Алгоритм проверки тривиальности «смешанных» идеалов в кольце дифференциальных многочленов

А. И. Зобнин М. А. Лимонов

Аннотация

В статье предлагается алгоритм проверки тривиальности идеала $[f] + (h_1, \ldots, h_t)$ в обыкновенном кольце дифференциальных многочленов при некотором дополнительном условии на многочлен f. Эта задача тесно связана, с одной стороны, с задачей Колчина об экспонентах дифференциальных идеалов, а с другой — с вопросами конечности дифференциальных стандартных базисов.

1 Введение

В одной из своих ранних работ [6] Эллис Колчин изучал возможные значения экспонент дифференциальных идеалов особого вида. Экспонентой идеала I называется минимальное натуральное число m, такое, что $\sqrt{I}^m \subset I$ (если такого числа не существует, то экспонента считается равной бесконечности). Колчин рассматривал идеалы, порождённые дифференциальным многочленом первого порядка. В его работе было разобрано несколько достаточно общих случаев (но не все), и в этих случаях было установлено, что экспонента может равняться 1, 2 или ∞. В частности им рассматривались дифференциальные многочлены, не имеющие сингулярных корней, то есть такие, что

$$[f, S_f] \neq (1), \tag{1}$$

где S_f — сепаранта f (частная производная многочлена f по старшей переменной). Колчин установил, что если, вдобавок, многочлен f удовлетворяет условию

$$[f] + (S_f) = (1), \tag{2}$$

то экспонента идеала $[f]$ равна 1, то есть, идеал $[f]$ является радикальным (этот результат справедлив для многочленов f любого порядка). В то же время случай

$$[f, S_f] = (1), \quad [f] + (S_f) \neq (1) \tag{3}$$

Колчин оставил неразобранным. Он даже не предложил никакого практического способа проверки того, выполняется ли условие (2) при предположении (1).

С другой стороны, в 2007 году Дмитрий Трушин, изучая так называемый идеал сепарант, доказал [3], что при предположении (1) условие (2) равносильно наличию в идеале квазилинейного многочлена (т. е. дифференциального многочлена, разрешённого относительно старшей производной). В свою очередь, это равносильно существованию у идеала $[f]$ конечного дифференциального стандартного базиса (аналога базиса Грёбнера) при порядках, близких в некотором смысле к лексикографическому [9].

Как мы видим, в этих задачах возникает одно и то же условие (2) на многочлен f. Если предположение (1) можно проверить алгоритмически с помощью алгоритма Розенфельда–Грёбнера [4, 8], то готового алгоритма для проверки тривиальности «смешанной» суммы дифференциального и недифференциального идеалов, т. е. проверки условия (2), не было известно. Более того, высказывались мнения[1], что такая задача алгоритмически неразрешима.

[1] Частная беседа одного из авторов с участниками конференции Gröbner Bases in Symbolic Analysis, Линц, Австрия, 2006.

В данной работе мы предъявим алгоритм, проверяющий условие (2) (а на самом деле, решающий более общую задачу): при более слабом предположении

$$\left[f, \frac{\partial f}{\partial y_0}, \ldots, \frac{\partial f}{\partial y_l}\right] = (1), \tag{4}$$

где l — порядок дифференциального многочлена f, проверить, верно ли равенство

$$[f] + (h_1, \ldots, h_t) = (1), \tag{5}$$

где $h_1, \ldots, h_t$ — произвольные заданные многочлены. Идеалы вида $[f] + (h_1, \ldots, h_t)$ мы будем называть «смешанными»: вообще говоря, они не являются дифференциальными. Мы надеемся, что предложенный алгоритм поможет в исследовании так называемой проблемы Ритта [7, 8], которая до сих пор является открытой.

Статья организована следующим образом. В главе 2 мы приводим необходимые определения из дифференциальной алгебры. В главе 3 строится разложение производной дифференциального многочлена по старшим переменным с помощью так называемых обобщенных сепарант. В их терминах в главе 4 формулируется алгоритм, решающий поставленную задачу. В главе 5 приводится несколько примеров, иллюстрирующих работу алгоритма.

2 Основные определения и обозначения

Мы будем работать над полем констант $\mathcal{F}$ нулевой характеристики.

Определение 1. Кольцо $\mathcal{R}$ называется *алгеброй Ритта*, если оно является алгеброй над $\mathbb{Q}$.

Определение 2. Отображение $\delta : \mathcal{R} \to \mathcal{R}$ называется *дифференцированием*, если для любых элементов a и b кольца $\mathcal{R}$ выполнены следующие свойства:

1. $\delta(a + b) = \delta(a) + \delta(b)$ — линейность;
2. $\delta(ab) = a\,\delta(b) + b\,\delta(a)$ — правило Лейбница.

Определение 3. Кольцо $\mathcal{R}$ называется *обыкновенным дифференциальным кольцом*, если на нем задано одно дифференцирование.

Определение 4. Пусть $\mathcal{F}$ — обыкновенное дифференциальное поле. *Кольцом дифференциальных многочленов* от одной неизвестной над $\mathcal{F}$ называется кольцо многочленов от счетного числа переменных $\mathcal{F}[y_0, \ldots, y_n, \ldots]$ (обозначается $\mathcal{F}\{y\}$) с дифференцированием δ, таким, что $\delta(y_i) = y_{i+1}$ и δ, ограниченное на $\mathcal{F}$, совпадает с дифференцированием поля $\mathcal{F}$. Дифференцирование δ, заданное таким способом, однозначно продолжается на $\mathcal{F}\{y\}$ по линейности и правилу Лейбница.

В дальнейшем для удобства мы будем обозначать n-ю производную многочлена f как $\delta^n f$.

Определение 5. Пусть $M = \prod_{i=0}^{n} y_i^{a_i}$, где $a_i \geqslant 0$, причем $a_n > 0$. Тогда n называется *порядком* монома M (обозначение: $\operatorname{ord} M = n$). Соответственно, порядком многочлена называется максимальный порядок мономов, его составляющих.

Будем говорить, что переменная y_i старше переменной y_j (обозначение: $y_i \succ y_j$), если $i > j$.

Определение 6. *Дифференциальным идеалом* дифференциального кольца $\mathcal{R}$ называется идеал I, такой, что $\delta(I) \subset I$.

Будем обозначать через (F) и $[F]$ сответственно алгебраический и дифференциальный идеалы, порождённые элементами из F.

Определение 7. Для элемента f кольца $\mathcal{F}\{y\}$ определим *сепаранту* S_f как частную производную по старшей переменной. Для элементов поля $\mathcal{F}$ полагаем ее нулем.

Определение 8. Многочлен называется *квазилинейным*, если его сепаранта — ненулевой элемент поля $\mathcal{F}$.

3 Обобщенные сепаранты

Далее мы будем использовать букву n для обозначения порядка дифференцирования и l для порядка многочлена.

Известно, что производные дифференциального многочлена «линейны» по своей старшей переменной. Более того, коэффициент перед этой переменной для любого порядка дифференцирования один и тот же — это сепаранта:

$$\delta^n f = S_f y_{l+n} + Q_{f,n}, \tag{6}$$

где $\operatorname{ord} Q_{f,n} < l + n$. Мы обобщим это наблюдение на переменные, «предшествующие» старшей.

Лемма 1. *Пусть моном M записан в виде $M = y_{r_1} \dots y_{r_d}$. Тогда*

$$\delta^n M = \sum_{\substack{s_i \geqslant 0, \\ s_1+\ldots+s_d=n}} \frac{n!}{s_1! \dots s_d!} \prod_{i=1}^{d} y_{r_i+s_i}.$$

Доказательство. Следует непосредственно из правила Лейбница. □

Лемма 2. *Пусть f — дифференциальный многочлен. Тогда для любого $s \in \mathbb{N}$*

$$\frac{\partial\, \delta f}{\partial y_s} = \delta\left(\frac{\partial f}{\partial y_s}\right) + \frac{\partial f}{\partial y_{s-1}},$$

где $\frac{\partial}{\partial y_s}$ — обычная частная производная.

Доказательство. Пусть $l = \operatorname{ord} f$. Воспользуемся формулой $\delta f = \sum\limits_{i=0}^{l} \frac{\partial f}{\partial y_i} y_{i+1}$, которая следует из правила Лейбница. Имеем

$$\frac{\partial\, \delta f}{\partial y_s} = \frac{\partial\left(\sum\limits_{i=0}^{l} \frac{\partial f}{\partial y_i} y_{i+1}\right)}{\partial y_s} = \sum_{i=0}^{l} \frac{\partial \frac{\partial f}{\partial y_i}}{\partial y_s} y_{i+1} + \sum_{i=0}^{l} \frac{\partial y_{i+1}}{\partial y_s} \frac{\partial f}{\partial y_i}.$$

Во второй сумме только слагаемое $\frac{\partial y_s}{\partial y_s} \frac{\partial f}{\partial y_{s-1}} = \frac{\partial f}{\partial y_{s-1}}$ не равно 0, т. е.

$$\frac{\partial\, \delta f}{\partial y_s} = \sum_{i=0}^{l} \frac{\partial \frac{\partial f}{\partial y_i}}{\partial y_s} y_{i+1} + \frac{\partial f}{\partial y_{s-1}} = \sum_{i=0}^{l} \frac{\partial \frac{\partial f}{\partial y_s}}{\partial y_i} y_{i+1} + \frac{\partial f}{\partial y_{s-1}} = \delta\left(\frac{\partial f}{\partial y_s}\right) + \frac{\partial f}{\partial y_{s-1}}.$$

□

Лемма 3. *Пусть f — дифференциальный многочлен. Тогда для любых $n, s \in \mathbb{N}$ верно*

$$\frac{\partial\, \delta^n f}{\partial y_s} = \sum_{i=0}^{n} C_n^i\, \delta^i\left(\frac{\partial f}{\partial y_{i+s-n}}\right).$$

Доказательство. Докажем это утверждение индукцией по n. База ($n = 1$) верна по лемме 2. Предположим, что для $n = k$ утверждение верно. Докажем, что утверждение верно при $n = k+1$. Пусть $\delta f = g$. Тогда $\frac{\partial\, \delta^{k+1} f}{\partial y_s} = \frac{\partial\, \delta^k g}{\partial y_s}$. Применим предположение индукции к многочлену $\delta^k g$. Имеем

$$\frac{\partial\, \delta^{k+1} f}{\partial y_s} = \sum_{i=0}^{k} C_k^i\, \delta^i\left(\frac{\partial g}{\partial y_{i+s-k}}\right) = \sum_{i=0}^{k} C_k^i\, \delta^i\left(\frac{\partial\, \delta f}{\partial y_{i+s-k}}\right).$$

Воспользуемся линейностью дифференцирования и леммой 2 в каждом слагаемом в последней сумме:

$$\delta^i\left(\frac{\partial\, \delta f}{\partial y_{i+s-k}}\right) = \delta^i\left(\frac{\partial f}{\partial y_{i+s-k-1}} + \delta\left(\frac{\partial f}{\partial y_{i+s-k}}\right)\right) = \delta^i\left(\frac{\partial f}{\partial y_{i+s-k-1}}\right) + \delta^{i+1}\left(\frac{\partial f}{\partial y_{i+s-k}}\right).$$

Следовательно,

$$\frac{\partial\,\delta^{k+1}f}{\partial y_s} = \sum_{i=0}^{k} C_k^i\,\delta^i\left(\frac{\partial f}{\partial y_{(i+s-k)-1}}\right) + \sum_{i=0}^{k} C_k^i\,\delta^{i+1}\left(\frac{\partial f}{\partial y_{i+s-k}}\right) =$$

$$= \sum_{i=0}^{k} C_k^i\,\delta^i\left(\frac{\partial f}{\partial y_{(i+s-k)-1}}\right) + \sum_{i=1}^{k+1} C_k^{i-1}\,\delta^i\left(\frac{\partial f}{\partial y_{i+s-k-1}}\right) = \sum_{i=1}^{k+1} C_{k+1}^i\,\delta^i\left(\frac{\partial f}{\partial y_{i+s-(k+1)}}\right).$$

Переход доказан. □

Рассмотрим дифференциальный многочлен g порядка l и произвольное целое число $k \geqslant 0$. Представим многочлен в виде $g = g_0 + A_{g,k}y_k$, где g_0 не зависит от y_k, а многочлен $A_{g,k}y_k$ получается из многочлена g нахождением всех мономов, зависящих от y_k, и вынесением этой переменной за скобки.

Лемма 4. *Пусть f — дифференциальный многочлен и $\operatorname{ord} f = l$. Тогда для любых k и n с условием $n \in \mathbb{N}, 0 \leqslant k \in \mathbb{Z}$, $n > 2k$ верно следующее равенство:*

$$A_{\delta^n f,n+l-k} = \sum_{j=0}^{l} C_n^{k-l+j}\,\delta^{k-l+j}\left(\frac{\partial f}{\partial y_j}\right).$$

Здесь мы по умолчанию понимаем $C_n^k = 0$ для отрицательных k.

Доказательство. Заметим, что в силу линейности дифференцирования мы можем считать f мономом. Пусть $\deg f = d$ и f представляется в виде

$$f = \prod_{i=0}^{l} y_i^{m_i} = \prod_{i=1}^{d} y_{r_i},$$

где $r_i \leqslant r_j$ при $i \leqslant j$. Тогда применив лемму 1 к $\delta^n f$, получим

$$\delta^n f = \sum_{\substack{s_i \geqslant 0,\\ s_1+\ldots+s_d=n}} \frac{n!}{s_1!\ldots s_d!}\prod_{i=1}^{d} y_{r_i+s_i}.$$

Так как $n > 2k$, то в каждом мономе вида $\prod_{i=1}^{d} y_{r_i+s_i}$ переменная y_{n+l-k} встречается лишь один раз. Действительно, пусть $y_{r_i+s_i} = y_{n+l-k}$ и $y_{r_j+s_j} = y_{n+l-k}$. Но тогда

$$r_i + s_i + r_j + s_j = 2(n + l - k).$$

Следовательно,

$$2(n + l - k) \leqslant 2r_d + \sum_{i=1}^{d} s_d = 2l + n.$$

Значит, $n \leqslant 2k$, что противоречит выбору $n > 2k$. Мы получили, что многочлен $\delta^n f$ линеен по всем переменным $y_{n+l-k}, n > 2k$. Пусть $\delta^n f = f_0 + A_{\delta^n f,n+l-k}y_{n+l-k}$. Тогда, в силу линейности $\delta^n f$ по y_{n+l-k},

$$\frac{\partial\,\delta^n f}{\partial y_{n+l-k}} = \frac{\partial(f_0 + A_{\delta^n f,n+l-k}y_{n+l-k})}{\partial y_{n+l-k}} = A_{\delta^n f,n+l-k}.$$

С другой стороны, по лемме 3 $\frac{\partial\,\delta^n f}{\partial y_{n+l-k}} = \sum\limits_{i=0}^{n} C_n^i\,\delta^i\left(\frac{\partial f}{\partial y_{i+l-k}}\right)$. Заметим, что так как $\operatorname{ord} f = l$, то для всех $i > k$ выполнено $\frac{\partial f}{\partial y_{i+l-k}} = 0$. Отсюда следует, что

$$A_{\delta^n f,n+l-k} = \sum_{i=0}^{n} C_n^i\,\delta^i\left(\frac{\partial f}{\partial y_{i+l-k}}\right) = \sum_{i=0}^{k} C_n^i\,\delta^i\left(\frac{\partial f}{\partial y_{i+l-k}}\right) =$$

$$= \sum_{j=l-k}^{l} C_n^{k-l+j}\,\delta^{k-l+j}\left(\frac{\partial f}{\partial y_j}\right) = \sum_{j=0}^{l} C_n^{k-l+j}\,\delta^{k-l+j}\left(\frac{\partial f}{\partial y_j}\right).$$

Последнее равенство верно, так как если $l > k$, то из $0 \leqslant j < l - k \Longrightarrow C_n^{k-l+j} = 0$, а если $l < k$, то $k - l \leqslant j < 0 \Longrightarrow \frac{\partial f}{\partial y_j} = 0$. □

Пусть f — дифференциальный многочлен, $\operatorname{ord} f = l$, $n \in \mathbb{N}$, $0 \leqslant k \in \mathbb{Z}$ и $n > 2k$. Введём более удобное обозначение

$$S_{f,n,k} := A_{\delta^n f, l+n-k} = \sum_{j=\max(l-k,0)}^{l} C_n^{k-l+j}\, \delta^{k-l+j}\left(\frac{\partial f}{\partial y_j}\right)$$

(по лемме 4). Коэффициенты $S_{f,n,k}$ будем называть *обобщёнными сепарантами* многочлена f. В частности, при $k = 0$ обобщённая сепаранта совпадает с обычной: $S_{f,n,0} = S_f = \frac{\partial f}{\partial y_l}$. Заметим, что при указанных предположениях $\operatorname{ord} S_{f,n,k} \leqslant k + l$.

Предложение 5. *При* $n > 2p$

$$\delta^n f = S_{f,n,0}\, y_{l+n} + S_{f,n,1}\, y_{l+n-1} + \ldots + S_{f,n,p}\, y_{l+n-p} + T_{f,n,p}, \tag{7}$$

где $\operatorname{ord} T_{f,n,p} < l + n - p$.

Доказательство. Докажем утверждение индукцией по p. База выполнена: при $p = 0$ утверждение превращается в формулу (6). Предположим, что для некоторого p утверждение доказано, и докажем его для $p + 1$, где $2(p + 1) < n$. Заметим, что

$$\operatorname{ord} S_{f,n,k} \leqslant k + l \leqslant p + l < l + n - p - 1,$$

поэтому переменная $y_{l+n-p-1}$ не встречается в слагаемых вида $S_{f,n,k}\, y_{l+n-k}$ формулы (7). Она может встретиться только в $T_{f,n,p}$, причём в этом случае она окажется старшей переменной $T_{f,n,p}$. Значит,

$$S_{f,n,p+1} = A_{\delta^n f,\, l+n-p-1} = A_{T_{f,n,p},\, l+n-p-1},$$

причем

$$T_{f,n,p} = S_{f,n,p+1}\, y_{l+n-p-1} + T_{f,n,p+1},$$

где $\operatorname{ord} T_{f,n,p+1} < l + n - p - 1$. □

4 Алгоритм, проверяющий равенство (5)

Сформулируем сначала несколько утверждений об идеалах в произвольном коммутативном кольце.

Предложение 6. *Если* S *— идеал, а* I *— радикальный идеал, то* $I = I : S \cap (I + S)$. □

Предложение 7. *Если* I *— идеал, то* $I : (g_1, \ldots, g_n) = \bigcap_{i=1}^{n} I : (g_i)$. □

Предложение 8. *Если* Q_i *— идеалы,* P *— простой идеал и* $\bigcap_{i=1}^{n} Q_i \subset P$*, то для некоторого* j $Q_j \subset P$. □

Пусть даны идеалы в кольце многочленов $\mathcal{F}[y_0, \ldots, y_s]$. Очевидно, что такие свойства идеалов, как тривиальность, простота, радикальность, включение не зависят от присоединения к кольцу дополнительных независимых переменных. Поэтому, говоря об идеалах, мы не будем уточнять, в кольцах многочленов от каких переменных они рассматриваются.

Перейдём теперь к формулировке задачи. Пусть $f \in \mathbb{Q}\{y\}$ — дифференциальный многочлен порядка l, а $h_1, \ldots, h_t$ — произвольные многочлены, образующие алгебраический идеал J. Для каждого натурального d пусть G_d — идеал, порожденный элементами $\delta^{d-l+j}\left(\frac{\partial f}{\partial y_j}\right)$, где

$$\max(l - d, 0) \leqslant j \leqslant l.$$

Отметим, что по определению $S_{f,n,d} \in G_d$. Предположим, что

$$[f] + G_0 + \ldots + G_p = (1),$$

где p — некоторое натуральное число. (Очевидно, что если выполнено (4), то такое p найдётся.) Требуется выяснить, равен ли идеал $I = [f] + J$ единичному. Заметим, что разделение случаев (2) и (3) является частным случаем этой задачи, когда $J = (S_f)$.

Обозначим через S_p идеал $G_0 + \ldots + G_p$. Пусть $I_k = (f, \delta f, \ldots, \delta^k f) + J$. Заметим, что

$$I = (1) \iff \exists\, k : I_k = (1) \iff \exists\, k : \sqrt{I_k} = (1).$$

Выберем теперь k таким, чтобы

— $(f, \delta f, \ldots, \delta^k f) + S_p = (1)$;

— $k \geqslant \operatorname{ord} h_i + p - l$ для всех многочленов h_i;

— $k \geqslant 2p$.

Проверим, выполняется ли равенство $I_k = (1)$.

Разложим идеал $\sqrt{I_k}$:

$$\sqrt{I_k} = \sqrt{I_k} : S_p \cap \left(\sqrt{I_k} + S_p\right).$$

Так как $\sqrt{I_k} + S_p = (1)$, то

$$\sqrt{I_k} = \sqrt{I_k} : S_p = \sqrt{I_k} : (G_0 + \ldots + G_d) = \bigcap_{d=0}^{p} \sqrt{I_k} : G_d.$$

Чтобы доказать, что этот идеал отличен от (1), необходимо и достаточно доказать, что один из идеалов $\sqrt{I_k} : G_d$ отличен от (1). Будем перебирать идеалы $\sqrt{I_k} : G_d$, увеличивая d.

Если $\sqrt{I_k} : G_d = (1)$, то и $\sqrt{I_n} : G_d = (1)$ для всех остальных $n \geqslant k$. Будем считать, что d — наименьший номер, такой, что $\sqrt{I_k} : G_d \neq (1)$. Наша цель — постараться получить аналогичное неравенство для $k+1$.

Идеал $\sqrt{I_k} : G_d$ является радикальным. Разложим его в минимальное пересечение простых идеалов $P_{k,d,i}$. Это в точности минимальные простые компоненты идеала $\sqrt{I_k}$, не содержащие G_d. Предположим, что имеет место **случай 1**: среди этих простых идеалов существует идеал P, не содержащий ни одной обобщенной сепаранты $S_{f,n,d}$ при $n \geqslant k$. Покажем, что тогда идеал $\sqrt{I_{k+1}} : G_d$ также является собственным, и среди его минимальных простых также есть идеал Q, не содержащей обобщенных сепарант. В таком случае по индукции мы получим, что $I \neq 1$.

Действительно, так как $k + 1 > 2p \geqslant 2d$, то к $\delta^{k+1} f$ применимо предложение 5:

$$\delta^{k+1} f = S_{f,k+1,0} y_{l+k+1} + \ldots + S_{f,k+1,d} y_{l+k+1-d} + T.$$

Первые $d-1$ обобщенных сепарант принадлежат, соответственно, идеалам $G_0, \ldots, G_{d-1}$, которые, в свою очередь, содержатся в $\sqrt{I_k}$ и в P. Пусть $z = y_{l+k+1-d}$ и R — подкольцо кольца многочленов, порожденное переменными, младшими z. Можно написать

$$\delta^{k+1} f \equiv S_{f,k+1,d} z + T \pmod{P},$$

причем $\operatorname{ord} T < \operatorname{ord} z$, т. е. $T \in R$. Покажем, что в идеале P можно выбрать систему образующих, порядок которых тоже меньше z. В самом деле, идеалы $J, G_0, \ldots, G_d$ таковы. Далее,

$$\delta^k f = S_{f,k,0} y_{l+k} + \ldots + S_{f,k,d-1} z + T_k,$$
$$\delta^{k-1} f = S_{f,k-1,0} y_{l+k-1} + \ldots + S_{f,k-1,d-2} z + T_{k-1},$$
$$\ldots$$
$$\delta^{k-d+1} f = S_{f,k-d+1,0} z + T_{k-d+1}.$$

Все участвующие в этих формулах обобщенные сепаранты лежат в идеале $S_{d-1} \subset \sqrt{I_k}$. Поэтому

$$\sqrt{I_k} = \sqrt{(f, \delta f, \ldots, \delta^{k-d} f, T_{k-d+1}, \ldots, T_k, h_1, \ldots, h_t) + S_{d-1}}.$$

Поэтому в $\sqrt{I_k}$, а значит и в $\sqrt{I_k} : G_d$, и в P можно выбрать систему образующих из R.

Если $h \in I_{k+1} \cap R$ — произвольный многочлен, то верно сравнение $h \equiv q\delta^{k+1} f \pmod{P}$, причем тогда $qS_{f,k+1,d} \in P$, так как $z \notin R$. Так как по предположению $S_{f,k+1,d} \notin P$ и P является простым, то множитель $q \in P$, откуда $h \in P$. Итак,

$$I_{k+1} \cap R \subset P \implies \sqrt{I_{k+1}} \cap R \subset \sqrt{P} = P \implies$$
$$\implies \sqrt{I_{k+1}} : G_d \cap R \subset P : G_d = P \implies \sqrt{I_k} : G_d \subset \sqrt{I_{k+1}} : G_d \cap R \subset P.$$

Пусть $\sqrt{I_{k+1}} : G_d = \cap_j Q_j$ — минимальное разложение на простые компоненты. Тогда все идеалы $Q_j \cap R$ тоже простые, причем

$$\sqrt{I_k} : G_d \subset \bigcap_j (Q_j \cap R) \subset P.$$

Отсюда следует, что найдется Q, такой, что $Q \cap R = P$, так как P — минимальный простой. Так как все обобщенные сепаранты лежат в R и не лежат в P, то они не лежат и в Q.

Предположим теперь, что имеет место **случай 2**: для каждого минимального простого идеала $P_{k,d,i}$ найдется принадлежащая ему обобщенная сепаранта $S_{f,n,d}$, где $n \geqslant k$. Заметим, что все обобщенные сепаранты лежат в идеале G_d. Выражение для этих обобщенных сепарант является многочленом по n степени d, не равным тождественно нулю по модулю каждого идеала $P_{k,d,i}$ (иначе получилось бы противоречие $G_d \subset P_{k,d,i}$). Отсюда следует, что лишь для конечного набора значений $n \geqslant k$ обобщенная сепаранта $S_{f,n,d}$ может оказаться в идеале $P_{k,d,i}$. Пусть число K больше всех этих значений. Перейдем от k к K и повторим процедуру. Покажем, что такой повтор может произойти не более $d+1$ раз. Действительно, пусть имеется цепочка наборов минимальных простых идеалов $P_{k_j,d,i}$ для идеалов $\sqrt{I_{k_j}} : G_d$ длины $d+1$

$$\bigcap_i P_{k_1,d,i} \subset \bigcap_i P_{k_2,d,i} \subset \ldots \subset \bigcap_i P_{k_{d+1},d,i},$$

причем в каждом из них содержится некоторая обобщенная сепаранта. Выберем по предложению 8 цепочку вложенных простых идеалов:

$$P_{k_1,d,i_1} \subset P_{k_2,d,i_2} \subset \ldots \subset P_{k_{d+1},d,i_{d+1}}.$$

Рассмотрим выражение для обобщенной сепаранты по модулю последнего идеала в этой цепочке. Это не тождественный ноль, а некоторый многочлен по n степени не выше d, имеющий корень по крайней мере в $d+1$ точке, что немедленно приводит нас к противоречию. Итак, по крайней мере за d таких повторов мы либо убедимся, что $\sqrt{I_k} : G_d = (1)$, либо получим простую компоненту этого идеала, не содержащую никаких обобщенных сепарант, и тогда по доказанному выше $I \neq (1)$.

Проведенные рассуждения записаны ниже в виде алгоритма. Алгоритм был реализован авторами в системе компьютерной алгебры Sage[2].

Функция MinimalPrimeDecomposition строит минимальное разложение радикального идеала на простые компоненты. Функция Reduce редуцирует указанный многочлен относительно базиса Грёбнера указанного идеала при каком-либо фиксированном упорядочении. Функция MaxIntegerRoot возвращает максимальный целый корень многочлена по переменной n, либо $-\infty$, если целых корней не существует. Для этого вычисляется наибольший общий делитель (как многочлен от n) всех коэффициентов перед остальными переменными $y_0, \ldots, y_s, \ldots$.

[2]Исходный код доступен на https://github.com/alzobnin/Kolchin/

Вход: многочлен $f \in \mathcal{F}\{y\}$ порядка l, такой, что $\left[f, \frac{\partial f}{\partial y_0}, \ldots, \frac{\partial f}{\partial y_l}\right] = (1)$;
многочлены $h_1, \ldots, h_t \in \mathcal{F}\{y\}$
Выход: `True`, если $[f] + (h_1, \ldots, h_t) = (1)$, и `False`, если $[f] + (h_1, \ldots, h_t) \neq (1)$.

1: **find** k **and** p **such that** $(f, \ldots, \delta^k f) + G_0 + \ldots + G_p = (1)$, $k \geqslant 2p$, **and** $k \geqslant \operatorname{ord} h_i + p - l$
2: $I_k \leftarrow (f, \ldots, \delta^k f, h_1, \ldots, h_t)$
3: $d \leftarrow 0$
4: **while** $d \leqslant p$ **do**
5: **if** $G_d \subset \sqrt{I_k}$ **then**
6: $d \leftarrow d + 1$
7: **continue**
8: $primes \leftarrow \textsc{MinimalPrimeDecomposition}(\sqrt{I_k} : G_d)$
9: $S_{f,n,d}(n) \leftarrow \sum_{j=\max(l-d,0)}^{l} C_n^{d-l+j}\, \delta^{d-l+j}\left(\frac{\partial f}{\partial y_j}\right)$
10: $K \leftarrow k$
11: **for all** $P \in primes$ **do**
12: $r(n) \leftarrow \textsc{Reduce}(S_{f,n,d}(n), P)$
13: $n_{\max} \leftarrow \textsc{MaxIntegerRoot}(r(n))$
14: **if** $n_{\max} < k$ **then**
15: **return** `False`
16: $K \leftarrow \max(K, n_{\max})$
17: $k \leftarrow K + 1$
18: $I_k \leftarrow (f, \ldots, \delta^k f, h_1, \ldots, h_t)$
19: **return** `True`

5 Примеры

В приводимых ниже выкладках можно убедиться с помощью любой системы компьютерной алгебры, позволяющей вычислять базисы Грёбнера.

Пример 1. Рассмотрим дифференциальный многочлен

$$f = y_0 y_1^2 + a y_1^2 + b y_0 y_1 + c,$$

где $c \neq 0$. Выясним, при каких константных значениях параметров a, b и c выполнено $[f] + (S_f) = (1)$. Хотя наш алгоритм не предполагает наличия параметров, мы решим эту задачу в общем виде.

Можно проверить, что $[f] + [S_f] = (1)$. В самом деле, c^2 полиномиально выражается через систему $f, \delta f, \delta^2 f, S_f, \delta S_f$. Поэтому на шаге 1 можно выбрать $p = 1$ и $k = 2$. Соответствующие идеалы G_d и I_k выглядят так:

$$G_0 = (S_f),$$
$$G_1 = \left(\delta S_f, \frac{\partial f}{y_0}\right),$$
$$I_2 = \left(f, \delta f, \delta^2 f, S_f\right).$$

Они рассматриваются в кольце $\mathbb{Q}[y_0, y_1, y_2, y_3]$ (при фиксированных значениях параметров). Заметим, что $G_0 \subset I_2$, поэтому на шаге 5 для $d = 0$ включение будет выполнено и алгоритм перейдет к $d = 1$. Построим идеал $\sqrt{I_2} : G_1$. Рассматривая его в $\mathbb{Q}[a, b, c, y_0, y_1, y_2, y_3]$ и исключая переменные y_j, получим многочлен $c + ab^2$. Итак, если $c + ab^2 \neq 0$, то $\sqrt{I_2} : G_1 = (1)$, то есть, включение на шаге 5 снова выполнено, цикл закончится и алгоритм вернет `True`. В этом случае $[f] + (S_f) = (1)$.

Пусть теперь $c + ab^2 = 0$. В этом случае алгоритм должен на шаге 8 построить разложение идеала $\sqrt{I_2} : G_1$ на минимальные простые компоненты. Выполним эту операцию в кольце $\mathbb{Q}[a, b, c, y_0, y_1, y_2, y_3]$. В результате мы получим разложение идеала $\sqrt{I_2} : G_1$ на две компоненты, которые, однако, могут утратить свойство простоты при подстановке вместо параметров a, b и c

конкретных значений. Тем не менее, уже в этом случае остатки $r(n)$ для каждой из компонент на шаге 12 дают многочлены, пропорциональные $b^2 n$, причем по предположению $b^2 \neq 0$, так как $c \neq 0$. Единственный целый корень 0 этих многочленов меньше текущего значения $k = 2$, поэтому алгоритм на шаге 15 вернет `False`, то есть, при $c + ab^2 = 0$ идеал $[f] + (S_f)$ отличен от всего кольца.

Пример 2. Рассмотрим многочлен $f = (y_1 - a)^2 - b^2 y_0^4 y_1^2$, где коэффициенты a и b отличны от нуля. Заметим, что ab полиномиально выражается через $f, \ldots, \delta^4 f, S_f, \delta S_f, \delta^2 S_f$. Значит, при любых ненулевых a и b идеал $[f] + [S_f]$ тривиален. Здесь нам потребовалось дважды продифференцировать сепаранту S_f. Выясним, возможна ли ситуация $[f] + (S_f, \delta S_f) = (1)$.

На шаге 1 можно выбрать $p = 2$ и $k = 4$. Тогда

$$I_4 = (f, \ldots, \delta^4 f, S_f, \delta S_f).$$

Заметим, что при $d = 0$ и $d = 1$ идеалы $\sqrt{I_4} : G_d$ оказываются тривиальными. Переходим к последней итерации внешнего цикла алгоритма при $d = 2$. В кольце $\mathbb{Q}[a, b, y_0, y_1, y_2, y_3]$ идеал $\sqrt{I_4} : G_2$ раскладывается в пересечение двух простых компонент, которые порождаются элементами

$$y_0,\ y_1 - a,\ y_2,\ y_3 - 2a^3 b$$

и

$$y_0,\ y_1 - a,\ y_2,\ y_3 + 2a^3 b.$$

Видно, что при конкретных значениях параметров a и b эти идеалы остаются простыми в кольце $\mathbb{Q}[y_0, y_1, y_2, y_3]$. Остаток от редукции многочлена $S_{f,n,2}(n)$ относительно первого из них равен $2a^3 bn(n-1)$. Целые корни этого многочлена, 0 и 1, меньше текущего значения $k = 4$, поэтому алгоритм вернет `False` в строке 15. Итак, при всех ненулевых a и b идеал $[f] + (S_f, \delta S_f)$ отличен от единичного.

Список литературы

[1] М. Атья, И. Макдональд. *Введение в коммутативную алгебру.* М., «Мир», 1972.

[2] Д. Кокс, Д. Литтл, Д. О'Ши. *Идеалы, многообразия и алгоритмы.* М., «Мир», 2000.

[3] Д. В. Трушин. *Идеал сепарант в кольце дифференциальных многочленов.* Фундаментальная и прикладная математика, том 13, вып. 1, 215–227, 2007.

[4] F. Boulier, D. Lazard, F. Ollivier, M. Petitot. *Representation for the Radical of a Finitely Generated Differential Ideal.* In Proceedings of 1995 International Symposium on Symbolic and Algebraic Computation (ISSAC-1995), ACM Press, 158–166, 1995.

[5] G. Carrà Ferro. *Diferential Gröbner Bases in One Variable and in the Partial Case.* Math. Comput. Modelling, Pergamon Press, vol. 25, 1–10, 1997.

[6] E. R. Kolchin. *On the Exponents of Differential Ideals.* The Annals of Mathematics, Second Series, vol. 42 (3), 740–777, 1941.

[7] E. R. Kolchin. *Differential algebra and algebraic groups.* Academic Press, 1973.

[8] W. Sit. *The Ritt-Kolchin Theory for Differential Polynomials.* Differential Algebra and Related Topics, 2000.

[9] A. Zobnin. *Admissible Orderings and Finiteness Criteria for Differential Standard Bases.* In Proceedings of International Symposium on Symbolic and Algebraic Computation (ISSAC-2005), ACM Press, 365–372 (2005).