

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев В. М., Тихомиров В. М., Фомин С. В. Оптимальное управление. М., 1979.
2. Треногин В. А. Функциональный анализ. М., 1980.
3. Ленг С. Введение в теорию дифференцируемых многообразий. М., 1967.
4. Аваков Е. Р., Аграчев А. А., Арутюнов А. В. Множество уровня гладкого отображения в окрестности особой точки и нули квадратичного отображения//Мат. сб. 1991. 182, № 8. С. 1091—1104.
5. Третьяков А. А. Структуры нелинейных вырожденных отображений и их применение к построению численных методов: Докт. дис. М., ИПК АН. 1987.
6. Иоффе О. Д., Тихомиров В. М. Теория экстремальных задач. М., 1974.
7. Третьяков А. А. Необходимые и достаточные условия оптимальности P -го порядка//ЖВМ и МФ. 1984. 24, № 2. С. 203—209.

Поступила в редакцию
16.07.92

ВЕСТН. МОСК. УН-ТА. СЕР. 15. ВЫЧИСЛ. МАТЕМ. И КИБЕРН. 1993. № 2

УДК 512.7

С. А. Абрамов, К. Ю. Квашенко

НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ ПОЛИНОМОВ, ЗАВИСЯЩИХ ОТ ПАРАМЕТРА

(кафедра алгоритмических языков факультета ВМиК)

1. *Введение.* При внимательном взгляде на алгоритмы компьютерной алгебры, опирающиеся на исследование корней результата полиномов бросается в глаза, что, как правило, после вычисления результата $R(a)$ полиномов $u(x, a)$, $v(x, a)$ требуется построение НОД $(u(x, a_i), v(x, a_i))$ для всех или некоторых значений $a_1, \dots, a_k$ корней $R(a)$. Примеров можно привести много: решение систем алгебраических уравнений методами теории исключения [1], нахождение логарифмической части интеграла рациональной функции [2, 3], решение дифференциальных и разностных уравнений [4, 5], суммирование рациональных функций [6, 7, 8] и т. д. Таким образом, возникает задача совместного исследования корней результата и вычисления соответствующих НОД. Эта задача является частным случаем более общей задачи вычисления НОД полиномов, зависящих от параметра.

2. *Субрезультанты и их свойства.* Важную роль в дальнейшем изложении будут играть *субрезультанты* полиномов. Приведем здесь определение и основные свойства субрезультантов. Рассмотрим полиномы $u(x)$, $v(x) \in I[x]$:

$$u(x) = u_m x^m + \dots + u_1 x + u_0, \quad v(x) = v_n x^n + \dots + v_1 x + v_0. \quad (1)$$

Здесь I — область целостности (т. е. коммутативное кольцо с единицей без делителей нуля). Известно, что результат $\text{Res}(u, v)$ полиномов $u(x)$ и $v(x)$ равен нулю тогда и только тогда, когда либо $u(x)$ и $v(x)$ обладают нетривиальным общим делителем, либо $u_m = v_n = 0$.

Понятие субрезультанта является обобщением понятия результата [9, 10]: j -м субрезультантом полиномов $u(x)$, $v(x)$, $0 \leq j < \min(m, n) - 1$, называется определитель следующей матрицы порядка $m + n - 2j$:

$$\begin{pmatrix} u_m & \dots & u_0 & & x^{n-j-1} u(x) \\ & \ddots & & & \vdots \\ & & u_m & \dots & u_0 & x^j u(x) \\ & & & \ddots & u_1 & x^{j-1} u(x) \\ & & & & \vdots & \vdots \\ & & & & u_{j+1} & u(x) \\ v_n & \dots & u_m & \dots & u_0 & x^{m-j-1} v(x) \\ & \ddots & & & \vdots & \vdots \\ & & v_n & \dots & v_0 & x^j v(x) \\ & & & \ddots & v_1 & x^{j-1} v(x) \\ & & & & \vdots & \vdots \\ & & & & v_{j+1} & v(x) \end{pmatrix}$$

Обозначим j -й субрезультант $u(x)$, $v(x)$ через $S_j(x)$; ясно, что $S_j(x) \in I[x]$. Можно показать, что $\deg S_j(x) \leq j$ для всех $j=0, \dots, n$; при этом $S_0(x) = \text{Res}(u(x), v(x))$.

Обычно рассматривается цепочка субрезультантов

$$S_k(x), S_{k-1}(x), \dots, S_0(x), \quad (2)$$

где

$$k = \begin{cases} m, & \text{если } m > 1. \\ n+1 & \text{в противном случае.} \end{cases}$$

При этом члены $S_{\min(m,n)-1}(x), \dots, S_0(x)$ определяются так, как объяснялось выше, $S_k(x) = u(x)$, $S_{k-1}(x) = v(x)$. При $m > n+1$ члены $S_{k-2}(x), \dots, S_{n+1}(x)$ полагаются равными нулю, а $S_n(x)$ — равным $(v_n)^{m-n-1}v(x)$. Смысл такого доопределения будет понятен из дальнейшего изложения.

Если в качестве кольца I привлекается $K[a]$, где K — некоторое поле, a — переменная (параметр), то все $S_i(x)$, $j=k, \dots, 0$, являются полиномами от x и a над K . Запишем исходные полиномы u, v в виде

$$u(x, a) = u_m(a)x^m + \dots + u_0(a), \quad v(x, a) = v_n(a)x^n + \dots + v_0(a), \quad (3)$$

$u_m(a), v_n(a)$ — ненулевые элементы $K[a]$. Мы можем построить для (3) цепочку субрезультантов. Пусть теперь для параметра a выбрано конкретное значение α , принадлежащее некоторому расширению L поля K (в частности, L может совпадать с K). Пусть α таково, что $u_m(\alpha), v_n(\alpha)$ одновременно не равны нулю, и, помимо этого, $u(x, \alpha), v(x, \alpha) \neq 0$ как элементы $L[x]$. (Последнее будет заведомо выполнено, если (3) — примитивные полиномы при взгляде на них как на полиномы от x над $K[a]$.)

Для $u(x, \alpha), v(x, \alpha)$ можно в свою очередь построить цепочку субрезультантов

$$S_l^*(x), \dots, S_0^*(x), \quad l \leq k.$$

Если $u_m(\alpha) \neq 0$ и $v_n(\alpha) \neq 0$, то $l=k$ и $S_k(x, \alpha) = S_k^*(x)$, ..., $S_0(x, \alpha) = S_0^*(x)$. Пусть теперь $u_m(\alpha) = 0$, $v_n(\alpha) \neq 0$ (случай $u_m(\alpha) \neq 0$, $v_n(\alpha) = 0$ рассматривается аналогично). Введем натуральное d такое, что $u_m(\alpha) = \dots = u_{m-d+1}(\alpha) = 0$, $u_{m-d}(\alpha) \neq 0$. Тогда с точностью до знака справедливы равенства

$$S_i(x, \alpha) = v_n^d(\alpha) S_i^*(x), \quad 0 \leq i \leq \min(n, m-d).$$

Приведенные равенства получаются несложными преобразованиями определителей; они показывают, что в интересующих нас пределах изменения индекса i полиномы $S_i(x, a)$ и $S_i^*(x)$ отличаются ненулевым множителем.

Наконец, известно, что если исходные полиномы являются полиномами от x над некоторым полем и если коэффициент при x^i в полиноме $S_j(x)$ равен s_j , то при $s_0 = \dots = s_{i-1} = 0$, $s_i \neq 0$ исходные полиномы имеют НОД, равный $S_i(x)$.

3. *Вычисление цепочки субрезультантов.* Здесь нам окажется полезным понятие *регулярного* (и соответственно *нерегулярного*) субрезультанта. Если $j \leq \min(m, n) - 1$, то для полиномов (1) субрезультант $S_j(x)$ регулярен тогда и только тогда, когда $\deg S_j(x) = j$. Нулевой субрезультант всегда нерегулярен. Начальный член цепочки (2) будем считать регулярным, член $S_{k-1}(x)$ считать регулярным при $m \leq n$, а при $m > n$ — если только $m - 1 = n$. Такое распространение на $S_k(x)$, $S_{k-1}(x)$ понятий регулярного и нерегулярного субрезультантов полностью согласуется с графическими диаграммами, приведенными в положившей начало теории субрезультантов работе [9].

Перед тем как обсуждать вычисление субрезультантов, напомним, что *псевдоостатком* $\text{prem}(u(x), v(x))$ от деления $u(x)$ на $v(x)$, где $u(x), v(x) \in I[x]$, называется $r(x) \in I[x]$ такой, что для некоторого $q(x) \in I[x]$ имеет место

$$(\text{lc } v(x))^{\deg u(x) - \deg v(x) + 1} u(x) = q(x) v(x) + r(x), \quad (4)$$

и при этом либо $r(x) = 0$, либо $\deg r(x) < \deg v(x)$.

Алгоритм вычисления цепочки субрезультантов основывается на теореме Габихта [9]. Эта теорема, по существу, утверждает, что если два исходных полинома (1) таковы, что $m > n > 0$, и если уже построенная начальная часть

$$S_k(x), \dots, S_{j+1}(x), S_j(x), 0 < j < k, \quad (5)$$

всей цепочки субрезультантов (2) и при этом предпоследний член (5) является регулярным, а последний — ненулевым субрезультантом, то (5) можно легко дополнить еще несколькими членами. В итоге получится либо вся цепочка (2), либо такая ее часть

$$S_k(x), S_{k-1}(x), \dots, S_i(x), 0 < i < j,$$

предпоследний член которой опять-таки является регулярным, а последний — ненулевым.

При нерегулярном $S_j(x)$ ($\deg S_j(x) = r$) следует положить $S_{j-1}(x) = \dots = S_{r+1}(x) = 0$, затем положить

$$S_r(x) = \begin{cases} (\text{lc } S_j(x))^{j-r} S_j(x), & \text{если } j = k-1, \\ (\text{lc } S_j(x))^{j-r} S_j(x) / (\text{lc } S_{j+1}(x))^{j-r} - \text{иначе,} \end{cases} \quad (6)$$

а после этого, если $r > 0$, положить еще

$$S_{r-1}(x) = \begin{cases} \text{prem}(S_{j+1}(x), S_j(x)), & \text{если } j = k-1, \\ \text{prem}(S_{j+1}(x), S_j(x)) / (\text{lc } S_{j+1}(x))^{j-r+2} - \text{иначе.} \end{cases} \quad (7)$$

Если же $S_j(x)$ — регулярный субрезультант, то к (5) добавляется только один член $S_{j-1}(x)$, вычисленный по формулам (7), в которых вместо r выступает j .

Если в результате этих вычислений последний найденный член цепочки субрезультантов окажется нулевым, то следует все ее оставшие-

ся члены положить равными нулю. Поскольку нам известны первые два члена цепочки (5) и для начальной части $S_k(x)$, $S_{k-1}(x)$ заведомо выполнено условие теоремы, то утверждение этой теоремы позволяет построить всю цепочку (2) целиком.

Может быть показано, что утверждение теоремы Габихта остается в силе и при $m < n$. В работе [10] теорема ошибочно распространяется на случай $m = n$. Это привело к тому, что описанный в этой работе алгоритм 4.1, предназначенный для вычисления цепочки субрезультантов, является неверным. Для внесения необходимого исправления можно использовать тот факт, что при нахождении по формуле (4) псевдоостатка от деления полиномов одинаковой степени производится домножение делимого на первую степень старшего коэффициента делителя, а во всех случаях — не меньше чем на вторую степень. Это дает возможность показать, как формулы (6) — (7) должны быть подкорректированы при $m = n$: в формулу (6) должно быть добавлено $S_r(x) = (\text{lc } S_j(x))^{j-r} S_j(x)$ при $j = k-2$; а в формулу (7) — $S_{r-1}(x) = \text{prem}(S_{j+1}(x), S_j(x)) / (\text{lc } S_{j+1}(x))$ при $j = k-2$.

4. Поиск НОД полиномов, зависящих от параметра. Пусть $u, v \in K[a][x]$, где K — некоторое поле, a — неопределенный параметр. Интересующий нас вопрос состоит в том, какой НОД имеют полиномы $u(x, a)$ и $v(x, a)$ при тех или иных значениях параметра a . В простейшем примере $u(x, a) = x$, $v(x, a) = x + a$ имеем

$$\text{НОД}(u, v) = \begin{cases} x, & \text{если } a = 0, \\ 1 & \text{в противном случае.} \end{cases}$$

В самом деле, $\text{Res}_x(u, v) = a$ и 0 — единственный корень результата.

Обратимся теперь к свойству субрезультантов, упомянутому в конце пункта 2. Вместе с рассмотренными в пункте 2 соотношениями между $S_i(x, a)$ и $S_i^*(x)$ это свойство говорит о том, что если полиномы (3) обладают ненулевым результатом $R(a) = \text{Res}_x(u, v) = S_0(x, a)$ и если α — корень $R(a)$, то для вычисления $\text{НОД}(u(x, \alpha), v(x, \alpha))$ достаточно просмотреть $S_0(x, a)$, $S_1(x, a)$, ... и выбрать из них первый $S_j(x, a)$, для которого выполнено $\deg_x S_j(x, a) = j$. Тогда $\text{НОД}(u(x, \alpha), v(x, \alpha)) = S_j(x, a)$. Если же $R(a) \neq 0$, то $\text{НОД}(u(x, a), v(x, a)) = 1$.

Если теперь $u(x, a)$, $v(x, a)$ обладают нетривиальным общим делителем в кольце $K[a, x]$, то $S_0(x, a)$ — нулевой полином. Пусть первым ненулевым субрезультантом среди $S_1(x, a)$, ..., $S_n(x, a)$ будет $S_t(x, a)$, $t > 0$. Согласно теории субрезультантов, $\deg_x S_t(x, a) = t$. Положив $R(a) = \text{lc}_x S_t(x, a)$, можно для любого корня α полинома $R(a)$ проделать те же действия, что и выше, и найти $\text{НОД}(u(x, \alpha), v(x, \alpha))$. Если же $R(a) \neq 0$, то $\text{НОД}(u(x, a), v(x, a)) = S_t(x, a)$.

Заметим, что для выполнения этой работы не обязательно иметь всю цепочку субрезультантов полиномов $u(x, a)$, $v(x, a)$ — достаточно рассмотреть ее подцепочку, состоящую из всех регулярных субрезультантов.

Представляет практический интерес модификация описанного выше метода, не требующая явного выписывания корней полинома $R(a)$. Подстановку корня α вместо a в субрезультанты можно заменить несложной НОД-техникой. Пусть $r(a)$ — это освобожденный от квадратов полином $R(a)$ и $S_j(x, a)$ — исследуемый в данный момент субрезультант. Найдем $h(a) = \text{НОД}(r(a), \text{lc}_x S_j(x, a))$, $w(a) = r(a)/h(a)$. Корни полинома $h(a)$ обращают в нуль старший коэффициент $S_j(x, a)$, а корни полинома $w(a)$ — нет. Поэтому для лю-

блого корня α полинома $w(a)$ выполнено $\text{НОД}(u(x, \alpha), v(x, \alpha)) = S_j(x, \alpha)$. Действия, аналогичные тем, которые были проделаны над $r(a)$ и $S_j(x, a)$, можно теперь проделать над $h(a)$ и S_{j+1} и т. д.

Ранее мы накладывали на значение параметра a некоторые ограничения: предполагалось, что $u_m(a)$ и $v_n(a)$ одновременно не равны нулю и что $u(x, a), v(x, a)$ — ненулевые полиномы от x . Отказ от этих ограничений влечет появление некоторых добавочных действий. Прежде всего выделим из $u(x, a)$ и $v(x, a)$ как полиномов от x над $K[a]$ их содержания, рассмотрим случаи равенства содержаний нулю и перейдем от исходных полиномов к их примитивным частям. Сохраним за примитивными частями обозначения (3). Пусть теперь $u_m(a), v_n(a)$ имеют нетривиальный общий делитель $b(a)$. Тогда, построив $r(a)$, можно разбить его на два множителя: $r_1(a) = \text{НОД}(r(a), b(a))$, $r_2(a) = r(a)/r_1(a)$. Все корни полинома $r_2(a)$ таковы, что при их подстановке вместо a полиномы $u_m(a)$ и $v_n(a)$ одновременно не обращаются в нуль. Рассматривая же случаи, когда значения параметра удовлетворяют уравнению $r_1(a) = 0$, можно, во-первых, удалить из полиномов (3) их старшие члены и, во-вторых, получив для этих новых полиномов аналог $\tilde{r}(a)$ полинома $r(a)$, подкорректировать его, заменив на $\text{НОД}(\tilde{r}(a), r_1(a))$.

Из сказанного видно, что обсуждаемый алгоритм удобно рассматривать как алгоритм, на вход которого подаются полиномы (3) и дополнительно некоторое алгебраическое условие $p(a) = 0$ (оно, в частности, может быть тривиальным: $0 = 0$). На выходе же получается список одного из двух видов:

$$(d_1(a), G_1(x, a)), \dots, (d_k(a), G_k(x, a)),$$

$$(d_1(a), G_1(x, a)), \dots, (d_k(a), G_k(x, a)), (0, G_{k+1}(x, a)).$$

Здесь $d_i(a)$ — полином, задающий условие $d_i(a) = 0$, а $G_i(x, a)$ — соответствующий данным значениям параметра НОД. Полиномы $d_1(a), \dots, d_k(a)$ являются взаимно простыми, свободными от квадратов, и, кроме того, для всех корней α полинома $d_i(a)$ старший коэффициент полинома $G_i(x, a)$ отличен от нуля ($i = 1, \dots, k$). Если последняя пара списка имеет вид $(0, G_{k+1}(x, a))$, то это означает, что для всех значений параметра a , не являющихся корнями полиномов $d_1(a), \dots, d_k(a)$, выполнено $\text{НОД}(u, v) = G_{k+1}(x, a)$ (такая ситуация возникает, только когда рассматриваемое условие $p(a) = 0$ тривиально.)

Для того чтобы найти НОД полиномов, зависящих от неопределенного параметра, достаточно применить описанный выше алгоритм, взяв в качестве полинома $p(a)$ нулевой полином. Область применения данного алгоритма достаточно широка: с его помощью можно, например, найти наибольший общий делитель полиномов с алгебраическими коэффициентами. Здесь в качестве полинома $p(a)$ выступает определяющий полином алгебраического числа. Может применяться алгоритм и при построении разбиений по методу D5 [11] — одному из методов работы с алгебраическими числами.

В частных ситуациях задача нахождения НОД полиномов, зависящих от параметра, может быть решена более простыми средствами. Например, в [3] интегрирование рациональной функции сводится к поиску $\text{НОД}(u(x), v(x) - au'(x))$, где a — неопределенный параметр, $u(x), v(x)$ — полиномы над некоторым числовым полем, $u(x)$ свободен от квадратов и $\deg v(x) < \deg u(x)$. Ясно, что НОД будет нетривиальным только для тех значений $a = \alpha$, которые являются корнями результата

$$\text{Res}_x(u(x), v(x) - au'(x)). \quad (8)$$

Используя известную процедуру разложения полинома на свободные от квадратов множители, результат (8) можно представить в виде

$$\prod_{i=1}^n r_i(a)^i. \quad (9)$$

В [3] показано, что для всех a таких, что $r_i(a) \neq 0$, выполнено $\text{НОД}(u(x), v(x) - au'(x)) = S_i(x, a)$, где $S_i(x, a)$ — i -й субрезультант полиномов $u(x)$, $v(x) - au'(x)$. Поэтому, построив цепочку субрезультантов и получив разложение (9), можно сразу получить ответ в виде

$$(r_1(a), S_1(x, a)), \dots, (r_n(a), S_n(x, a)), (0, 1).$$

Здесь существенно использовано то обстоятельство, что для случая, когда один из исходных полиномов не зависит от параметра a , а во второй полином этот параметр входит в первой степени, степень их НОД при конкретном значении a параметра равна кратности a как корня результата. В общем случае отождествление степени НОД с кратностью корня результата неправомерно. Например, $\text{Res}_x(x^2 - a^2, x^2 + a^2) = 4a^4$, здесь $a=0$ — корень кратности 4, которому соответствует НОД степени 2. Поэтому схема, предложенная в [3], не может быть перенесена на общий случай.

5. *Реализация алгоритма.* Описанный выше алгоритм реализован в виде программы, предназначенной для использования в системе компьютерной алгебры Редьюс [12]. Приведем ряд примеров работы алгоритма, полученных на персональном компьютере IBM-PC/AT (286, 12 МГц). Время поиска НОД указано в миллисекундах (10^{-3} с).

GCD of the polynomials in the variable $\langle X \rangle$ with the parameter $\langle A \rangle$

$$X^2 + (A-1)X + A$$

$$(A+1)X^2 + 2A$$

is equal to:

$$\{A-1, X^2+1\},$$

$$\{3A^2+2A, X+3A\},$$

$$\{0, 1\}$$

Time: 440 ms

GCD of the polynomials in the variable $\langle X \rangle$ with the parameter $\langle A \rangle$

$$AX^3 + (A^3 - A + 1)X^2 + (A^2 + 2)X + 3A^2 - 3$$

$$AX^3 + (A+1)X^2 + 4X + 3$$

is equal to:

$$\{A^2-2, 2X^3+X^2(A+2)+4XA+3A\},$$

$$\{A, X+3\},$$

$$\{0, X^2A+X+3\}$$

Time: 600 ms

GCD of the polynomials in the variable $\langle Y \rangle$ with the parameter $\langle S \rangle$

$$Y^4 - S^2Y^2 + (S^2+S)Y - S^3 - S^2$$

$$SY^3 + (-S^2+1)Y^2 - SY$$

under condition

$$S^7 + S^6 + 3S^5 + 4S^4 + 2S^2 - 3 = 0$$

is equal to:

$$\{S+1, Y^3-Y\},$$

$$\{S^4+S-1, Y^2+Y(S^4+S^3)-S^4-S\},$$

$$\{S^2+3, Y-S\}$$

Time: 1040 ms

СПИСОК ЛИТЕРАТУРЫ

1. Варден Б. Л. ван дер. Современная алгебра. М.; Л., 1947, Т. 1, 2.
2. Trager B. M. Algebraic factoring and rational function integration//Proc. 1976 Symp. on Symbolic and Algebraic Computation. 1976. P. 219—226.
3. Lazard D., Rioboo R. Integration of rational functions: rational computation of the logarithmic part//J. Symb. Comp. 1990. N 9. P. 113—115.
4. Абрамов С. А. Задачи компьютерной алгебры, связанные с поиском полиномиальных решений линейных дифференциальных и разностных уравнений//Вестн. Моск. ун-та. Сер. 15, Вычисл. матем. и киберн. 1989. № 3. С. 56—60.
5. Абрамов С. А. Рациональные решения линейных обыкновенных дифференциальных и разностных уравнений с полиномиальными коэффициентами//ЖВМ и МФ. 1989. № 11. С. 1611—1620.
6. Абрамов С. А. О суммировании рациональных функций//ЖВМ и МФ. 1971. № 1. С. 1071—1075.
7. Абрамов С. А. Рациональная компонента решения линейного рекуррентного соотношения первого порядка с рациональной правой частью//ЖВМ и МФ. 1975. № 4. С. 1035—1039.
8. Gosper R. W. Decision procedure for indefinite hypergeometric summation//Proc. Nat. Acad. Sci. USA 75/1. 1978. P. 40—42.
9. Habicht W. Eine Verallgemeinerung des Sturmschen Wurzelzählverfahrens//Commentarii math. Helvetici. 1948. N 21. S. 99—116.
10. Лоос Р. Обобщенные последовательности полиномиальных остатков//Компьютерная алгебра. Символьные и алгебраические вычисления. М., 1986. С. 151—177.
11. Della Dora J., Dicrescenzo C., Duval D. About a new method for computing in algebraic number fields//LNCS. 204. P. 289—290.
12. Hearn A. C. REDUCE User's Manual, version 3.4. The RAND Corporation. Santa Monica, 1991.

Поступила в редакцию
10.06.92