

О стандартных базисах в кольце дифференциальных многочленов

А. И. ЗОБНИН

Московский государственный университет
им. М. В. Ломоносова
e-mail: al_zobnin@shade.msu.ru

УДК 512.628.2+512.714+512.711

Ключевые слова: дифференциальная алгебра, базисы Грёбнера, стандартные базисы, задача вхождения в идеал, допустимые упорядочения.

Аннотация

В работе рассматриваются стандартные базисы в кольце обыкновенных дифференциальных многочленов от одной независимой переменной, называемые также дифференциальными базисами Грёбнера по Оливье. Установлена их связь с процессом редукции, предложенным Леви. Доказано, что идеал $[x^p]$ обладает конечным стандартным базисом всего из одного элемента $\{x^p\}$ при так называемом β -упорядочении. Изучаются различные свойства допустимых упорядочений на дифференциальных мономах, ставится вопрос о существовании конечного стандартного базиса у произвольных конечно порождённых дифференциальных идеалов.

Abstract

A. I. Zobnin, On standard bases in rings of differential polynomials, Fundamentalnaya i prikladnaya matematika, vol. 9 (2003), no. 3, pp. 89–102.

We consider Ollivier's standard bases (also known as differential Gröbner bases) in an ordinary ring of differential polynomials in one indeterminate. We establish a link between these bases and Levi's reduction process. We prove that the ideal $[x^p]$ has a finite standard basis (w.r.t. the so-called β -orderings) that contains only one element. Various properties of admissible orderings on differential monomials are studied. We bring up the following problem: whether there is a finitely generated differential ideal that does not admit a finite standard basis w.r.t. any ordering.

1. Введение

Базисы Грёбнера полиномиальных идеалов играют важную роль в компьютерной алгебре. Существует множество обобщений базисов Грёбнера на другие алгебраические структуры, например на кольца некоммутативных многочленов или свободные модули над кольцами многочленов. В данной работе мы рассмотрим обобщение базисов Грёбнера на кольца дифференциальных многочленов. Первые попытки сделать это были предприняты Карра Ферро [3] в 1987 г. (дифференциальные базисы Грёбнера) и Оливье [12, 13] в 1990 г. (стандартные

Фундаментальная и прикладная математика, 2003, том 9, № 3, с. 89–102.

© 2003 Центр новых информационных технологий МГУ,
Издательский дом «Открытые системы»

базисы). В целом эти два подхода эквивалентны. Мы будем придерживаться терминологии Ф. Оливье.

Как и в алгебраическом случае, конечные стандартные базисы позволяют проверить принадлежность многочлена заданному дифференциальному идеалу; однако они могут быть бесконечными. Этот факт долгое время препятствовал их изучению и использованию.

Отметим сразу, что нас будут интересовать только конечно порождённые дифференциальные идеалы (точнее, порождённые одним мономом), поскольку для бесконечно порождённых идеалов проблема принадлежности в общем случае алгоритмически неразрешима (результат Галло, Мишра и Оливье, 1991 г. [5]). С другой стороны, для конечно порождённых дифференциальных идеалов сегодня это открытая проблема.

Задача принадлежности полностью решена для *радикальных* дифференциальных идеалов с помощью характеристического разложения. Эффективный алгоритм, основанный на идеях Ритта для простых идеалов, был предложен Булье, Лазаром, Оливье и Птито в 1995 г. [2]. Сейчас эти методы активно развиваются (см., например, [6]). Однако они неприменимы к нерадикальным идеалам. Так как решения систем дифференциальных уравнений в алгебраически замкнутых полях описываются радикальными идеалами, может показаться, что изучение нерадикальных идеалов бесполезно. Но с теоретической точки зрения это не так!

Задача принадлежности также решена для идеалов, однородных относительно какой-либо весовой функции [5]. Тем не менее существуют дифференциальные идеалы (например, $[x_1^2 + x]$), которые не являются таковыми.

В начале работы мы рассмотрим свойства допустимых упорядочений, дадим определение стандартного базиса по Оливье. Затем мы обратимся к классической работе Леви [8] 1942 г. и с её помощью укажем упорядочения, при которых базис идеала $[x^p]$ является конечным. Этот факт особенно поразителен потому, что идеал $[x^2]$ самими создателями теории дифференциальных базисов Грёбнера приводился в качестве примера идеала, не обладающего конечным стандартным базисом [3]. И если Оливье [12, 13] при этом уточняет, что он рассматривает лишь лексикографическое упорядочение, то некоторые математики, цитирующие Оливье, забывают указать эту важную деталь. Далее мы рассмотрим задачу о бесконечном сокращении мономов в производных данного многочлена. Она связана с вопросом о существовании конечно порождённых дифференциальных идеалов, все стандартные базисы которых бесконечны при любом, даже самом общем, допустимом упорядочении. Мы выдвигаем гипотезу, что таким является идеал $[xx']$.

2. Основные определения и обозначения

2.1. Кольца дифференциальных многочленов

Напомним некоторые определения дифференциальной алгебры, которые можно найти в [7, 17]. *Дифференциальным кольцом* $\mathcal{R}$ называется коммута-

тивное кольцо с единицей и с заданными на нём коммутирующими *элементарными дифференцированиями* $\delta_1, \dots, \delta_m$ (они должны быть линейными и удовлетворять правилу Лейбница). *Дифференциальный оператор* на $\mathcal{R}$ может быть однозначно записан в виде

$$\theta = \delta^\alpha = \delta_1^{\alpha_1} \dots \delta_m^{\alpha_m}.$$

Порядком оператора θ называют $\text{ord } \theta := \sum_{i=1}^m \alpha_i$.

Пусть Θ обозначает моноид всех дифференциальных операторов. Идеал $I \subset \mathcal{R}$ называется *дифференциальным*, если $I = \Theta I$. Если F — произвольное подмножество $\mathcal{R}$, то через $[F]$ обозначается наименьший дифференциальный идеал в $\mathcal{R}$, содержащий F .

Пусть $x_1, \dots, x_n$ — *независимые переменные*. Тогда кольцо многочленов

$$\mathcal{R}\{x_1, \dots, x_n\} := \mathcal{R}[\Theta x_1, \dots, \Theta x_n]$$

от бесконечного числа *дифференциальных переменных* называется *кольцом дифференциальных многочленов* над $\mathcal{R}$. Оно является дифференциальным кольцом с тем же множеством дифференцирований, что и $\mathcal{R}$.

В этой работе мы будем рассматривать только кольца *обыкновенных* дифференциальных многочленов от одной переменной над *полем констант* нулевой характеристики, т. е. кольца вида $\mathcal{F}\{x\}$, где $\Theta = \{\delta^i, i \geq 0\}$, а $\delta \mathcal{F} = 0$. Дифференциальную переменную $\delta^i x$ мы будем обозначать x_i , а также будем часто писать x' вместо $\delta x = x_1$.

Каждый дифференциальный многочлен являются конечной суммой *дифференциальных термов*, т. е. выражений вида $c \cdot M$, где $c \in \mathcal{F}$, $c \neq 0$, и M — *дифференциальный моном*, $M = \prod_{i=0}^k x_i^{\alpha_i}$, $\alpha_i \geq 0$. Коэффициент c при мономе M в f будем обозначать $\text{cf}(f, M)$.

Ниже мы будем опускать прилагательное «дифференциальный», говоря о мономах и многочленах. Мы будем использовать буквы M, P, Q для обозначения мономов и f, g, h — для многочленов.

Рассмотрим моном $M = \prod_{i=0}^k x_i^{\alpha_i}$. *Степень* M определяется как $\deg M := \sum_{i=0}^k \alpha_i$,

а *вес* M как $\text{wt } M := \sum_{i=0}^k i \alpha_i$. Как обычно, многочлен f называется *однородным по степени*, если все входящие в f мономы имеют одинаковую степень, и *однородным по весу*, если все они одного веса.

2.2. Допустимые упорядочения и ранжиры

Напомним определение ранжира и обобщим понятие допустимого упорядочения на дифференциальный случай.

Пусть $X = \{x_1, \dots, x_m\}$ — независимые переменные. *Допустимым ранжиром* $\prec$ называют линейный порядок на ΘX , такой что для всех $x_i, x_j \in X$, $\theta, \theta_1, \theta_2 \in \Theta$ выполнены следующие свойства:

$$\text{R1. } \theta_1 x_i \prec \theta_2 x_j \implies \theta \theta_1 x_i \prec \theta \theta_2 x_j;$$

$$\text{R2. } x_i \preceq \theta x_i.$$

Любой допустимый ранжир вполне упорядочивает множество X .

Пусть теперь $\mathcal{M}$ — множество всех дифференциальных мономов. Линейный порядок $\prec$ на $\mathcal{M}$ называется *допустимым упорядочением*, если выполнены следующие свойства.

$$\text{O1. Свойство сдвига: } x \prec_{\mathcal{M}} y \implies x \cdot z \prec_{\mathcal{M}} y \cdot z \quad \forall x, y, z \in \mathcal{M}.$$

$$\text{O2. Свойство положительности: } 1 \preceq_{\mathcal{M}} x \quad \forall x \in \mathcal{M}.$$

$$\text{O3. Свойство ограничения: ограничение } \prec \text{ на множество дифференциальных переменных } \Theta X \text{ есть допустимый ранжир.}$$

Этих свойств достаточно для доказательства того, что $\prec$ вполне упорядочивает $\mathcal{M}$ (см. [20]).

Старшим мономом $\text{lm}_{\prec} f$ многочлена f называется моном из f , старший относительно $\prec$. *Старший коэффициент* f — это $\text{lc}_{\prec} f = \text{cf}(f, \text{lm}_{\prec} f)$. Мы будем опускать индекс $\prec$ там, где это не приведёт к недоразумению.

В случае обыкновенных многочленов от одной независимой переменной существует только один ранжир: $x_i \prec x_{i+1}$. Таким образом, *лексикографическое* (lex) и *сначала по степени, затем лексикографическое* (deglex) упорядочения на мономах определены однозначно.

2.3. Стандартные базисы дифференциальных идеалов

Напомним определения, которые можно найти, например, в [12, 13]. Для простоты мы приведём их для кольца $\mathcal{F}\{x\}$ с одним дифференцированием.

Пусть зафиксировано некоторое допустимое упорядочение $\prec^1$. Многочлен f *элементарно редуцируется* относительно многочлена g , если существует число $k \geq 0$, такое что $M := \text{lm } \delta^k g$ делит некоторый моном Q в f . Результатом редукции является многочлен

$$\tilde{f} = f - \frac{\text{cf}(f, Q)}{\text{lc } \delta^k g} \frac{Q}{M} \delta^k g.$$

Отношение редукции получается из элементарной редукции рефлексивно-транзитивным замыканием. Это отношение мы будем записывать так: $f \xrightarrow{g} \tilde{f}$. Каждая цепочка элементарных редукций всегда обрывается.

Множество G называется *стандартным базисом* дифференциального идеала I в кольце $\mathcal{F}\{x\}$, если $G \subset I$ и каждый элемент из I редуцируется относительно G к нулю. Эквивалентные формулировки, аналогичные определениям обычных базисов Грёбнера, можно найти в [13].

Пример 1 (Оливье, [12, с. 85]). Идеал $[x^2 + x + 1]$ обладает стандартным базисом из двух элементов: $\{x^2 + x + 1, x'\}$.

¹Как правило, от $\prec$ требуются некоторые дополнительные свойства. Мы рассмотрим их в следующем разделе.

Стандартный базис G идеала I называется *минимальным*, если никакое собственное подмножество G не является стандартным базисом I . Базис G называется *редуцированным*, если каждый элемент $g \in G$ редуцирован относительно $G \setminus \{g\}$.

Оливье [12, 13] предложил процесс пополнения, который, в случае если он останавливается, возвращает минимальный стандартный базис. Этот процесс существенно использует критерии отбора нужных S -полиномов, аналогичные критериям Бухбергера. Однако, как мы увидим, даже если стандартный базис конечен, они не гарантируют остановку процесса.

Если стандартный базис идеала конечен и известен, то он позволяет эффективно решить задачу о принадлежности произвольного многочлена этому идеалу. Так, например, обстоит дело с идеалами, порождёнными наборами линейных многочленов. В общем же случае стандартные базисы бесконечны. Тем не менее в некоторых случаях (например, если идеал порождён многочленами, однородными по весу) проверить принадлежность *данного* многочлена идеалу всё-таки можно, вычислив лишь несколько первых элементов бесконечного базиса (до заданного веса). По этому поводу см. [5, 12].

Стандартные базисы в $\mathcal{F}\{X\}$ можно рассматривать как удобную параметризацию бесконечных базисов Грёбнера в алгебраическом кольце $\mathcal{F}[\Theta X]$. Эта параметризация обеспечивается дифференциальными операторами и является совместимой со структурой дифференциального кольца $\mathcal{F}\{X\}$. Таким образом, мы можем работать с одним элементом f вместо целого семейства Θf .

3. Дополнительные свойства допустимых упорядочений

Для всякого монома P положим $\delta_{\prec} P := \text{lm}_{\prec} \delta P$. Такая запись позволяет определить действие оператора δ на мономах.

Определение 1. Будем говорить, что $\prec$ является *δ -устойчивым* (строго *δ -устойчивым*), если из $P \preccurlyeq Q$ следует $\delta_{\prec} P \preccurlyeq \delta_{\prec} Q$ (соответственно $P \prec Q \implies \delta_{\prec} P \prec \delta_{\prec} Q$).

Примерами строго δ -устойчивых упорядочений являются lex и deglex .

В диссертации Оливье [12] от упорядочения требовались свойства сдвига и положительности, строгая δ -устойчивость и неравенство $P \prec \delta P$ (доминирование дифференцирований). Рассмотрим подробнее это свойство. Нетрудно убедиться, что это неравенство получается автоматически, если потребовать его выполнения на дифференциальных переменных, т. е. потребовать допустимость упорядочения.

Замечание. Если не требовать строгую δ -устойчивость, то свойство доминирования дифференцирований может не выполняться для многочленов! Действительно, пусть $\prec$ — это упорядочение degrevlex . Напомним, что если

$$\sum_{i=0}^k \alpha_i = \sum_{i=0}^k \beta_i, \text{ то}$$

$$\prod_{i=0}^k x_i^{\alpha_i} \prec_{\text{degrevlex}} \prod_{i=0}^k x_i^{\beta_i} \iff$$

$\iff$ первая ненулевая координата вектора $\alpha - \beta$ положительна.

В отличие от алгебраического случая, здесь мы сравниваем векторы α и β слева, для того чтобы упорядочение получилось допустимым.

Имеем $\text{lm}_{\prec}(2x_0x_2 - x_1^2) = x_1^2$, но

$$\text{lm}_{\prec} \delta(2x_0x_2 - x_1^2) = \text{lm}_{\prec}(2x_0x_3) = x_0x_3 \prec x_1^2.$$

Чтобы не происходило такого противоречия, упорядочение $\prec$ можно переопределить, сначала сравнивая веса мономов. В частности, так переопределённое упорядочение degrevlex мы будем обозначать wt-degrevlex .

Определение 2 ([20]). Пусть P_v и Q_v обозначают наборы переменных из мономов P и Q (причём переменные входят в наборы с учётом их кратностей). Моном P *мажорирует* моном Q , если либо $Q = 1$, либо существует инъективное отображение $\phi: Q_v \rightarrow P_v$, такое что $\forall v \in Q_v \ v \prec \phi(v)$.

Например, если $x \prec y$ и z — дифференциальные переменные, то xyz мажорирует x^2 . Заметим, что в случае обыкновенного кольца $\mathcal{F}\{x\}$ от одной переменной нет необходимости уточнять, какое упорядочение рассматривается, так как для переменных всегда выполнено $x_i \prec x_{i+1}$. При этом мажорирование означает просто сдвиг нижних индексов в мономе на некоторый неотрицательный вектор.

Предложение 1. Пусть P и Q — мономы, причём $\deg P = \deg Q$ и $\text{wt } P \geq \text{wt } Q$. Моном P встречается среди мономов многочлена $\delta^{\text{wt } P - \text{wt } Q} Q$ тогда и только тогда, когда P мажорирует Q .

Доказательство. Очевидно, так как все слагаемые в производной имеют положительные коэффициенты и не могут сократиться. $\square$

Замечание. Доказательство достаточности существенно использует единственность дифференциального оператора и независимой переменной в кольце $\mathcal{F}\{x\}$, в то время как необходимость верна и без этих предположений.

Предложение 2. Пусть $M = \prod_{i=1}^d x_{a_i}$, причём $a_1 \leq a_2 \leq \dots \leq a_d$. Если упорядочение $\prec$ является строго δ -устойчивым, то

$$\text{lm}_{\prec} \delta M = \left(\prod_{i=1}^{d-1} x_{a_i} \right) x_{a_d+1}.$$

Другими словами, $\text{lm}_{\prec} \delta M = \text{lm}_{\text{lex}} \delta M$.

Доказательство. Рассмотрим все мономы, входящие в δM . Все они имеют вид $\frac{M}{x_i}x_{i+1}$. Сравним два таких монома между собой. Неравенство $\frac{M}{x_a}x_{a+1} \prec \frac{M}{x_b}x_{b+1}$ равносильно неравенству $x_b x_{a+1} \prec x_a x_{b+1}$, так как $\prec$ — допустимое упорядочение. Требуется установить, что в этом случае $a < b$. Переобозначая индексы, сформулируем эквивалентное утверждение:

$$i \leq j \implies P := x_i x_j \prec Q := x_{i-1} x_{j+1}.$$

Продифференцируем левую и правую части $j - i + 1$ раз. Тогда все мономы, входящие в $\delta^{j-i+1}P$, будут мажорировать моном Q и по предложению 1 встретятся среди мономов $\delta^{j-i+1}Q$. В частности, это относится и к старшему моному $\ln_{\prec} \delta^{j-i+1}P$. Ввиду строгой δ -устойчивости P не может быть больше Q . $\square$

Итак, строго δ -устойчивые упорядочения в некотором смысле похожи на лексикографические (ср. [19]).

Следствие 1. Пусть $\prec$ — строго δ -устойчивое упорядочение, f — многочлен, $\deg \ln f > 1$ и x_i — младшая переменная в $\ln f$. Тогда x_i присутствует во всех $\ln \delta^k f$.

4. Дифференциальные идеалы вида $[x^p]$

4.1. Критерии принадлежности монома идеалу $[x^p]$

Сначала приведём достаточный критерий принадлежности монома идеалу вида $[x^p]$.

Теорема 1 (Леви, [8], [17, с. 16]). Пусть $d = a(p-1) + b$, где $p > 1$, $a \geq 0$, $0 < b \leq p-1$ — целые числа. Положим

$$f(p, d) = a(a-1)(p-1) + 2ab.$$

Тогда любой моном веса w и степени d , такой что $w < f(p, d)$, принадлежит идеалу $[x^p]$.

Следствие 2. $x_i^{(i+1)p-i} \in [x^p]$.

Доказательство. Для монома $x_i^{(i+1)p-i}$ в обозначениях предыдущей теоремы имеем

$$\begin{aligned} d &= (i+1)(p-1) + 1, & w &= id, & a &= i+1, & b &= 1, \\ f(p, d) &= i(i+1)(p-1) + 2(i+1) = id + i + 2 > id = w. \end{aligned} \quad \square$$

Эта теорема была впервые доказана Леви в работе [8] 1942 г. Там же было показано, что если $w \geq f(p, d)$, то существует моном веса w и степени d , не принадлежащий $[x^p]$. В 50–70-е годы была опубликована масса работ, посвящённых улучшению критерия. В частности, Колчин предложил свой метод вывода критерия и обобщил результаты на случай нескольких переменных и

дифференцирований [7, 17]. Однако поиск необходимого условия принадлежности монома идеалу $[x^p]$ в виде явной формулы от степеней монома не увенчался успехом. Так, одна из проблем Ритта, сформулированная в [17], требует определить минимальную степень q_i , такую что $x_i^{q_i} \in [x^p]$. Она была точно решена в [11] лишь при $i \leq 2$: $q_1 = 2p - 1$, $q_2 = 3p - 2$. Имеется правдоподобная гипотеза, что $q_i = (i + 1)p - i$ (ср. со следствием из теоремы).

Лучше обстоят дела с идеалом $[uv]$ в кольце $\mathcal{F}\{u, v\}$: имеется необходимое и достаточное условие принадлежности монома этому идеалу, выраженное в терминах весов и степеней [9].

Доказательство достаточных критериев Леви получается из *процесса редукции Леви*, который нам понадобится в дальнейшем.

Определение 3 (Леви, [8]). Моном $M = \prod_{i=0}^k x_i^{\alpha_i}$ называется α -термом (по отношению к целому числу p), если для всех i от 1 до k выполнено $\alpha_{i-1} + \alpha_i < p$. Все остальные мономы называются β -термами.

Нетрудно убедиться, что для всякого $k \geq 0$ многочлен $\delta^k x^p$ содержит в качестве слагаемого только один β -терм по отношению к p . Если $k = ap + b$, где $0 \leq b < p$, то этот β -терм имеет вид $x_a^{p-b} x_{a+1}^b$. Разумеется, при $b = 0$ получаются мономы x_a^p .

Определение 4. Всякое допустимое упорядочение, при котором старший моном $\text{lm } \delta^m x_k^p$ является β -термом для всех $m \geq 0$ и $k \geq 0$ будем называть β -упорядочением.

Заметим, что упорядочения degrevlex и wt-degrevlex являются β -упорядочениями.

Теорема 2 (Леви, [8], [17, с. 17]).

I. Для любого монома P верно равенство

$$P \equiv \sum c_i M_i \pmod{[x^p]},$$

где M_i — α -термы по отношению к p , а c_i — рациональные коэффициенты.

II. Никакая нетривиальная линейная комбинация α -термов не принадлежит $[x^p]$.

Доказательство первого пункта в изложении Леви выглядело так. Рассмотрим произвольный моном P . Если он является β -термом по отношению к p , то он делится на $x_i^a x_{i+1}^{p-a}$, $0 < a \leq p$. Вычислим $(p(i + 1) - a)$ -ю производную от x^p ; она тоже будет содержать этот моном. Вычтем эту производную с нужным множителем из P и повторим процесс. Рано или поздно мы превратим P в линейную комбинацию α -термов и процесс остановится.

4.2. Конечный стандартный базис идеала $[x^p]$

Заметим, что процесс Леви — это не что иное, как дифференциальная редукция монома P относительно многочлена x^p при любом β -упорядочении.

Принимая во внимание второй пункт теоремы, заключаем, что $P \in [x^p]$ тогда и только тогда, когда $P \rightarrow_{x^p} 0$. Таким образом, $\{x^p\}$ — это стандартный базис по Оливье идеала $[x^p]$. Примечательно, что он не только конечен, но и состоит из одного элемента. Тем не менее следует заметить, что β -упорядочения не являются строго δ -устойчивыми:

$$\text{lm } x_0 x_2 \prec_\beta \text{lm } x_1^2, \text{ но } \text{lm } \delta(x_0 x_2) = x_1 x_2 = \text{lm } \delta x_1^2.$$

В связи с этим докажем следующий факт.

Предложение 3. *Идеал $[x^p]$, $p > 1$, не обладает конечным стандартным базисом ни при каком строго δ -устойчивом упорядочении.*

Доказательство похоже на частный случай доказательства Оливье для лексикографического упорядочения [12].

Доказательство. По следствию 2 в идеале $[x^p]$ лежит семейство мономов $x_r^{(p-1)r+p}$. Каждый из этих мономов должен редуцироваться относительно некоторого элемента стандартного базиса. Если бы число элементов базиса было конечным, то нашёлся бы бесконечный набор мономов $\{x_{r_i}^{d_i}\}$, $d_i = (p-1)r_i + p$, которые редуцировались бы относительно одного и того же элемента f . Не теряя общности, можем считать, что $\text{lm } f = x_{r_1}^d$. Но тогда по следствию 1 старшие мономы всех производных f содержат x_{r_1} , а значит, не могут делить $x_{r_2}^{d_2}$, так как $r_2 \neq r_1$. $\square$

Итак, мы вынуждены расширить множество допустимых упорядочений, заменив строгую δ -устойчивость на нестрогую. Тогда, как мы видели, идеал $[x^2]$ приобретает конечный стандартный базис. Конечно, этот факт не особенно актуален с вычислительной точки зрения, так как принадлежность идеалу, порождённо-му однородными по весу многочленами¹, всегда проверяется алгоритмически без предположений на упорядочение [12]. Однако он может пролить свет на решение в какой-либо форме проблемы принадлежности произвольному конечно порождённому дифференциальному идеалу. Оказывается, стандартный базис по Оливье не столь безнадёжный теоретический инструмент в нелинейном случае, как может показаться на первый взгляд. Тем не менее остаётся множество проблем.

Во-первых, процесс Оливье (предложенный в [13]), запущенный на идеале $[x^p]$ с любым β -упорядочением, никогда не остановится, хотя и будет на каждой итерации выдавать $\{x^p\}$. (На самом деле, он не всегда останавливается и при строгой δ -устойчивости.) Необходимо получить эффективный критерий остановки этого алгоритма. (Как выяснилось из общения с Франсуа Оливье, конечность базиса для $[x^2]$ можно доказать, используя критерии отбора S -полиномов.)

Во-вторых, вполне могут существовать конечно порождённые идеалы, не обладающие стандартным базисом ни при каком допустимом упорядочении.

¹Идеалы, порождённые одним мономом, являются однородными по отношению к любой весовой функции.

5. Допустимые упорядочения, не являющиеся строго δ -устойчивыми

5.1. Сокращения мономов в производных и стандартные базисы для $[xx']$

Лемма 1. Пусть моном M записан в виде $M = x_{a_1} \dots x_{a_d}$. Тогда

$$\delta^n M = \sum_{\substack{s_i \geq 0 \\ \sum_{i=1}^d s_i = n}} \frac{n!}{\prod_{i=1}^d s_i!} \prod_{i=1}^d x_{a_i + s_i}.$$

Доказательство. Формула немедленно следует из обобщения правила Лейбница

$$\delta^n(xy) = \sum_{i=0}^n \binom{n}{i} \delta^i x \delta^{n-i} y$$

на случай нескольких множителей. $\square$

Определение 5. Пусть f — однородный по степени и весу многочлен, причём $\deg f = d$ и $\text{wt } f = w$. Последовательность мономов (M_k) , такую что $\deg M_k = d$ и M_{k+1} мажорирует M_k , будем называть *исчезающей* в многочлене f , если для всех достаточно больших k моном M_k не входит в качестве слагаемого в $\delta^{\text{wt } M_k - w} f$ (производную такого же веса, как и M_k).

Нас будет интересовать вопрос о существовании исчезающих последовательностей. Ясно, что если все коэффициенты f одного знака, то ни в каких производных f не могут произойти сокращения мономов, а значит, рано или поздно в $\delta^n f$ будут представлены все мономы степени d и веса $n + w$ от переменных начиная с x_{n_0} . Другими словами, для таких многочленов не существует исчезающих последовательностей.

Однако если коэффициенты f имеют разные знаки, исчезающие последовательности могут существовать. Ниже мы явно построим многочлен, для которого последовательность β -термов $(x_r^d)_{r=2}^\infty$ будет исчезающей. Это означает, что если не требовать *строгую* δ -устойчивость, то, вообще говоря, δ^i и Im не будут коммутировать.

Отыщем коэффициент при x_r^d в многочлене $\delta^n M$, где $M = \prod_{i=1}^d x_{a_i}$ и $n = rd - w$. В этом случае формула в лемме 1 содержит одно слагаемое, отвечающее x_r^d . При этом $s_i = r - a_i$ и

$$\text{cf}(\delta^n M, x_r^d) = \frac{(rd - w)!}{\prod_{i=1}^d (r - a_i)!}.$$

Рассмотрим теперь многочлен $f = \sum_{k=1}^m c_k M_k$ с неопределёнными коэффициентами $c_k \in \mathcal{F}$, где $M_k = \prod_{i=1}^d x_{a_{ki}}$, причём $\sum_{i=1}^d a_{ki} = w = \text{wt } M_k$ для всех k . Будем считать, что $a_{k1} \leq a_{k2} \leq \dots \leq a_{kd}$ и что наборы $(a_{k1}, \dots, a_{kd})$ различны при разных k (т. е. различны сами мономы M_k). Постараемся подобрать коэффициенты c_k так, чтобы последовательность $(x_r^d)_{r=r_0}^{+\infty}$ исчезала в f . Для этого приравняем к 0 коэффициент при x_r^d в $\delta^{rd-w} f$:

$$\sum_{k=1}^m c_k \frac{(rd-w)!}{\prod_{i=1}^d (r-a_{ki})!} = 0.$$

Обозначая $a = \min a_{ki}$, получаем

$$\frac{(rd-w)!}{((r-a)!)^d} \sum_{k=1}^m c_k \prod_{i=1}^d ((r-a_{ki}+1)(r-a_{ki}+2)\dots(r-a)) = 0.$$

Обозначим произведение в k -м слагаемом через $g_k(r)$. Мы видим, что уравнение

$$\sum_{k=1}^m c_k g_k(r) := \sum_{k=1}^m c_k \prod_{i=1}^d ((r-a_{ki}+1)\dots(r-a)) = 0$$

должно иметь бесконечно много целых положительных корней относительно r . Но в левой части стоит многочлен степени не выше w , который в силу нашего требования должен оказаться тождественным нулем. Это означает, что функции $g_k(r)$ должны быть линейно зависимыми над $\mathcal{F}$.

Заметим, что попутно мы установили следующий факт: если система $\{x_r^d\}$ исчезает в f для какого-то бесконечного набора индексов r , то она исчезает и при всех r .

Укажем теперь явно многочлен f , для которого функции $g_k(r)$ линейно зависимы. Пусть

$$f = 2x_0x_2^2 - x_0x_1x_3 - x_1^2x_2.$$

Тогда $d = 3$, $m = 3$, $a = 0$ и

$$\begin{aligned} 2g_1(r) - g_2(r) - g_3(r) &= 2(r-1)^2r^2 - (r-2)(r-1)r^2 - (r-1)r^3 = \\ &= (r-1)r^2(2(r-1) - (r-2) - r) \equiv 0. \end{aligned}$$

Мономы $x_{r-1}x_r^2$ также исчезают в f , поскольку только из них при дифференцировании могут получиться мономы x_r^3 .

Заметим, что исчезновение заданной в общем виде последовательности в фиксированном многочлене можно проверить алгоритмически.

5.2. Недостатки общих допустимых упорядочений

Доказанное утверждение имеет серьёзные следствия, которые отличают дифференциальные базисы Грёбнера (стандартные базисы по Оливье) от обычных.

Если G — стандартный базис дифференциального идеала I , то результат авторедукции G может уже не быть стандартным базисом! Действительно, в процессе редукции некоторого элемента базиса относительно остальных элементов может получиться многочлен с иным набором старших мономов у производных. Поэтому, хотя редуцированный базис всё же можно определить так же, как и раньше, не каждый базис можно превратить в редуцированный.

Напомним ещё раз, что эти выводы были сделаны при замене свойства строгой δ -устойчивости на нестрогую. Таким образом, нестрогая δ -устойчивость не даёт каких-либо положительных утверждений, поэтому мы ничего не потеряем, если откажемся от неё. Итак, будем рассматривать самые общие упорядочения, удовлетворяющие лишь основным свойствам О1—О3. Цепочки редукций при этом всё равно будут обрываться, так как уже эти три аксиомы гарантируют, что множество мономов является вполне упорядоченным (см. [20]).

5.3. Обладает ли идеал $[xx']$ конечным стандартным базисом?

Возникает естественный вопрос: всякий ли конечно порождённый дифференциальный идеал обладает конечным стандартным базисом при каком-либо общем упорядочении? Скорее всего, ответ на него отрицательный. Судя по всему, даже идеал $[\delta(x^2)] = [xx']$ не обладает таким базисом ни при каком упорядочении. Можно доказать следующие утверждения.

Лемма 2. Семейства мономов

- (1) $x_0^2 x_r$, $r \geq 1$,
- (2) $x_r^{t_r}$, $r \geq 1$ (для некоторых $t_r \geq r + 2$),
- (3) $x_r^2 x_{r+2}^2 \dots x_{r+2k_r}^2$, $r \geq 0$ (для некоторых $k_r \geq r$),
- (4) $x_r^2 x_{r+3}^2 \dots x_{r+3l_r}^2$, $r \geq 0$ (для некоторых $l_r \geq 1$)

принадлежат идеалу $[xx']$.

Следствие 3. Если идеал $[xx']$ обладает конечным стандартным базисом G при некотором упорядочении $\prec$, то в G должны быть элементы g_1 , g_2 , g_3 и g_4 , такие что старшие мономы их производных делят мономы семейств 1—4 из предыдущей леммы соответственно.

Итак, в каждом из многочленов g_i должны исчезать делители других семейств. Скорее всего, это невозможно, хотя, как мы видели, исчезновения семейств мономов в многочлене вполне могут происходить.

Доказательство леммы.

(1). Для $r = 1$ доказывать нечего. Предположим, что $x_0^2 x_k \in [xx']$. Дифференцируя этот моном, мы получаем $2x_0 x_1 x_k + x_0^2 x_{k+1}$. Итак, $x_0^2 x_{k+1} \in [xx']$.

(2). Так как $x_1 \delta(x x_1) - x_2(x x_1) = x_1^3$, доказательство следует из следствия 2.

(3). Рассмотрим моном $M := \prod_{i=0}^{s-1} x_{r+2i}^2$. Так как $\text{wt } M = \sum_{i=0}^{s-1} 2(r + 2i) = 2s(r + s - 1)$ и $\deg M = 2s$, то по теореме 1 заключаем, что $M \in [x^2]$ при

$r < s$. Редуцируя M относительно xx_1 при любом β -упорядочении, получаем выражение вида $x^2 f$, $f \in \mathcal{F}\{x\}$. Заметим, что f не содержит мономов вида x_0^k , $k \geq 0$. Используя первое утверждение леммы, убеждаемся в том, что $M \in [xx']$.

(4). Доказательство аналогично случаю (3). Действительно, для монома $M := \prod_{i=0}^{s-1} x_{r+3i}^2$ имеем $\text{wt } M = 2r + 3s - 3$ и $\deg M = 2s$. Согласно теореме 1 $M \in [x^2]$ (а значит, $M \in [xx']$) при $2r - 1 < s$.

Заметим, что этот метод доказательства уже неприменим к мономам $\prod_{i=0}^{s-1} x_{r+ki}^2$, $k \geq 4$. □

6. Благодарности

Я хотел бы поблагодарить моего научного руководителя Е. В. Панкратьева и всех участников семинара по компьютерной и дифференциальной алгебре механико-математического факультета МГУ за важные комментарии и поддержку при подготовке этой работы. Особенно хочу поблагодарить М. В. Кондратьеву и Франсуа Оливье за ценные обсуждения рассматриваемых проблем.

Работа выполнена при финансовой поддержке РФФИ, грант 02-01-01033.

Литература

- [1] Панкратьев Е. В. Стандартные базисы в дифференциальной алгебре // Вестник Моск. ун-та. Сер. 1, Математика, механика. — 2003. — № 3. — С. 48–56.
- [2] Boulier F., Lazard D., Ollivier F., Petitot M. Representation for the radical of a finitely generated differential ideal // Proceedings of 1995 International Symposium on Symbolic and Algebraic Computation. — ACM Press, 1995. — P. 158–166.
- [3] Carrà Ferro G. Gröbner bases and differential algebra // Lecture Notes in Computer Science, vol. 356. — 1989. — P. 141–150.
- [4] Carrà Ferro G. Differential Gröbner bases in one variable and in the partial case // Math. Comput. Modelling, vol. 25. — Pergamon Press, 1997. — P. 1–10.
- [5] Gallo G., Mishra B., Ollivier F. Some constructions in rings of differential polynomials // Lecture Notes in Computer Science, vol. 539. — 1991. — P. 171–182.
- [6] Hubert E. Factorization-free decomposition algorithms in differential algebra // J. Symb. Comp. — 2000. — Vol. 29. — P. 641–662.
- [7] Kolchin E. R. Differential Algebra and Algebraic Groups. — Academic Press, 1973.
- [8] Levi H. On the structure of differential polynomials and on their theory of ideals // Trans. Amer. Math. Soc. — 1942. — Vol. 51. — P. 532–568.
- [9] Mead D. G. A necessary and sufficient condition for membership in $[uv]$ // Proc. Amer. Math. Soc. — 1966. — Vol. 17. — P. 470–473.
- [10] Mead D. G., Newton M. E. Syzygies in $[y^p z]$ // Proc. Amer. Math. Soc. — 1974. — Vol. 43, no. 2. — P. 301–305.

- [11] O’Keefe K. B. A property of the differential ideal $[y^p]$ // Trans. Amer. Math. Soc. — 1960. — Vol. 94. — P. 483–497.
- [12] Ollivier F. Le problème de l’identifiabilité structurelle globale. — Doctoral Dissertation. — Paris, 1990.
- [13] Ollivier F. Standard bases of differential ideals // Lecture Notes in Computer Science, vol. 508. — 1990. — P. 304–321.
- [14] Ovchinnikov A., Zobnin A. Classification and applications of monomial orderings and the properties of differential orderings // Proceedings of the Fifth International Workshop on Computer Algebra in Scientific Computing (CASC-2002) / V. G. Ganzha, E. W. Mayr, E. V. Vorozhtsov (Eds.). — Technische Universität München, Garching, Germany, 2002. — P. 237–252.
- [15] Pankratiev E. V. Some approaches to construction of standard bases in commutative and differential algebra // Proceedings of the Fifth International Workshop on Computer Algebra in Scientific Computing (CASC-2002) / V. G. Ganzha, E. W. Mayr, E. V. Vorozhtsov (Eds.). — Technische Universität München, Garching, Germany, 2002. — P. 265–268.
- [16] Pankratiev E. V. Some approaches to construction of the differential Gröbner bases // Calculemus 2002. 10th Symposium on the Integration of Symbolic Computation and Mechanized Reasoning. Marseille, France, July 3–5, 2002. Work in Progress Papers. — Univ. Saarlandes, 2002. — P. 50–55.
- [17] Ritt J. F. Differential Algebra. — Vol. XXXIII of Colloquium Publications. — New York: American Mathematical Society, 1950.
- [18] Rust C., Reid G. J. Rankings of partial derivatives // Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation. — New York: ACM Press, 1997. — P. 9–16.
- [19] Weispfenning V. Differential term-orders // Proceedings of the 1993 International Symposium on Symbolic and Algebraic Computation. — Kiev: ACM Press, 1993. — P. 245–253.
- [20] Zobnin A. Essential properties of admissible orderings and rankings. Contributions to General Algebra, vol. 14, 2004. Available at http://shade.msu.ru/~difalg/Articles/Our/Zobnin/ess_properties.ps.