1 Лекция 8 - Схемы симплификации

1.1 Схемы симплификации

Определение 1. Схемой симплификации называется следующий набор данных $(M, \leqslant, R)$, где:

- $(M, \leqslant)$ – частично упорядоченное множество, удовлетворяющее условию обрывы убывающих цепей, то есть для любой цепочки элементов

$$x_1 \geqslant x_2 \geqslant \ldots \geqslant x_n \geqslant \ldots$$

существует номер m такой, что $x_m = x_{m+1} = \ldots$ – выполняется равенство для всех с некоторого номера.

- R – некоторое семейство неувеличивающих отображений, то есть

$$R = \{\, r \mid r \colon M \to M,\ rx \leqslant x \,\}$$

и содержит тождественное отображение $1 \in R$.

Условие обрыва убывающих цепей эквивалентно тому, что в любом подмножестве X множества M существует минимальный элемент. В частности, из этого следует, что существуют неподвижные элементы.

Определение 2. Неподвижные элементы множества M называются нормальными. То есть элемент нормальный тогда и только тогда, когда для любого $r \in R$ имеем $rx = x$. Множество нормальных элементов будем обозначать как

$$N = \{\, x \in M \mid \forall r \in R :\ rx = x \,\}$$

Смысл схемы симплификации в следующем. Множество M – это интересующее нас множество элементов, порядок на нем - это некоторая меря сложности элемента, то есть чем меньше элемент, тем он проще. Множество R – это множество «операторов» упрощения, применяя которые к фиксированному элементу, мы за конечное число шагов получим какой-то более простой, а в конце концов, и самый простой (неподвижный). При этом надо понимать, что разные способы применения «упрощения» к элементу могут дать разные результаты. Именно понимание процесса применения отображений из R как упрощения и дает название этой структуре – схема симплификации.

Пусть задан элемент $x \in M$, тогда можно применять к нему всевозможные конечные наборы элементов из R, то есть рассмотреть множество

$$N(x) = \{\, r_1 \cdots r_n x \mid r_i \in R,\ n \in \mathbb{Z}_+ \,\}$$

Минимальные элементы этого множества – это все возможные неподвижные элементы из M получающиеся из x.

Определение 3. Минимальные элементы множества $N(x)$ называются нормальной формой элемента x и обозначаются через $\operatorname{nor} x$, или если есть необходимость рассмотреть несколько (они могут быть различны), то через $\operatorname{nor}_i x$.

Если все нормальные формы элемента x совпадают, то говорят, что он обладает канонической формой. Тогда его единственная нормальная форма обозначается через $\operatorname{can} x = \operatorname{nor} x$.

Важно понимать, что нормальные элементы не обязаны быть минимальными во всем M. Например, просто потому, что R может состоять только из тождественного оператора, а тогда все элементы нормальны.

Множество элементов, имеющих нормальную форму, будем обозначать через L. Легко видеть, что неподвижные элементы имеют нормальную форму и с ней совпадают. Поэтому имеется включение множество

$$N \subseteq L \subseteq M$$

в частности L не пусто.

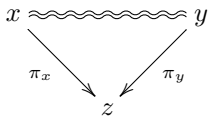
Замечание 4. Важно заметить, что множества N, $N(x)$ и L инвариантны относительно R.

Если все элементы M обладают канонической формой, то есть $M = L$, будем говорить, что она каноническая. Наша задача дать внятный критерий того является ли схема симплификации канонической.

1.2 Граф Ньюмана и критерий каноничности

С каждой схемой симплификации можно связать граф Γ по следующему правилу: его вершины – это в точности множество M, элементы x и y соединены ребром $x \to y$, если и только если $rx = y$, для некоторого $r \in R$. Можно рассматривать как ориентированный граф так и не ориентированный. Условие минимальности обеспечивает отсутствие бесконечных ориентированных путей. Конечные вершины (концы путей) соответствуют нормальным элементам. Поэтому конечные произведения $r_1 \cdots r_n$ элементов из R будем называть путями.

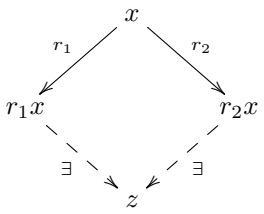
В любом графе можно говорить о связанных компонентах. А именно, можно ввести отношение эквивалентности $x \sim y$, если существует путь от x к y в неориентированном графе. Классы эквивалентности этого отношения и есть компоненты связности. Ориентированный граф позволяет ввести отношение Черча-Россера. А именно, будем писать $x \approx y$, если существуют такие пути $\pi_x = r_1 r_2 \cdots r_n$ и $\pi_y = r'_1 r'_2 \cdots r'_m$, что $\pi_x x = \pi_y y$. Иными словами, для некоторого $z \in M$ имеет место следующая диаграмма



Ясно что оно рефлексивно ($x \approx x$) и симметрично ($x \approx y$ тогда и только тогда, когда $y \approx x$), но вообще говоря не транзитивно.

Теорема 5. *Следующие условия на схему симплификации $(M, \leqslant, R)$ эквивалентны:*

1. *Схема каноническая.*
2. *Всякая связная компонента графа Ньюмана имеет единственную конечную вершину.*
3. *Условие локального слияния (Diamond lemma). Для любого элемента x из M и любых двух элементов r_1 и r_2 из R выполнено $r_1 x \approx r_2 x$. Или, что тоже самое, для таких элементов следующая диаграмма коммутативна*



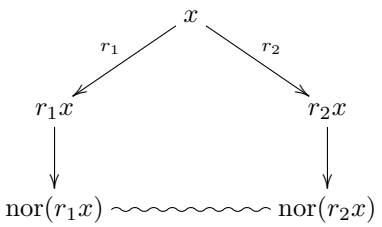
4. *Отношение Черча-Россера – эквивалентность.*
5. *$\approx$ совпадает с $\sim$.*

Доказательство. (1)⇒(2). Пусть X – связная компонента, $x, y \in X$ – две конечные вершины. Рассмотрим соединяющий их путь

$$x \text{ —— } \ldots \text{ —— } a \text{ —— } b \text{ —— } \ldots \text{ —— } y$$

Для произвольных промежуточных элементов имеем $a \to b$ или $b \to a$, но в любом случае из определения канонического элемента и условия каноничности схемы имеем, что $\operatorname{can} a = \operatorname{can} b$. Следовательно это верно для любых элементов пути и в частности $\operatorname{can} x = \operatorname{can} y$. Однако они минимальны, а значит $x = \operatorname{can} x = \operatorname{can} y = y$.

(2)⇒(3). Рассмотрим элементы $x \in M$, $r_1, r_2 \in R$. Приведем каждый из элементов $r_1 x$ и $r_2 x$ к какой-то нормальной форме, тогда имеем следующую картинку:

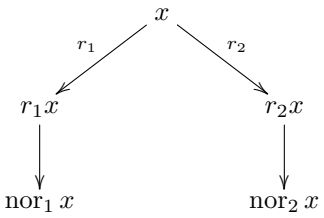


Но, как это указано на рисунке, элементы $\operatorname{nor}(r_1 x)$ и $\operatorname{nor}(r_2 x)$ по построению лежат в одной компоненте связности и являются конечными вершинами. Следовательно они совпадают, что и требовалось.

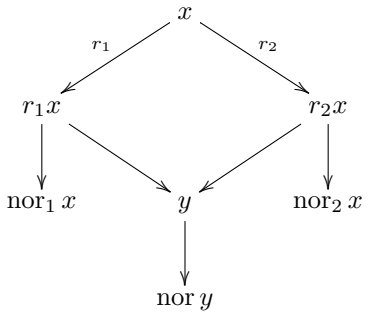
(3)⇒(1). Это единственное содержательное место теоремы. Нам даже понадобится метод от противного. Предположим, что элементы не обладающие канонической формой. Обозначим множество таких

элементов через X. В нем существует минимальный элемент x (условие обрыва убывающих цепей для M). Так как x не обладает канонической формой, то у него есть хотя бы две различные нормальные формы $\mathrm{nor}_1 x$ и $\mathrm{nor}_2 x$.

Пусть $\mathrm{nor}_1 x = r_n \cdots r_2 r_1 x$ и $\mathrm{nor}_2 x = r'_n \cdots r'_2 r'_1 x$. Можно считать, что $r_1 x \neq x$, иначе его можно рассмотреть $\mathrm{nor}_1 x = r_n \cdots r_2 x$ и так далее. Поэтому, можем считать, что эта запись самая короткая, причем $x \neq \mathrm{nor}_1 x$, иначе он обладает канонической формой. А значит хотя бы один такой r_1 присутствует. Аналогично с r'_1. Изобразим сказанное на рисунке

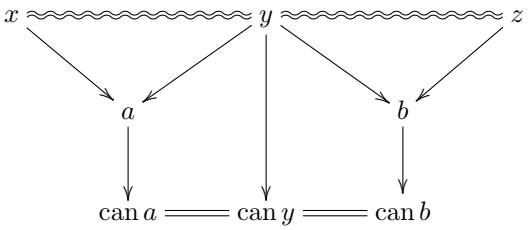


Теперь воспользуемся условием слияния для x, то есть тем, что существует такой y и соответствующие пути как на диаграмме

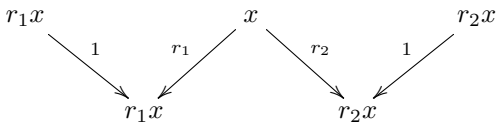


на которой мы дополнительно изобразили какую-то нормальную форму элемента y. Но теперь внимание! Элементы $r_1 x$ и $r_2 x$ строго меньше x, а значит и обладают канонической формой, то есть любые их нормальные формы равны. (Напомним, нормальная форма – это конечная вершина пути, выходящего из данного элемента.) Но по определению $\mathrm{nor}_1 x$ и $\mathrm{nor}\, y$ – нормальные формы $r_1 x$, а $\mathrm{nor}\, y$ и $\mathrm{nor}_2 x$ – нормальные формы $r_2 x$, то есть они все совпадают. Значит $\mathrm{nor}_1 x = \mathrm{nor}_2 x$, противоречие.

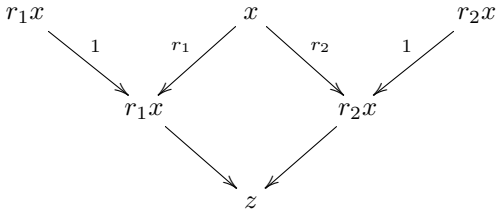
(1-3)⇒(4). Доказательство транзитивности следует из следующей диаграммы



(4)⇒(1-3). Докажем, что выполняется локальное слияние. Пусть даны $x \in M$, $r_1, r_2 \in R$, тогда имеем по определению $r_1 x \approx x$ и $r_2 x \approx x$. И на рисунке это означает:



Но, в силу транзитивности отношения Черча-Россера имеем $r_1 x \approx r_2 x$, то есть



Что и требовалось.

(5)⇒(1-4). Если $\sim$ совпадает с $\approx$, то $\approx$ является отношением эквивалентности.

(1-4)⇒(5). Условие $x \approx y$ по определению влечет $x \sim y$. Надо обратное. Пусть $x \sim y$, тогда есть неориентированный путь

$$x \text{ —— } \ldots \text{ —— } a \text{ —— } b \text{ —— } \ldots \text{ —— } y$$

где для всех соседних элементов a и b по определению выполнено $a \approx b$, и в силу транзитивности $\approx$ имеем, что $x \approx y$. □

Замечание 6. Надо отметить, что доказательства по типу пункта (3) часто применяются для ЧУМ-ов с условием обрыва с той или иной стороны.

Подчеркнем важность условия (5). Дело в том, равенство $x \approx y$ в канонической схеме симплификации легко проверяется алгоритмически, а именно – приведением каждого элемента к его канонической форме. Для условие же $x \sim y$ *a priori* надо бы было проверять наличие произвольно неориентированного пути между ними. Однако пункт (5) утверждает, что достаточно проверить наличие пути только очень специального вида. То есть на самом деле, мы имеем эффективный алгоритм проверки принадлежности элементов одной компоненте связности. Дело в том, что на практике реально нужно выяснить именно это условие. Например для линейных схем симплификации принадлежность одной компоненте связности означает совпадение образов в некотором фактор пространстве. И данный пункт дает эффективный способ решить проверку равенства элементов в факторе.

1.3 Линейные схемы симплификации

Определение 7. Схема симплификации $(M, \leqslant, R)$ называется линейной, если множество M является векторным пространством над некоторым полем K, а все элементы R суть линейные операторы.

Напомним, что множество элементов, обладающих канонической формой, обозначалось через L, множество неподвижных (нормальных) элементов обозначалось через N. Через U обозначим множество элементов, имеющих нулевую каноническую форму. Для линейных схем симплификации верно следующее.

Утверждение 8. *Для любой линейной схемы симплификации подмножества U, N, L являются подпространствами и верно следующее разложение $L = N \oplus U$.*

Доказательство. В начале покажем, что L является подпространством в M. Пусть $x, y \in L$ и $\lambda_1.\lambda_2 \in K$. Рассмотрим $z = \lambda_1 x + \lambda_2 y$. Пусть пусть $r = r_1 \cdots r_n$ приводит z к некоторой нормальной форме. Покажем, что все они совпадают с $\lambda_1 \operatorname{can} x + \lambda_2 \operatorname{can} y$. Действительно, имеем

$$\operatorname{nor} z = \lambda_1 rx + \lambda_2 ry$$

Так как L инвариантно относительно R, то rx и ry обладают канонической формой. Пусть путь r' приводит rx к $\operatorname{can}(rx) = \operatorname{can}(x)$, тогда

$$\operatorname{nor} z = r' \operatorname{nor} z = \lambda_1 \operatorname{can} x + \lambda_2 r' ry$$

Действую аналогично для y, получаем, что

$$\operatorname{nor} z = \lambda_1 \operatorname{can} x + \lambda_2 \operatorname{can} y$$

То есть все его нормальные формы совпадают и равны $\operatorname{can} z$, а значит

$$\operatorname{can} z = \lambda_1 \operatorname{can} x + \lambda_2 \operatorname{can} y$$

То есть отображение $\operatorname{can}\colon L \to L$ – линейный оператор. Ясно что $\operatorname{can}(\operatorname{can} x) = \operatorname{can} x$, то есть оператор can является проектором. Как видно из определения его образ есть в точности N, а ядро U. Тогда искомое разложение получается из общих свойств проекторов. □

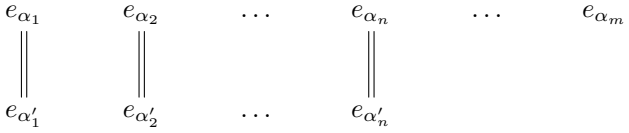
1.4 Линейные схемы симплификации с выделенным базисом

Нас будут интересовать схемы симплификации сугубо определенного вида. А именно, когда частичный порядок на пространстве M задан весьма специфическим образом. С этого момента мы будем обозначать основное множество схемы симплификации через V, а поле над которым оно определено через K.

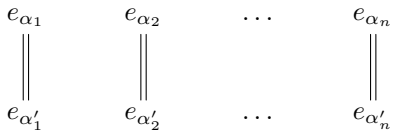
Пусть V – произвольное векторное пространство над K. Мы опишем процедуру введения частичного порядка на V с помощью произвольного линейно упорядоченного базиса. Подробнее, пусть $E = \{ e_\alpha \}$ – некоторый базис V, и предположим, что на нем задан линейный порядок с условием обрыва убывающих цепей, то есть множество E вполне упорядочено. Любой элемент v из V можно разложить по базису $v = \sum \lambda_\alpha e_\alpha$, где только конечное число ненулевых слагаемых. Пусть это слагаемые при базисных векторах $e_{\alpha_1}, \ldots, e_{\alpha_n}$. Тогда набор $(e_{\alpha_1}, \ldots, e_{\alpha_n})$ называется носителем элемента v и обозначается $\operatorname{supp} v$. Теперь надо научиться сравнивать носители элементов. Пусть v, u – два произвольных элемента V, а $(e_{\alpha_1}, \ldots, e_{\alpha_n})$ и $(e_{\alpha'_1}, \ldots, e_{\alpha'_m})$ их носители соответственно. Тогда сравнение происходит покомпонентно. Если $e_{\alpha_1} > e_{\alpha'_1}$, то $v > u$ (или в обратную сторону), в случае равенства надо перейти к сравнению следующих. В результате описанной процедуры сравнения возможны три случая:

1. Мы встретим сравнение $e_{\alpha_i} > e_{\alpha'_i}$, причем все предыдущие равны.

2. Для всех элементов первого носителя имеется равенство $e_{\alpha_i} = e_{\alpha'_i}$, но в первом носителе больше элементов, тогда $v > u$ (то есть меньше тот чей носитель короче).



3. Носители совпали и если элементы не равны, то они считаются несравнимыми.



Введение последнего условия нужно для того, чтобы у нас получился настоящий порядок, а не предпорядок, то есть, чтобы условия $x \leqslant y$ и $y \leqslant x$ влекли $x = y$. Единственное, что нам надо доказать, так это то что наш порядок удовлетворяет условию обрыва убывающих цепей.

Пример 9. Пусть $K[x]$ – кольцо многочленов от одной переменной. Тогда множество $\{ x^n \mid n \in \mathbb{Z}_+ \}$ является базисом, линейно упорядоченным по степеням. Тогда, например, многочлен $x^2 + x$ старше чем x^2 и чем x, а x^2 не сравним с cx^2, если $c \neq 0, 1$.

Утверждение 10. *Введенный порядок на V удовлетворяет условию обрыва убывающих цепей.*

Доказательство. Будем доказывать от противного. Пусть существуют бесконечно убывающие последовательности элементов в V. Рассмотрим произвольную такую цепочку

$$\operatorname{supp} v_1 > \operatorname{supp} v_2 > \ldots > \operatorname{supp} v_n > \ldots$$

пусть первый элемент носителя $\operatorname{supp} v_i$ равен e_i. Тогда по определению сравнения носителей получаем цепочку

$$e_1 \geqslant e_2 \geqslant \ldots \geqslant e_i \geqslant \ldots$$

Порядок на E удовлетворяет условию обрыва, значит начиная с какого-то момента в любой убывающей цепочки носителей первый элемент стабилизируется. То есть существуют бесконечные убывающие цепочки носителей с постоянным первым вектором. Рассмотрим среди всех таких цепочек ту у которой этот первый вектор наименьший (так как E удовлетворяет условию обрыва, это можно сделать). Пусть это цепочка

$$\operatorname{supp} v_1 > \operatorname{supp} v_2 > \ldots > \operatorname{supp} v_n > \ldots$$

со старшим вектором e. Но тогда вычеркнем этот вектор из каждого носителя, получим строго убывающую цепочку

$$\operatorname{supp} v'_1 > \operatorname{supp} v'_2 > \ldots > \operatorname{supp} v'_n > \ldots$$

у которой начиная с какого-то момента первый вектор стабилизируется. Он будет не больше первого вектора v'_1, который строго меньше первого вектора v_1, равного e. Получили бесконечно убывающую цепочку с постоянным первым вектором, меньшим чем e, противоречие. □

Если v некоторый элемент из V, то старший базисный вектор в его носителе будем обозначать через $\overline{v}$ и называть старшим вектором v.

Определение 11. Пусть $(V, \leqslant, R)$ – схема симплификации такая, что ее порядок задается некоторым базисом E указанным выше способом. Тогда такой базис называется выделенным, если для любого $r \in R$ и любого $e \in E$ выполнено $\overline{re} < e$. (То есть либо старший базисный вектор re строго меньше e, либо равен ему, но есть и другие слагаемые.)

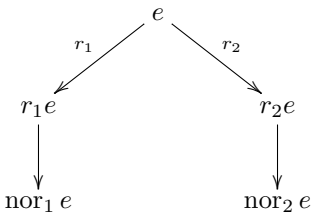
Для схем симплификации с выделенным базисом проверка ее каноничности сводится к проверке некоторого условия на базис, а именно.

Утверждение 12. *Для линейной схемы симплификации $(M, \leqslant, R)$ с выделенным базисом E следующие условия эквивалентны:*

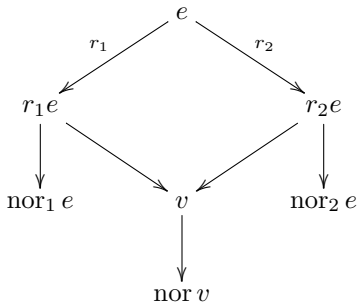
1. *Схема симплификации каноническая*
2. *Условие локально слияния верно для элементов базиса. То есть для любых $e \in E$, $r_1, r_2 \in R$ верно, что $r_1 e \approx r_2 e$.*

Доказательство. (1)⇒(2). Следует из общей теоремы 5.

(2)⇒(1). Так как множество элементов, обладающих канонической формой, образуют подпространство (предложение 8), то достаточно показать, что любой вектор из E обладает канонической формой. Предположим противное, и рассмотрим минимальный плохой вектор из E. Приведем его к двум нормальным формам.



Так же как и при доказательстве теоремы 5, мы считаем, что $r_1 e < e$ и $r_2 e < e$. Воспользовавшись условием слияния, получим вектор $v \in E$, такой что



Но, в силу того что базис E выделенный, все базисные векторы в разложениях $r_1 e$ и $r_2 e$ строго меньше чем e, а значит лежат в L – подпространстве векторов с нормальной формой. А значит и $r_1 e$ и $r_2 e$ там лежат. Как и в теореме 5 получаем из этого цепочку равенств $\mathrm{nor}_1 e = \mathrm{nor}\, v = \mathrm{nor}_2 e$. □

На данный момент мы научились в любом векторном пространстве с помощью его базиса задавать частичный порядок. Теперь надо научиться задавать семейство операторов R разумным образом. Такие семейства будут задаваться подпространствами в V.

Пусть U – подпространство в V. Через $\overline{U}$ обозначим множество старших базисных векторов элементов из U, то есть

$$\overline{U} = \{\, \overline{u} \mid u \in U \,\}$$

Дополнение к U в E обозначим через H. Пусть $u \in U$,тогда он имеет вид $u = \lambda\overline{u} + u'$. Оператор $R_u \colon V \to V$ определим на базисе так: $\overline{u} \mapsto -1/\lambda u'$, и если $e \neq \overline{u}$, то $e \mapsto e$. Таким образом построена схема симплификации (свойство неувеличения порядка очевидно). Теперь покажем, что для данной схем симплификации верно, что $N =< H >$ и $V = L = N \oplus U$.

В начале заметим, что R сохраняет U. Рассмотрим произвольный элемент $v \in V$, и пусть $\mathrm{nor}_1 v$ и $\mathrm{nor}_2 v$ – его две нормальные формы. Но тогда $u = \mathrm{nor}_1 v - \mathrm{nor}_2 v \in U$ и к нему можно применить оператор R_u, переводящий эту разность в 0. А значит нормальные формы совпали. То есть $V = L$. Теперь заметим, что U все редуцируется к нулю, а если какой-то элемент редуцируется к нулю, то, расписав действия операторов R_u мы получаем, что он лежит в U. Значит наши обозначения согласуются с обозначениями предложения 8. Осталось заметить, что H – множество неподвижных векторов и по определению $V =< H > \oplus U$.

1.5 Базисы Гребнера

Основным применением техники схем симплификации является теория базисов Гребнера. Основной ее результат – критерий Бухбергера мы выведем из общей теоремы 5. Нашим основным объектом в этом разделе будет кольцо многочленов от нескольких переменных над произвольным полем. Построим интересующую нас схему симплификации.

Пусть K – произвольное поле, $X = \{ x_1, \ldots, x_n \}$ – конечное множество. Рассмотрим кольцо многочленов $R = K[X] = K[x_1, \ldots, x_n]$ от переменных X. Множество мономов кольца многочленов обозначим через

$$M = \{ x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} \mid k_i \in \mathbb{Z}_+ \}$$

В качестве основного векторного пространство будет выступать кольцо многочленов. Его выделенным базисом будет множество мономов M. Потому нам надо задать линейный порядок с условием минимальности на M, при этом надо потребовать некоторую согласованность с умножением.

Определение 13. Мономиальным упорядочиванием на M называется линейный порядок, удовлетворяющий следующим свойствам:

1. Для любых мономов $m, n, k \in M$ условие $n \leqslant m$ влечет $nk \leqslant mk$.
2. Для любого монома $m \in M$ верно, что $1 \leqslant m$.

Важно, что такие упорядочивания бывают. Например на множестве мономов от одной переменной – это степень. Следующий пример показывает основные примеры мономиальных упорядочиваний для произвольного числа переменных.

Примеры 14. Пусть $m = x_1^{k_1} \cdots x_n^{k_n}$ и $n = x_1^{k'_1} \cdots x_n^{k'_n}$ – произвольные мономы.

1. Лексикографическое упорядочивание (lex):

   Алгоритм сравнения следующий. Вначале сравниваются элемента k_1 и k'_1, если $k_1 > k'_1$, то моном m объявляется больше n (при обратном строгом сравнении меньше), если же $k_1 = k'_1$, то переходят к сравниванию k_2 и k'_2, и так далее. В итоге, либо на каком-то этапе сравнения выяснится, что $k_i > k'_i$, то $m > n$ (или наоборот), либо на всех шагах эти числа совпали, то есть мономы равны.

$$\begin{array}{ccccccc} k_1 & k_2 & \ldots & k_i & \ldots & k_n \\ \| & \| & & \vee & & \\ k'_1 & k'_2 & \ldots & k'_i & \ldots & k'_n \end{array}$$

2. По степени, затем лексикографическое (deglex):

   Вначале мономы сравнивают по степени, а потом как в предыдущем пункте.

$$\begin{array}{ccccccc} \sum_i k_i & k_1 & k_2 & \ldots & k_i & \ldots & k_n \\ \| & \| & \| & & \vee & & \\ \sum_i k'_i & k'_1 & k'_2 & \ldots & k'_i & \ldots & k'_n \end{array}$$

3. Обратное лексикографическое(revlex):

   Мономы сравниваются также как и в первом пункте, но с заменой порядка переменных. То есть, сначала сравниваются k_n и k'_n, затем, если надо, k_{n-1} и k'_{n-1} и так далее.

$$\begin{array}{ccccccc} k_1 & \ldots & k_i & \ldots & k_{n-1} & k_n \\ & & \vee & & \| & \| \\ k'_1 & \ldots & k'_i & \ldots & k'_{n-1} & k'_n \end{array}$$

Пусть на M задано произвольное мономиальное упорядочивание. Тогда данное упорядочивание порождает частичный порядок на многочленов по схеме из предыдущей части, а именно, два многочлена f и g сравниваются по своим старшим мономам $\overline{f}$ и $\overline{g}$, потом по следующим по старшинству и так далее.

Теперь самое время ввести семейство операторов на кольце многочленов. Мы введем сразу несколько таких семейств и будем выбирать из них наилучшее. Пусть $\mathfrak{a}$ – произвольный идеал в R. Пусть E – произвольная система образующих идеала $\mathfrak{a}$. Каждый $f \in E$ имеет вид $\lambda \overline{f} + h$, и пусть $m \in M$ – произвольный моном. Тогда можно задать оператор $R_{f,\,m} \colon R \to R$ действует так $\overline{f} m \mapsto -1/\lambda h m$, а остальные мономы оставляет на месте. То есть редукция какого-то кратного $\overline{f}$ монома. Соответствующее E множество операторов будем обозначать через R_E. В итоге для каждого множества образующих E идеала $\mathfrak{a}$ получается схема симплификации $(K[X], \leqslant, R_E)$. Процесс применения оператора $R_{f,\,m}$ к многочлену будем называть редукцией.

Замечание 15. Важно отметить, что именно для того, чтобы данные операторы были не увеличивающими, нам и нужен такой сложный порядок на многочленах! Смысл этих операторов в том, что с помощью них мы можем редуцировать не только старшие мономы наших многочленов, но и любые другие мономы, как нам будет удобно.

Следующий вопрос состоит в том как восстановить идеал $\mathfrak{a}$ по какой-либо из схем симплификации. В данном случае есть два полезных замечания. Если в качестве E выбрать весь идеал $\mathfrak{a}$, то данная конструкция совпадет с описанной в предыдущей секции и идеал $\mathfrak{a}$ будет в точности множеством элементов с нулевой канонической формой. Но если множество образующих E идеала $\mathfrak{a}$ выбрано неудачно, то схема симплификации может даже не быть канонической, то есть появятся элементы имеющие разные нормальные формы. (На самом деле так бывает очень часто, любое наперед заданное множество образующих почти всегда дает не каноническую схему.)

На самом деле, пользуясь теоремой 5 и раскручивая все определения в обратную сторону, мы можем найти условие на образующие E. Мы так и сделаем, однако, для простоты изложения мы вначале сформулируем ответ, а потом, пользуясь указанной теоремой, докажем, что это действительно то самое условие на E.

Определение 16. Множество образующих E идеала $\mathfrak{a}$ называется его базисом Гребнера, если для любого $f \in \mathfrak{a}$ существует $g \in E$ такой, что $\overline{g}$ делит $\overline{f}$.

Пример 17. Пусть $K[x]$ – кольцо многочленов от одной переменной, и пусть $\mathfrak{a} = (f)$ – идеал, порожденный многочленом f. Тогда, используя порядок из примера 9, мы видим, что f – это базис Гребнера идеала $\mathfrak{a}$. Действительно, так как любой многочлен из $\mathfrak{a}$ делится на f, то и любой старший моном, как следствие, делится на старший моном f.

Мы покажем, что это условие, вместе с кучей других эквивалентно тому, что схема симплификации каноническая. Однако, сейчас надо подготовить некоторую технику.

Определение 18. Пусть f и g два многочлена, имеющие следующий вид

$$f = \lambda ad + h$$
$$g = \mu bd + p$$

где $ad = \overline{f}$ и $bd = \overline{g}$ – мономы, причем d – наибольший общий делитель $\overline{f}$ и $\overline{g}$. Тогда многочлен

$$S_{f,\,g} = \mu bf - \lambda ag$$

называется S-полиномом многочленов f и g. Если $d = 1$, то говорят, что многочлены f и g не зацепляются.

Смысл этого определения в том, что мы, домножив оба многочлена на мономы и вычитая их с подходящими коэффициентами, наиболее эффективным методом убиваем их старшие мономы.

Определение 19. Пусть $f, g_1, \ldots, g_n$ – многочлены такие, что

$$f = h_1 g_1 + \cdots + h_n g_n \qquad (*)$$

то есть f принадлежит идеалу $(g_1, \ldots, g_n)$. Тогда запись $(*)$ называется представлением многочлена f. Моном

$$m = \max_{1 \leqslant i \leqslant n} \overline{h_i g_i}$$

называется параметром представления. Надо отметить, что параметр представления f больше или равен $\overline{f}$. Если параметр представления равен $\overline{f}$, то такое представление называется H-представлением.

Пример 20. Представление $S_{f,\,g} = \mu bf - \lambda ag$ для S-полинома не является H-представлением. Так как параметр представления $w = abd$ сокращается.

Определение 21. Для произвольного идеала $\mathfrak{a}$, его множества образующих E и монома z введем обозначение

$$\mathfrak{a}_z = \{\, f \in \mathfrak{a} \mid \text{существует представление } f \text{ с параметром } w < z \,\}$$

Заметим, что это линейное пространство.

Для произвольного множества X через $\overline{X}$ обозначим множество старших мономов элементов из X. Следующая теорема – это важнейший результат всей этой науки.

Теорема 22. *Пусть $\mathfrak{a}$ идеал кольца многочленов $K[X]$, а E – множество его образующих. Пусть фиксировано какое-то мономиальное упорядочивание на M. Тогда следующие условия эквивалентны:*

1. *множество E – базис Гребнера идеала $\mathfrak{a}$.*
2. *Всякий элемент из $\mathfrak{a}$ каким-то способом редуцируется к нулю.*
3. *Всякий элемент из $\mathfrak{a}$ обладает H-представлением.*

4. *Всякий S-полином элементов E обладает представлением с параметром меньшим его первоначального представления из определения .*

5. *Схема симплификиции $(K[X], \leqslant, R_E)$ – каноническая.*

6. *Идеал $(\overline{\mathfrak{a}})$ порожден множеством $\overline{E}$.*

Доказательство. (1)⇒(2). Пусть $0 \neq h \in \mathfrak{a}$. Тогда редуцируем его каким-нибудь образом до неподвижного элемента h'. Если $0 \neq h' \in \mathfrak{a}$, то по определению базиса Гребнера существует такой элемент $g \in E$, что $\overline{g}$ делит $\overline{h'}$, то есть $\overline{h'} = m\overline{g}$. Тогда элемент h' может быть редуцирован с помощью $R_{g,\,m}$. Значит $h' = 0$.

(2)⇒(3). Пусть $h \in \mathfrak{a}$, выпишем его какой-нибудь процесс редукции

$$h - \lambda_1 p_1 g_1 - \lambda_2 p_2 g_2 - \cdots - \lambda_n p_n g_n = 0$$

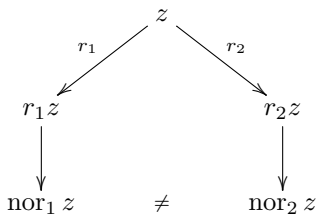
Причем по определению редукции $\overline{p_i g_i} \leqslant \overline{h}$. То есть это и есть H-представление.

(3)⇒(4). Раз всякий элемент из $\mathfrak{a}$ обладает H-представление, то, в частности, и любой S-полином элементов из E таким представление обладает. Пусть $f, g \in E$, тогда

$$S_{f,\,g} = \mu b f - \lambda a g$$

Параметр изначального представления для S-полинома строго выше его порядка, который совпадает с порядком H-представления. То есть H-представление удовлетворяет необходимым требованиям.

(4)⇒(5). Это самый содержательный момент доказательства. Так как множество L – элементов обладающих канонической формой образует подпространство, то достаточно доказать, что каждый моном элемент обладает канонической формой. Предположим противное. Пусть z – минимальный плохой моном, то есть, все мономы меньшие z, а значит и их линейные комбинации, обладают канонической формой. В частности элементы $\mathfrak{a}_z$ обладают канонической формой. И пусть r_1 и r_2 два оператора из R_E такие, что они приводят к двум разным нормальным формам z:



Пусть оператор r_i соответствует паре (g_1, m_i). Так как z редуцируем относительно обоих, то z делится как на $\overline{g_1}$ так и на $\overline{g_2}$. Рассмотрим отдельно два случая:

1) Случай $\overline{g_1}$ и $\overline{g_2}$ взаимно просты и $g_i = \overline{g_i} + h_i$ (считаем для простоты, что их старшие коэффициенты равны 1). Тогда $z = m\overline{g_1 g_2}$ и

$$r_1 z = -m h_1 \overline{g_2}$$
$$r_2 z = -m \overline{g_1} h_2$$

Тогда рассмотрим разность

$$r_1 z - r_2 z = -m h_1 \overline{g_2} + m h_2 \overline{g_1} = -m h_1 \overline{g_2} - m h_1 h_2 + m h_2 \overline{g_1} + m h_2 h_1 =$$
$$= -m h_1 g_2 + m h_2 g_1$$

Таким образом получено представление для разности с параметром меньшим z, то есть $r_1 z - r_2 z \in \mathfrak{a}_z$. Покажем, что каноническая форма разности есть ноль.

Так как элемент $m h_1 g_2$ и $m h_2 g_1$ также лежат в $\mathfrak{a}_z$, то как мы знаем каноническая форма их разности есть разность канонических форм. Но каждый из них редуцируется к нулю (например, первый относительно $R_{g_1,\,m_j}$ для каких-то мономов m_j).

Тогда пусть путь π приводит к канонической форме, то $\pi(r_1 z - r_2 z) = 0$, то есть

$$\mathrm{nor}_1\, z = \pi(r_1 z) = \pi(r_2 z) = \mathrm{nor}_2\, z$$

противоречие.

2) Старшие мономы имеют вид $\overline{g_1} = ad$ и $\overline{g_2} = bd$, где d – наибольший общий делитель. Тогда $z = abcd$ и

$$r_1 z - r_2 z = -bc h_1 + ac h_2 = c(a h_1 - b h_2) = c S_{g_1,\,g_2}$$

Но полином S_{g_1,g_2} обладает параметром представления меньшим его изначального, который равен abd. Значит разность $r_1 z - r_2 z$ обладает представление с параметром меньшим z, то есть лежит в $\mathfrak{a}_z$. Значит как и в предыдущем случае получаем, что ее каноническая форма рана нулю. И как и выше приходим к противоречию.

(5)⇒(2). Покажем, что если $(K[X], \leqslant, R_E)$ – каноническая, то подпространство редуцируемых к нулю элементов U образует идеал. Достаточно показать, что для каждого монома m и многочлена $f \in U$ многочлен mf редуцируется к нулю. Но если Операторы $R_{g_1,\,m_1}, \ldots, R_{g_n,\,m_n}$ осуществляли редукцию f к нулю, то операторы $R_{g_1,\,m_1 m}, \ldots, R_{g_n,\,m_n m}$ осуществляют редукцию mf.

Так как каждый элемент из E редуцируется к нулю, то и весь идеал натянутый на E редуцируется к нулю, а последний совпадает с $\mathfrak{a}$.

(2)⇒(1). Пусть $h \in \mathfrak{a}$, так как он редуцируется к нулю, то в частности, в какой-то момент отредуцируется $\overline{h}$, что и означает определения базиса Гребнера.

(1)⇒(6). Из определения базиса Гребнера следует, что любой старший моном многочлена из $\mathfrak{a}$ делится на какой-то из старших мономов многочлена из E. А значит $\overline{E}$ порождает $(\overline{\mathfrak{a}})$, по определению последнего.

(6)⇒(1). Пусть $(\overline{\mathfrak{a}}) = (\overline{E})$. И пусть $f \in \mathfrak{a}$, тогда $\overline{f} \in (\overline{E})$. Напишем это соотношение

$$\overline{f} = \mu_1 h_1 \overline{g_1} + \cdots + \mu_n h_n \overline{g_n},$$

где h_i – произвольные мономы, $\lambda_i \in K$, а многочлены g_i могут совпадать. В силу однородности $\overline{f}$, можно считать, что в правой части стоят мономы той же степени, что и $\overline{g}$, а раз в левой и правой частях находятся линейные комбинации мономов одинаковой степени, то для любого i имеем $\overline{f} = h_i \overline{g_i}$ и $\sum \mu_i = 1$. В частности существует по крайней мере один g такой, что $\overline{g}$ делит $\overline{f}$.

□

Замечание 23. Заметим, что при доказательстве импликации (4)⇒(5) мы не пользовались условием (4) в случае если S-полином построен по многочленам с взаимно простыми старшими мономами.

1.6 Критерий Бухбергера

Данный раздел посвящен следствиям из теоремы 22. Вначале отметим простое следствие.

Утверждение 24. *Множество образующих E идеала $\mathfrak{a}$ является его базисом Гребнера тогда и только тогда, когда любой S-полином элементов из E со взаимно непростыми мономами каким-либо образом редуцируется к нулю.*

Доказательство. Если E базис Гребнера, то пункт (2) теоремы 22 гласит, что любой элемент из $\mathfrak{a}$ редуцируется к нулю, и в частности S-полиномы такого вида.

Обратно, если S-полиномы редуцируются к нулю, то процесс редукции дает нам представление указанных S-полиномов с параметром строго меньшим его первоначального (сравни цепочку доказательств (2)⇒(3), (3)⇒(4)). А оставшиеся S-полиномы можно не рассматривать в силу замечания 23. □

Таким образом мы имеем эффективный критерий проверки является ли данный набор порождающих идеала его базисом Гребнера. Более того, надо отметить, что редукцию S-полиномов можно вести любым удобным способом, не обязательно начинать со старших коэффициентов.

Обозначим множество мономов не делящихся на мономы $\overline{E}$ через H. Тогда верно следующее.

Утверждение 25. *Пусть E базис Гребнера идеала $\mathfrak{a}$. Пусть U – множество редуцируемых к нулю, а N – неподвижных относительно R_E многочленов. Тогда $\mathfrak{a} = U$, $N =< H >$ и $K[X] =< H > \oplus \mathfrak{a}$.*

Доказательство. Покажем первое равенство. Если многочлен лежит в U, то он редуцируется к нулю, тогда процесс редукции даст его выражение через элементы E (сравни (2)⇒(3) теоремы 22). Обратный пункт следует из пункта (2) той же теоремы 22. Пункт (5) теоремы 22 гласит, что наша схема симплификации каноническая. Тогда из предложения 8 мы знаем, что $K[X] = N \oplus U$, что в свете доказанного равенства означает $K[X] = N \oplus \mathfrak{a}$. Осталось заметить, что многочлен неподвижен тогда и только тогда, когда в нем ни один моном не может быть редуцирован, то есть лежит в H, отсюда $N =< H >$. □

Замечание 26. Заметим, что если E базис Гребнера $\mathfrak{a}$, то схемы симплификации $(K[X], \leqslant, R_E)$ и $(K[X], \leqslant, R_{\mathfrak{a}})$ имеют одно и тоже разложение, в частности, у них совпадает множество неподвижных элементов. Вдобавок с условием $R_E \subseteq R_{\mathfrak{a}}$ имеем, что каждый многочлен имеет одинаковую каноническую форму в обеих схемах. Таким образом каноническая форма элемента не зависит от базиса Гребнера при фиксированном порядке, так как схема $(K[X], \leqslant, R_{\mathfrak{a}})$ не зависит от базиса Гребнера.

То есть если вам надо проверить лежит ли данный многочлен f в идеале $\mathfrak{a}$, то вам достаточно отредуцировать его относительно его какого-то базиса Гребнера, и если получен ноль, то лежит, иначе не лежит. Аналогично можно проверить является ли произведение элементов ноль. На самом деле с помощью

базисов Гребнера можно алгоритмически посчитать абсолютно все, что только возникает в коммутативной алгебре. Например, зная базисы Гребнера идеалов можно построить базис Гребнера их пересечения, произведения, суммы, отношения, радикала, насыщения относительно любого множества и так далее.

Прежде чем говорить о построении базиса Гребнера (конечного!) надо пару слов сказать о его видах.

Определение 27. Пусть E – базис Гребнера идеала $\mathfrak{a}$ тогда можно считать, что

1. Коэффициенты при старших мономах элементов $g \in E$ равны единице.
2. Все $\overline{g}$ не делят друг друга.
3. Пусть $g = \overline{g} - h$, где h – сумма меньших членов. Для любого g многочлено h редуцирован относительно $E \setminus \{ g \}$.

Если указанные условия выполнены, то базис Гребнера называется редуцированным.

Ясно, что описанные условия (2) и (3) эквивалентны тому, что каждый многочлен базиса Гребнера отредуцирован относительно его дополнения.

Определение 28. Рассмотрим множество $\overline{\mathfrak{a}}$ всех старших мономов идеала $\mathfrak{a}$, тогда оно частично упорядоченно по делению. Его минимальные элементы называются абструкциями.

При фиксированном порядке редуцированный базис Гребнера определен однозначно.

Утверждение 29. *Пусть E – редуцированный базис Гребнера идеала $\mathfrak{a}$, тогда множество $\{ \overline{g} \mid g \in E \}$ – это в точности абструкции и $g = \overline{g} - \operatorname{can} \overline{g}$, где каноническая форма берется в схеме симплификации $(K[X], \leqslant, R_{\mathfrak{a}})$.*

Доказательство. Заметим, что абструкции – это в точности те мономы, которые являются старшими мономами каких-то элементов из $\mathfrak{a}$ и не могут быть поделены на другие. Но так как они лежат в $\overline{\mathfrak{a}}$, то по определению базиса Гребнера они должны делиться на какие-то элементы из $\overline{E}$, то есть совпадать с ними. По определению редукции $R_{g,1}(\overline{g}) = h$, где $g = \overline{g} - h$. Но по определению редуцированного базиса Гребнера h – неподвижный элемент, то есть из замечания 26 следует, что это $\operatorname{can} \overline{g}$ для схемы $(K[X], \leqslant, R_{\mathfrak{a}})$. □

Следующая задача – это научиться строить базис Гребнера и желательно конечный! Вначале вопрос, существуют ли базисы Гребнера в принципе? Ответ, Да. Базис Гребнера идеала $\mathfrak{a}$ при любом порядке $\leqslant$ это весь идеал $\mathfrak{a}$. Потому интересным становится вопрос поиска наиболее экономного такого базиса. Точнее, мы знаем, что любой идеал в кольце многочленов $K[x_1, \ldots, x_n]$ имеет вид $(f_1, \ldots, f_m)$. Мы планируем преобразовать это исходное множество образующих в его базис Гребнера. Вначале покажем, что из любого базиса Гребнера всегда можно выбрать конечное подмножество, также являющееся базисом Гребнера. Существует два способа это доказывать: основанный на теореме Гильберта о базисе и основанный на лемме Диксона.

Утверждение 30 (Лемма Диксона)**.** *Пусть Σ – множество мономов в $K[x_1, \ldots, x_n]$ такое, что для любых его элементов $m, m' \in \Sigma$ верно $m \nmid m'$ и $m' \nmid m$. Тогда множество Σ – конечно.*

Доказательство. Утверждение докажем индукцией по количеству переменных. Для одной переменной утверждение очевидно, так как не может быть больше одного монома с указанными свойствами.

Рассмотрим случай n переменным. Предположим противное и пусть $\{ m_k \}$ – бесконечная цепочка мономов, не делящих друг друга. Мономы имеют вид $m_k = x_1^{d_k} n_k$, где n_k – мономы от переменных $x_2, \ldots, x_n$. Переходя к подпоследовательности в m_k, можно считать, что d_k не убывают. Следовательно n_i с меньшим номером не делит n_j с большим номером (т. е. при $i < j$). Теперь можно выбрать подпоследовательность в которой разные n_i не делят друг друга. А именно, в качестве первого элемента выберем $m_1 = x_1^{d_1} n_1$. Количество делителей n_1 конечно, потому, существует номер s такой, что n_s не делит n_1, в качестве второго элемента надо выбрать $m_s = x_1^{d_s} n_s$. Количество делителей n_1 и n_s конечно, а значит можно выбрать третий элемент и т. д. Таким образом мы построили бесконечную цепочку мономов от меньшего числа переменных и не делящих друг друга, противоречие. □

Утверждение 31. *Пусть $\mathfrak{a}$ – произвольный идеал в кольце $K[x_1, \ldots, x_n]$, пусть задан произвольный порядок на мономах и E – некоторый базис Гребнера для идеала $\mathfrak{a}$. Тогда существует такое конечное подмножество $G \subseteq E$, что G также является базисом Гребнера идеала $\mathfrak{a}$.*

Доказательство основанное на теореме Гильберта о базисе. Рассмотрим идеал $(\overline{\mathfrak{a}})$. Мы знаем, что он конечно порожден. Пусть $f_1, \ldots, f_k$ – его образующие. Тогда для каждого i они имеют вид $f_i = h_1 m_1 + \cdots + h_k m_k$, где m_j из $\mathfrak{a}$. Значит идеал $(\overline{\mathfrak{a}})$ порожден конечным числом мономов $n_1, \ldots, n_d$. По определению базиса Гребнера каждый из них делится на старший моном какого-то элемента из E. Рассмотрим для каждого монома n_i ровно по одному такому многочлену и покажем, что это и есть базис Гребнера. Из построения ясно, что старшие мономы выбранных многочленов порождают идеал $(\overline{\mathfrak{a}})$, а значит по теореме 22 пункт 6 получаем требуемое. □

Доказательство основанное на лемме Диксона. Рассмотрим множество мономов $\overline{\mathfrak{a}}$. Тогда все абструкции из него должны редуцироваться, а значит делятся на старшие мономы каких-то элементов из E. В силу определения абструкций это означает, что они являются старшими мономами каких-то элементов из E. Выберем для каждой абструкции ровно по одному многочлену из E и назовем это множество E'. Покажем, что полученное множество и есть искомый конечный базис Гребнера.

Так как любой старший моном делится на какую-то абструкцию, то E' – базис Гребнера по определению. Так как все абструкции не делят друг друга, то по лемме Диксона их конечное число. □

Теперь опишем алгоритм получения конечного базиса Гребнера из произвольной конечной системы образующих идеала $\mathfrak{a}$ в кольце многочленов $K[x_1, \dots, x_n]$ при любом фиксированном упорядочивании $\leqslant$. Мы пишем алгоритм для человека, а не для машины. Поэтому много внимания уделяется именно первому шагу, и идее как продолжить потом. В строгом смысле слова алгоритм, ниже изложенные тексты таковыми не являются.

Алгоритм 32 (Идейная версия, алгоритм Бухбергера)**.** Пусть $f_1, \dots, f_m$ – образующие идеала.

1. Построим все возможные S-полиномы $S_{i,\,j}$ многочленов f_i и f_j, для которых старшие мономы имеют нетривиальный общий делитель.
2. Отредуцируем все построенные S-полиномы относительно $\{ f_1, \dots, f_m \}$. ($S_{i,\,j} \overset{\{ f_1, \dots, f_m \}}{\rightsquigarrow} g_{i,\,j}$.)
3. Если результаты всех редукций $g_{i,\,j}$ оказались нулевыми, то $\{ f_1, \dots, f_m \}$ и есть базис Гребнера. Если нет, то надо добавить ненулевые $g_{i,\,j}$ к $\{ f_1, \dots, f_m \}$ и повторить пункты (1) и (2) для $\{ f_1, \dots, f_m, \dots, g_{i,\,j}, \dots \}$.

В целом прозрачный алгоритм не особенно приятен когда надо делать вычисления в ручную. Можно слегка модифицировать его для того, чтобы было не сильно тоскливо считать очередной миллионный результат редукции.

Алгоритм 33 (Подправленная версия)**.** Пусть $E = \{ f_1, \dots, f_m \}$ – образующие идеала. Также заведем некоторые промежуточные множества E' и E''.

1. Вначале отредуцируем каждый f_i относительно $E \setminus \{ f_i \}$.
2. (S-полиномы теперь будем строить по-очереди). Множество E' полагаем пустым. В него помещаем результаты редукций. Будем перебирать все пары f_i и f_j, у которых старшие мономы имеют нетривиальный общий делитель. Для каждой такой пары
   (a) Посчитаем $S_{i,\,j}$.
   (b) Отредуцируем его относительно $E \cup E'$.
   (c) Если результат редукции ноль переходим к следующей паре f_i и f_j, если не ноль, то добавляем в E'.
3. Отредуцировать каждый элемент множества $E \cup E'$ относительно его дополнения.
4. Если E' пусто, то E и есть базис Гребнера, если нет, то устанавливаем E'' пустым. Теперь надо перебирать все пары f_i и f_j из множества $E \cup E'$, у которых старшие мономы имеют нетривиальный общий делитель и так, чтобы f_i и f_j одновременно не лежали в E.
   (a) Посчитаем $S_{i,\,j}$.
   (b) Отредуцируем его относительно $E \cup E' \cup E''$.
   (c) Если результат редукции ноль переходим к следующей паре f_i и f_j, если не ноль, то добавляем в E''.
5. Полагаем $E = E \cup E'$, а $E' = E''$.
6. Повторить с пункта (3).

Мы не утверждаем, что это самый эффективный вариант алгоритма. Существует вагон и маленькая тележка работ многотысячной армии фанатов посчитать по оптимизации оригинального алгоритма Бухбергера. При подсчете руками автор пользуется подправленной версией алгоритма и килограммами макулатуры.

1.7 Пример вычисления

Проведем два демонстрационных вычисления. Первое очень простое, для того чтобы познакомиться с вычислительной техникой, второе посложнее, чтобы понять какие могут встретиться трудности при подсчетах и впредь их не бояться.

Пример 34. Пусть $K[x,y,t]$ – кольцо многочленов и идеал $\mathfrak{a} = (t^3-y, t^2-x)$. Выберем различные порядки и посчитаем базис Гребнера.

Упорядочим переменные так $t < x < y$ и выберем лексикографическое упорядочивание. Отметим старшие мономы в многочленах, соответствующие данному упорядочиванию, подчеркивание $\underline{x}-t^2, \underline{y}-t^3$. Как мы видим данные многочлены не зацепляются, а значит при указанном упорядочивании это уже базис Гребнера.

Выберем другой порядок переменных, а именно, $x < y < t$ и также лексикографическое упорядочивание мономов. Тогда множество E выглядит так

$$\begin{array}{cc} E & E \\ \underline{t^3}-y & \underline{xt}-y \\ \underline{t^2}-x & \underline{t^2}-x \end{array}$$

где во второй колонке мы редуцировали первый многочлен относительно второго. Теперь вычислим единственный S-полином

$$\begin{array}{cc} E & E' \\ \underline{xt}-y & \underline{yt}-x^2 \\ \underline{t^2}-x & \end{array}$$

Вычисления $t(xt-y) - x(t^2-x) = -yt + x^2$. Теперь надо посчитать S полиномы для пар, не лежащих целиком в E, а именно

$$\begin{array}{ccc} & E\cup E' & E'' \\ E & \underline{xt}-y & y^2-x^3 \\ & \underline{t^2}-x & 0 \\ E' & \underline{yt}-x^2 & \end{array}$$

Вычисления

$$y(xt-y) - x(yt-x^2) = -y^2 + x^3 \rightsquigarrow \underline{y^2} - x^3$$
$$y(t^2-x) - t(yt-x^2) = -xy + x^2 \overset{xt-y}{\rightsquigarrow} 0$$

Теперь повторим процедуру, обновив E и E'.

$$\begin{array}{ccc} & E\cup E' & E'' \\ E & \underline{xt}-y & \\ & \underline{t^2}-x & \\ & \underline{yt}-x^2 & 0 \\ E' & \underline{y^2}-x^3 & \end{array}$$

Вычисления

$$y(yt-x^2) - t(y^2-x^3) = x^3t - yx^2 \overset{xt-y}{\rightsquigarrow} 0$$

Базис Гребнера идеала (t^2-x, t^3-y) при указанном упорядочивании это

$$\{\, t^2-x, yt-x^2, xt-y, y^2-x^3 \,\}$$

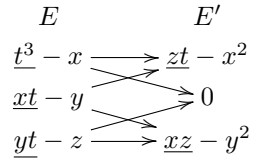
В предыдущем примере организация вычислений очень проста. Приведем еще один пример, отвечающей задаче из книги Хартсхорна, а после поясним геометрический смысл столь «странного» порядка.

Пример 35. Пусть $K[x,y,z,t]$ – кольцо многочленов и идеал $\mathfrak{a} = (t^3-x, t^4-y, t^5-z)$. Упорядочим переменные так $x < y < z < t$ и выберем лексикографическое упорядочивание.

Построим множество E и отредуцируем многочлены (третий относительно второго и второй относительно первого)

$$\begin{array}{cc} \underline{t^3}-x & \underline{t^3}-x \\ \underline{t^4}-y & \underline{xt}-y \\ \underline{t^5}-z & \underline{yt}-z \end{array}$$

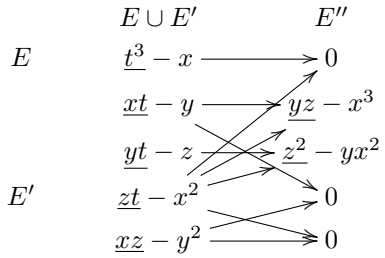
Теперь рассчитаем все S-полиномы



Расчет полиномов ведется в указанном ниже порядке

$$y(xt-y)-x(yt-z)=xz-y^2$$
$$x(t^3-x)-t^2(xt-y)=yt^2-x^2 \overset{yt-z}{\rightsquigarrow} yt^2-x^2-t(yt-z)=zt-x^2$$
$$y(t^3-x)-t^2(yt-z)=zt^2-xy \overset{zt-x^2}{\rightsquigarrow} zt^2-xy-t(zt-x^2)=x^2t-xy \overset{xt-y}{\rightsquigarrow} 0$$

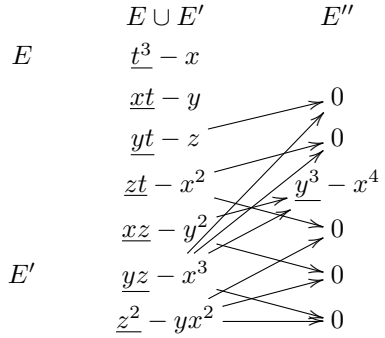
Рассчитываем S-полиномы для зацепляющихся элементов, не лежащих одновременно в E



Расчет полиномов ведется в указанном ниже порядке

$$z(xt-y)-x(zt-x^2)=-yz+x^3 \rightsquigarrow yz-x^3$$
$$z(yt-z)-y(zt-x^2)=-z^2+yx^2 \rightsquigarrow z^2-yx^2$$
$$z(t^3-x)-t^2(zt-x^2)=x^2t^2-xz \overset{xt-y}{\rightsquigarrow} x^2t^2-xz-xt(xt-y)=xyt-xz \overset{yt-z}{\rightsquigarrow} 0$$
$$z(xt-y)t(xz-y^2)=y^2t-yz \overset{yt-z}{\rightsquigarrow} 0$$
$$x(zt-x^2)-t(xz-y^2)=y^2t-x^3 \overset{yt-z}{\rightsquigarrow} y^2t-x^3-y(yt-z)=yz-x^3 \overset{yz-x^3}{\rightsquigarrow} 0$$

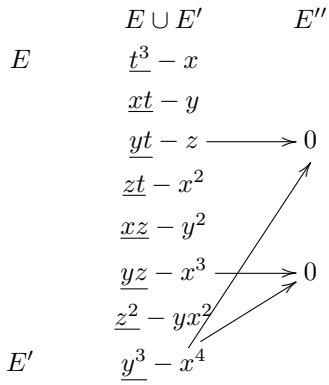
Строим новые E и E' и видим, что редуцировать относительно друг друга уже ничего нельзя, потому считаем S-полиномы зацепляющихся элементов, не лежащих одновременно в E



Расчет полиномов ведется в указанном ниже порядке

$$z(yt-z)-t(yz-x^3)=x^3-t-z^2 \overset{xt-y}{\rightsquigarrow} x^3t-z^2-x^2(xt-y)=-z^2+x^2y \overset{z^2-x^2y}{\rightsquigarrow} 0$$
$$y(zt-x^2)-t(yz-x^3)=x^3t-x^2y \overset{xt-y}{\rightsquigarrow} 0$$
$$y(xz-y^2)-x(yz-x^3)=-y^3+x^4 \rightsquigarrow y^3-x^4$$
$$z(zt-x^2)-t(z^2-x^2y)=x^2yt-x^2z \overset{yt-z}{\rightsquigarrow} 0$$
$$z(xz-y^2)-x(z^2-x^2y)=-y^2z+yx^3 \overset{yz-x^3}{\rightsquigarrow} 0$$
$$z(yz-x^3)-y(z^2-x^2y)=-x^3z+x^2y^2 \overset{xz-y^2}{\rightsquigarrow} 0$$

Строим новые E и E' и видим, что редуцировать относительно друг друга уже ничего нельзя, потому считаем S-полиномы зацепляющихся элементов, не лежащих одновременно в E



Расчет полиномов ведется в указанном ниже порядке

$$y^2(yt-z) - t(y^3-x^4) = x^4t - y^2z \overset{xt-y}{\rightsquigarrow} x^4t - y^2z - x^3(xt-y) = -y^2z + x^3y \overset{z-x^3}{\rightsquigarrow} 0$$
$$y^2(yz-x^3) - z(y^3-x^4) = x^4z - x^3y^2 \overset{xz-y^2}{\rightsquigarrow} 0$$

Базис Гребнера идеала (t^3-x, t^4-y, t^5-z) при указанном упорядочивании это

$$\{\, t^3-x, zt-x^2, yt-z, xt-y, z^2-x^2y, yz-x^3, xz-y^2, y^3-x^4 \,\}$$

Теперь поясним геометрический смысл этих вычислений. Начнем с общей задачи. Пусть X – алгебраическое многообразие в K^n, заданное уравнениями

$$f_1(x_1,\ldots,x_n) = 0, \ldots, f_s(x_1,\ldots,x_n) = 0$$

и Y – алгебраическое многообразие в K^m, заданное уравнениями

$$g_1(y_1,\ldots,y_m) = 0, \ldots, g_r(y_1,\ldots,y_m) = 0,$$

и пусть задано отображение $\varphi\colon X \to Y$ правилами

$$y_1 = h_1(x_1,\ldots,x_n), \ldots, y_m = h_m(x_1,\ldots,x_n).$$

Тогда декартово произведение многообразий X и Y в аффинном пространстве K^{n+m} задается уравнениями

$$f_i(x_1,\ldots,x_n) = 0, g_j(y_1,\ldots,y_m) = 0.$$

Следовательно график отображения φ задается уравнениями

$$f_i(x_1,\ldots,x_n) = 0, g_j(y_1,\ldots,y_m) = 0, y_k - h_k(x_1,\ldots,x_n) = 0.$$

Нам хочется узнать как устроен образ отображения φ. На самом деле мы можем узнать как устроено замыкание образа, а именно, в кольце многочленов $K[x_1,\ldots,x_n,y_1,\ldots,y_m]$, рассмотрим идеал порожденный всеми указанными многочленами $\mathfrak{a} = (f_i, g_j, y_k - h_k)$. Можно показать, что пересечение $K[y_1,\ldots,y_m] \cap \mathfrak{a}$ как раз и задает замыкание образа φ. Таким образом возникает задача нахождения заданного пересечения. Для этого надо выбрать упорядочивание на переменных так, чтобы моном, содержащий хотя бы одну переменную x_i всегда был старше любого монома, зависящего только от y_j. Например, можно выбрать лексикографическое упорядочивание, при котором переменные сравниваются так $y_1 < \ldots < y_m < x_1 < \ldots < x_n$. Посчитаем базис Гребнера идеала $\mathfrak{a}$ при таком упорядочивании и выберем в базисе Гребнера те многочлены, которые зависят только от y_j, тогда это и будет базис Гребнера пересечения при ограничении порядка на мономы только от y_j. Действительно, любой многочлен f из пересечения $K[y_1,\ldots,y_m] \cap \mathfrak{a}$ лежит в $\mathfrak{a}$, а значит, редуцируется относительно всего базиса Гребнера. Рассмотрим эту редукцию. Так как f зависит только от переменных y_j, то он будет редуцироваться относительно тех элементов базиса, у которых старший моном зависит только от y_j, а в силу устройства нашего порядка, то и весь он будет зависеть только от y_j. Доказано, что любой элемент пересечения редуцируется относительно части базиса Гребнера, зависящей только от y_j, значит это и есть базис Гребнера пересечения.

Теперь поясним на первом примере, что было сделано. Мы рассматриваем в качестве X прямую K с координатой t, а в качестве Y плоскость K^2 с координатами x, y. Отображение $\varphi\colon K \to K^2$ задается формулами $x = t^2, y = t^3$. Из сказанного выше следует, что замыкание образа прямой задается уравнением

$y^2 - x^3$. В данном случае можно показать, что образ совпадает со своим замыканием. Действительно, рассмотрим пару колец

$$K[x,y]/(y^2 - x^3) \subseteq K[x,y,t]/(x - t^2, y - t^3)$$

Тогда элемент t, удовлетворяя уравнению $t^2 - x = 0$, является целым над первым подкольцом, а мы знаем, что в таком случае любой простой, и в частности максимальный, идеал имеет в прообразе отображения сужения простой идеал. Пусть $\mathfrak{m}$ – максимальный идеал первого кольца, и пусть $\mathfrak{q}$ – какой-то сужающийся в него идеал, тогда можно рассмотреть максимальный его содержащий $\mathfrak{n}$, который также сужается в $\mathfrak{m}$ в силу максимальности последнего. Если вспомнить, что максимальные идеалы соответствуют точкам, удовлетворяющим уравнениям под знаком факторизации, то мы и доказали, что у любой точки из замыкания образа есть прообраз.

Второй пример соответствует случаю $\varphi\colon K \to K^3$, по правилу $x = t^3, y = t^4, z = t^5$, и образ задается уравнениями

$$z^2 - x^2y, yz - x^3, xz - y^2, y^3 - x^4.$$