldots, w_m$ порождают все пространство, можно выбрать несколько достаточно малых ε, чтобы полученные вектора также порождали все пространство (через них будут выражаться $w_1, \ldots, w_m$ в силу определителя Вандермонда). Тогда положительный ортант в базисе из этих векторов будет лежать в нашем конусе и содержать непустое открытое множество.

Пусть первая строка M лежит в $\operatorname{Int}(C_F)$. Тогда старшими мономами f_i относительно $<_M$ являются действительно x^{α_i}. Рассмотрим также упорядочение $<$, для которого F является базисом Грёбнера. В силу первой леммы этой лекции, F является базисом Грёбнера и относительно $<_M$.

Если бы два выпуклых конуса пересекались на по грани, то их внутренности имели бы непустое пересечение, а значит одному и тому же порядку соответствовало бы два редуцированных отмеченных базисов Гребнера, чего не может быть.

Последний пункт остается как упражнение. □

Набор соответствующих конусов и их граней называется *веером Грёбнера идеала I*.

Интересный пример о том, как веер Грёбнера строить и жить помогает можно найти в статье [15].

Задача 10.1. Построить веер Грёбнера идеала $\langle y - x^2, z - x^3 \rangle$.

Задача 10.2. Построить веер Грёбнера идеала $\langle x - t^4, y - t^2 - t \rangle$.

Задача 10.3. Докажите, что всякий ненулевой вектор с неотрицательными координатами является первой строкой матрицы для некоторого мономиального упорядочения.

Задача 10.4. Всякое ли разбиение $\mathbb{R}^2_{\geqslant}$ лучами с рациональным углом наклона может быть получено как веер Грёбнера некоторого идеала?

Задача 10.5. Привести пример многочлена, в котором есть моном M, такой, что M не является делителем ни одного другого монома в многочлене, но M не является старшим мономом ни при одном упорядочении.

11. Gröbner walk

Материал этой лекции можно найти в §8.5 книги [8].

Gröbner walk («маршрут Грёбнера») — это алгоритм, предложенный в 1997 году для преобразования базиса Грёбнера от одного упорядочения к другому [16]. Зачастую построить базис Грёбнера при одном упорядочении (например, degrevlex), а затем преобразовать его к другому упорядочению (например, lex, для исключения переменных) бывает выгоднее, чем строить такой базис непосредственно. Алгоритм Gröbner walk решает ту же задачу, что и алгоритм FGLM, но, в отличие от FGLM, он работает не только для идеалов нулевой размерности.

Идея алгоритма опирается на то, что веер Грёбнера любого идеала конечен. Пусть $\prec_s$ — исходное упорядочение (заданное матрицей M_s), а $\prec_t$ — конечное упорядочение (заданное матрицей M_t). Пусть $\mathbf{w}_s$ и $\mathbf{w}_t$ — первые строки этих матриц.

Рассмотрим некоторый путь в веере Грёбнера от вектора $\mathbf{w}_s$ к вектору $\mathbf{w}_t$. Например, это может быть отрезок

$$(1-u)\mathbf{w}_s + u\mathbf{w}_t,$$

где $u \in [0,1]$.

Такой отрезок пересекает разные конусы в веере Грёбнера. Основная идея алгоритма — шаг за шагом находить точки пересечения отрезка с границей текущего конуса и пересчитывать при этом базис Грёбнера для упорядочения из следующего конуса. Рассмотрим эти шаги подробнее.

Пусть на текущем шаге у нас есть отмеченный базис Грёбнера G_{old}, соответствующий конусу C_{old}, а упорядочение $\prec_{old}$ задается матрицей M_{old} с первой строкой $\mathbf{w}_{old}$. Пусть $\mathbf{w}_{new}$ — последний вектор в конусе C_{old} на пути к вектору $\mathbf{w}_t$. Покажем, как вычислить $\mathbf{w}_{new}$.

Пусть

$$G_{old} = \left\{ x^{\alpha(i)} + \sum_{i,\beta} c_{i,\beta} x^{\beta} \mid 1 \leqslant i \leqslant t \right\},$$

где $x^{\alpha(i)}$ — старший моном. Пусть $v_1, \ldots, v_m$ — все возможные векторы вида $\alpha(i) - \beta$, где $1 \leqslant i \leqslant t$ и $c_{i,\beta} \neq 0$. C_{old} состоит из тех векторов $\mathbf{w}$ ортанта $(\mathbb{R}^n)^+$, для которых

$$\mathbf{w} \cdot v_j \geqslant 0, \quad 1 \leqslant j \leqslant m.$$

Записывая $\mathbf{w}$ в виде

$$(1-u)\mathbf{w}_{old} + u\mathbf{w}_t$$

для $u \in [0,1]$, получаем условие на u:

$$(1-u)(\mathbf{w}_{old} \cdot v_j) + u(\mathbf{w}_t \cdot v_j) \geqslant 0.$$

Тогда

$$\mathbf{w}_{new} = (1-u_{last})\mathbf{w}_{old} + u_{last}\mathbf{w}_t,$$

где u_{last} — минимальный параметр, такой, что предыдущее неравенство для j обращается в равенство, где $\mathbf{w}_t \cdot v_j < 0$.

Лемма 11.1. *Пусть u_{last} определен как выше. Если $\mathbf{w}_{old}$ задается матрицей вида $\begin{pmatrix} \mathbf{w}_{old} \\ M_t \end{pmatrix}$. Тогда $u_{last} > 0$.*

Вектор $\mathbf{w}_{new}$ лежит на границе конуса Грёбнера. Это значит, что некоторые неравенства, задающие C_{old}, становятся равенствами. Обозначим через $\mathrm{in}_{\mathbf{w}}(f)$ однородную $\mathbf{w}$-часть многочлена f. Рассмотрим идеал

$$\langle \mathrm{in}_{\mathbf{w}_{new}}(G_{old}) \rangle.$$

В идеальном случае этот идеал будет порождаться набором мономов и одним биномом. На практике базис Грёбнера такого идеала вычисляется очень быстро. Оказывается, что зная

базис Грёбнера для такого идеала, можно легко построить базис Грёбнера G_{new} исходного идеала относительно $\prec_{new}$.

Теорема 11.2. *Пусть G_{old} — отмеченный базис Грёбнера идеала I относительно $\prec_{old}$. Пусть $\prec_{new}$ представлено матрицей $\begin{pmatrix} \mathbf{w}_{new} \\ M_t \end{pmatrix}$, где $\mathbf{w}_{new}$ — произвольный вектор из C_{old}. Пусть H — редуцированный базис Грёбнера идеала $\langle \mathrm{in}_{\mathbf{w}_{new}}(G_{old}) \rangle$ относительно $\prec_{new}$. Разложим каждый $h_j \in H$ по базису:*

$$h_j = \sum_{g \in G_{old}} p_{j,g} \, \mathrm{in}_{\mathbf{w}_{new}}(g).$$

Тогда многочлены

$$\overline{h_j} = \sum_{g \in G_{old}} p_{j,g} g$$

образуют базис Грёбнера идеала I относительно $\prec_{new}$.

Задача 11.1. Докажите теорему 11.2.

Задача 11.2. Рассмотрим упорядочения $\prec_s = \prec_{(2,7,1),degrevlex}$ и $\prec_t = \prec_{(3,1,6),degrevlex}$. Преобразуйте базис Грёбнера

$$\{x^4 - x^2 z - xz, y - x^2\}$$

от $\prec_s$ к $\prec_t$.

Задача 11.3. В задаче неявного представления нам даны многочлены $f_i \in F[t_1, \ldots, t_m]$, и требуется исключить t_i из уравнений вида $x_i = f_i(t_1, \ldots, t_m)$. Для этого можно построить исключающий идеал

$$J = \langle x_1 - f_1(t_1, \ldots, t_m), \ldots, x_n - f_n(t_1, \ldots, t_m) \rangle \cap F[x_1, \ldots, x_n]$$

с помощью лексикографического упорядочения. Покажите, как это можно сделать непосредственно с помощью Gröbner walk. (Обратите внимание, что исходные образующие уже образуют некоторый базис Грёбнера.) Найдите этим методом неявное представление кривой $x = t^4, y = t^2 + t$.

Список литературы

[1] А. Г. Хованский, С. П. Чулков. Геометрия полугруппы $\mathbb{Z}^n_{\geqslant 0}$: приложения к комбинаторике, алгебре и дифференциальным уравнениям. М., МЦНМО, 2006.

[2] Cox D., Little J., O'Shea D., *Ideals, Varieties and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra,* New York, NY: Springer, 1998. [Имеется перевод: Кокс Д., Литтл Дж., О'Ши Д., *Идеалы, многообразия и алгоритмы,* М., Мир, 2000.]

[3] Hong H. and Weispfenning V., *Algorithmic Theory of Admissible Term Orders,* preprint, 1999.

[4] Kreuzer M. and Robbiano L., *Computational Commutative Algebra,* Springer, 2008.

[5] Robbiano L., *Term Orderings on the Polynomial Ring,* in Proceedings of EUROCAL 85, Springer Lecture Notes in Computer Science 204, 513-517, 1985.

[6] Robbiano L., *On the Theory of Graded Structures,* The Journal of Symbolic Computation, 2, 139-170, 1986.

[7] Trevisan G., *Classificazione dei semplici ordinamenti di un gruppo libero commutativo con N generatori,* Rend. Sem. Mat. Padova, 22, 143-156, 1953.

[8] Cox D., Little J., O'Shea D., *Using algebraic geometry*, Springer, 1997.

[9] J.-C. Faugère *A New Efficient Algorithm for Computing Gröbner Bases (F_4).* Journal of Pure and Applied Algebra, 139 (1999), 61–88.

[10] B. H. Roune. *The F_4 algorithm.* http://www.broune.com/papers/f4.pdf

[11] J.-C. Faugère. *A new efficient algorithm for computing Gröbner bases without reduction to zero (F5).* http://www-salsa.lip6.fr/~jcf/Papers/F02a.pdf

[12] M. Bardet, J.-C. Faugère, B. Salvy. *On the Complexity of the F_5 Gröbner basis Algorithm.* http://arxiv.org/pdf/1312.1655.pdf

[13] C. Eder, J.-C. Faugère. *A survey on signature-based Gröbner basis computations.* http://arxiv.org/pdf/1404.1774.pdf

[14] Boldini R., *A topological approach to leading monomial ideals,* http://arxiv.org/pdf/1008.0286.pdf.

[15] Laubenbacher R., Stigler B., *A computational algebra approach to the reverse engeneering of gene regulatory networks,* J. of Theoretical Biology, 229, pp. 523-537, 2004.

[16] S. Collart, M. Kalkbrener and D. Mall. *Converting bases with the Gröbner walk,* J. Symbolic Comput. 24 (1997), 465–469.