

On the greatest common divisor of polynomials which depend on a parameter

S.A.Abramov K.Yu.Kvashenko
Computer Center of the Russian Academy of Science
Vavilova 40, Moscow 117967, Russia
e-mail: abramov@sms.ccas.msk.su

Abstract

The following computer algebra problem is considered : how to compute the gcd of the polynomials $u(x, a)$ and $v(x, a)$ for various values of the parameter a ? This problem appears, for example, in solving systems of algebraic equations by the elimination methods [Waer53], in computing the logarithmic part of the integral of a rational function [Trag76, Laz&Rio90], in solving difference and differential equations [Abr89], in summing rational functions [Abr71, Abr75, Gosp78], etc...

A fast algorithm to solve this problem is described, and some applications of this algorithm are discussed.

1 Subresultants

Polynomial subresultants play an important role in our consideration. Let us briefly point out the main properties of subresultants, considering the polynomials $u(x), v(x) \in I[x]$:

$$\begin{aligned} u(x) &= u_m x^m + \dots + u_1 x + u_0, \\ v(x) &= v_n x^n + \dots + v_1 x + v_0, \end{aligned} \tag{1}$$

where I is an integral domain. It is well known that the resultant $\text{Res}(u, v)$ of the polynomials (1) is equal to zero iff either $u(x)$ and $v(x)$ have a nontrivial gcd, or $u_m = v_n = 0$.

The notion of subresultant generalizes the one of resultant (cf. [Hab48, Loos83]): the determinant of the $m + n - 2j$ -dimensional Subresultant matrix (Figure 1) with $0 \leq j < \min(m, n) - 1$ is called the j^{th} subresultant of the polynomials $u(x)$ and $v(x)$. Let us write

Permission to copy without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage, the ACM copyright notice and the title of the publication and its date appear, and notice is given that copying is by permission of the Association for Computing Machinery. To copy otherwise, or to republish, requires a fee and/or specific permission.

ACM-ISSAC '93-7/93/Kiev, Ukraine

© 1993 ACM 0-89791-604-2/93/0007/0152...\$1.50

$S_j(x)$ for the j^{th} subresultant of $u(x)$ and $v(x)$; obviously, $S_j(x) \in I[x]$. It is easy to see that $\deg S_j(x) \leq j$ for $j = 0, \dots, n$; besides, $S_0(x) = \text{Res}(u(x), v(x))$.

In the rest of this paper, we will ignore the signs of the subresultants.

The subresultant chain of the polynomials (1) is

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

where

$$k = \begin{cases} m, & \text{if } m > n, \\ n + 1, & \text{otherwise.} \end{cases}$$

Here $S_{\min(m,n)-1}(x), \dots, S_0(x)$ are determined as above, $S_k(x) = u(x)$, $S_{k-1}(x) = v(x)$. For $m > n + 1$ the subresultants $S_{k-2}(x), \dots, S_{n+1}(x)$ are set to zero and $S_n(x) = (v_n)^{m-n-1} v(x)$. The sense of the last assignments will be clear from the further considerations.

If $I = K[a]$, where K is a field and a is a variable (parameter), then all the $S_i(x)$, $i = k, \dots, 0$ are polynomials in x and a over K . Let us rewrite the polynomials (1) as

$$\begin{aligned} u(x, a) &= u_m(a)x^m + \dots + u_0(a), \\ v(x, a) &= v_n(a)x^n + \dots + v_0(a), \end{aligned} \tag{3}$$

where $u_m(a), v_n(a)$ are non-zero elements of $K[a]$. One can construct the subresultant chain $S_k(x, a), \dots, S_0(x, a)$ of the polynomials (3). Let now the parameter a have a value α in some extension L of the field K (in particular $L = K$). Let α be such that $u_m(\alpha), v_n(\alpha)$ are not zero simultaneously, moreover $u(x, \alpha), v(x, \alpha) \neq 0$ as elements of $L[x]$.

It is possible, in turn, to construct the subresultant chain of $u(x, \alpha), v(x, \alpha)$

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

If $u_m(\alpha) \neq 0$ and $v_n(\alpha) \neq 0$, then $l = k$ and $S_k(x, \alpha) = S_k^*(x), \dots, S_0(x, \alpha) = S_0^*(x)$. Suppose that $u_m(\alpha) = 0$ and $v_n(\alpha) \neq 0$ (the case $u_m(\alpha) \neq 0$ and $v_n(\alpha) = 0$ is

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

Figure 1: Subresultant matrix.

analogous). One can introduce the positive integer d such that

$$\begin{aligned} u_m(\alpha) &= \dots = u_{m-d+1}(\alpha) = 0, \\ u_{m-d}(\alpha) &\neq 0. \end{aligned}$$

The following equalities are then satisfied:

$$\begin{aligned} S_i(x, \alpha) &= v_n^d(\alpha) S_i^*(x), \\ 0 \leq i &\leq \min(n, m-d). \end{aligned} \quad (4)$$

Those equalities are obtained by transformations of determinants; they point out that the polynomials $S_i(x, \alpha)$ and $S_i^*(x)$ differ by a non-zero constant for some i 's.

If $\deg \gcd(u(x, \alpha), v(x, \alpha)) = i$ then, obviously, $i \leq \min(n, m-d)$. The subresultant chain $S_k(x, a), \dots, S_0(x, a)$ can have two elements of degree i . The above reasoning guarantees that the element with lower index (i.e. the regular element of degree i) gives $\gcd(u(x, \alpha), v(x, \alpha))$ if α is substituted for a in it.

Finally, let (1) be polynomials in x over a field, and s_j be the coefficient of x^j in $S_j(x)$. It is known that if $s_0 = \dots = s_{t-1} = 0$ and $s_t \neq 0$, then the gcd of the polynomials (1) is equal to $S_t(x)$.

2 Subresultant chain computation

Let us define the notion of a *regular* (and, correspondingly *irregular*) subresultant. The subresultant $S_j(x)$ of the polynomials (1) is regular iff $\deg S_j(x) = j$. The zero subresultant is always irregular. The first member of the chain (2) is always regular; the second one is regular iff $m \leq n+1$.

Let us recall that the polynomial $r(x) \in I[x]$ is called the *pseudo-remainder* $\text{prem}(u(x), v(x))$ of $u(x), v(x) \in I[x]$, if there exists $q(x) \in I[x]$ such that

$$(\text{lc } v(x))^{\deg u(x) - \deg v(x) + 1} u(x) = q(x)v(x) + r(x), \quad (5)$$

and either $r(x) = 0$, or $\deg r(x) < \deg v(x)$.

The algorithm to compute the subresultant chain is based on a theorem of Habicht [Hab48]. That theorem states that if one has polynomials (1) with $m > n > 0$, and has already constructed the part

$$S_k(x), \dots, S_{j+1}(x), S_j(x), \quad 0 < j < k \quad (6)$$

of the subresultant chain (2), where $S_{j+1}(x)$ is a regular subresultant and $S_j(x)$ is non-zero, then one can easily add some new members to (6). This process results in either the complete chain (2) or a part of (2)

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

such that again $S_{i+1}(x)$ is a regular subresultant and $S_i(x)$ is non-zero.

For an irregular $S_j(x)$ ($\deg S_j(x) = r$), one has to set $S_{j-1}(x) = \dots = S_{r+1}(x) = 0$, then set

$$S_r(x) = \begin{cases} (\text{lc } S_j(x))^{j-r} S_j(x), & \text{if } j = k-1, \\ \frac{(\text{lc } S_j(x))^{j-r} S_j(x)}{(\text{lc } S_{j+1}(x))^{j-r}}, & \text{otherwise,} \end{cases} \quad (7)$$

and after that, if $r > 0$, set

$$S_{r-1}(x) = \begin{cases} \text{prem}(S_{j+1}(x), S_j(x)), & \text{if } j = k-1, \\ \frac{\text{prem}(S_{j+1}(x), S_j(x))}{(\text{lc } S_{j+1}(x))^{j-r+2}}, & \text{otherwise.} \end{cases} \quad (8)$$

If $S_j(x)$ is now a regular subresultant, then one has to add to (6) only $S_{j-1}(x)$ which is computed by formula (8) with $r = j$.

Finally, if the last computed subresultant is equal to zero, then all the noncomputed subresultants must be set to zero. We know the first two members of the chain (6), and for $S_k(x), S_{k-1}(x)$ the conditions of the theorem hold, so we can construct the complete chain (2).

One can prove that the theorem is correct for $m < n$. In [Loos83] the theorem is extended by mistake to the case $m = n$. This causes a gap in algorithm 4.1, which computes the subresultant chain. To overcome this gap, the following fact can be used: when one evaluates the pseudo-remainder of two polynomials of the same degree by formula (5), then $u(x)$ is multiplied by the first power of $\text{lc } v(x)$; in all the other cases $u(x)$ is multiplied by at least the square of $\text{lc } v(x)$. This makes it possible to conclude that for $m = n$ formula (7) must include one more case: $S_r(x) = (\text{lc } S_j(x))^{j-r} S_j(x)$ if $j = k - 2$; and formula (8) also has one more case: $S_{r-1}(x) = \text{prem}(S_{j+1}(x), S_j(x)) / (\text{lc } S_{j+1}(x))$ if $j = k - 2$.

3 GCD with a parameter

Let $u, v \in K[a][x]$, where K is a field and a is an undetermined parameter. The question is what is the gcd of the polynomials $u(x, a)$ and $v(x, a)$ for various values of a . The simple example $u(x, a) = x$, $v(x, a) = x + a$ gives

$$\gcd(u, v) = \begin{cases} x, & \text{if } a = 0, \\ 1, & \text{otherwise.} \end{cases}$$

Let us turn back to the property of subresultants mentioned at the end of Section 1. This property together with the equalities (4) point out that if the polynomials (3) have a non-zero resultant $R(a) = \text{Res}_x(u, v) = S_0(x, a)$, and if α is a root of $R(a)$ then one can obtain $\gcd(u(x, \alpha), v(x, \alpha))$ as the first subresultant $S_j(x, \alpha)$ among $S_0(x, \alpha), S_1(x, \alpha), \dots$ such that $\deg S_j(x, \alpha) = j$. If α is not a root of $R(a)$ then $\gcd(u(x, \alpha), v(x, \alpha)) = 1$.

Suppose that $u(x, a)$ and $v(x, a)$ have a nontrivial gcd in $K[a, x]$. Then, $S_0(x, a)$ is the zero polynomial. Let $S_t(x, a), t > 0$ be the first non-zero subresultant among $S_1(x, a), \dots, S_n(x, a)$. In accordance with the subresultant theory, $\deg_x S_t(x, a) = t$. One can set $R(a) = \text{lc}_x S_t(x, a)$ and carry out the actions above for a root α of $R(a)$. If $R(\alpha) \neq 0$ then $\gcd(u(x, \alpha), v(x, \alpha)) = S_t(x, \alpha)$.

One can notice that the complete subresultant chain (2) is redundant for this procedure: it is sufficient to consider the *regular subresultant chain*, i.e. the sub-chain of (2) which consists of the regular subresultants

only.

It is not necessary to build up an explicit form of the roots of $R(a)$. Let $r(a)$ be the squarefree part of $R(a)$, and consider a subresultant $S_j(x, a)$ and $h(a) = \gcd(r(a), \text{lc}_x S_j(x, a))$, $w(a) = r(a)/h(a)$. Obviously, the leading coefficient of $S_j(x, a)$ is non-zero for any root α of $w(a)$ and $\gcd(u(x, \alpha), v(x, \alpha)) = S_j(x, \alpha)$. Conversely, $\text{lc}_x S_j(x, a)$ is zero for any root of $h(a)$, so one can act as above, considering the gcd of $h(a)$ and the leading coefficient of $S_{j+1}(x, a)$, etc...

We assumed before that the value α of the parameter a satisfies some restrictions: $u_m(\alpha), v_n(\alpha)$ are not simultaneously zero, and $u(x, \alpha), v(x, \alpha)$ are non-zero polynomials in x . Now let α be free of the assumptions. First, one has to extract the contents (polynomials in a) of $u(x, a)$ $v(x, a)$ and consider the case where they are zero. If now the polynomials (3) are primitive and $b(a) = \gcd(u_m(a), v_n(a))$, then $r(a)$ can be decomposed in the product of two factors: $r_1(a) = \gcd(r(a), b(a))$, $r_2(a) = r(a)/r_1(a)$. For any root of $r_2(a)$ the values of $u_m(a)$ $v_n(a)$ are both non-zero, and the above algorithm can be applied. Otherwise, one has to consider $\gcd(u(x, a), v(x, a))$ under the condition $r_1(a) = 0$.

The algorithm can now be presented in the following manner: its input contains the polynomials (3) and in addition an algebraic condition $p(a) = 0$ (the trivial condition $0 = 0$ may occur). The algorithm returns a list of pairs of one of the forms

$$(d_1(a), G_1(x, a)), \dots, (d_k(a), G_k(x, a)), \quad (9)$$

$$(d_1(a), G_1(x, a)), \dots, (d_k(a), G_k(x, a)), \\ (0, G_{k+1}(x, a)), \quad (10)$$

where the $d_i(a)$'s are polynomials providing conditions $d_i(a) = 0$ on the values of the parameter a , and the $G_i(x, a)$'s are the gcd's corresponding to those. The polynomials $d_1(a), \dots, d_k(a)$ are relatively prime and squarefree; moreover, for any root α of $d_i(a)$ the leading coefficient of $G_i(x, a)$ is non-zero ($i = 1, \dots, k$). If the last pair in the list has the form $(0, G_{k+1}(x, a))$ then for all values α of a such that $d_1(a) \neq 0, \dots, d_k(a) \neq 0$ the identity $\gcd(u, v) = G_{k+1}(x, a)$ holds (this situation appears only when the input condition $p(a) = 0$ is trivial).

To compute the gcd of polynomials which depend on an undetermined parameter, it is sufficient to apply the above algorithm with initially the trivial condition. But the algorithm can be applied in other ways: for instance, to compute the gcd of polynomials with algebraic coefficients. Here the defining polynomial of the algebraic number plays the role of $p(a)$. The algorithm can be used also to implement the D5 method [Del et al.] of algebraic numbers handling; it also generalizes to the

case of multiple algebraic numbers. Moreover, the list (9)-(10) provides in a sense the solution of the system $u(x, a) = v(x, a) = 0$ of two algebraic equations with two variables. Indeed, one obtains the set of triangular systems $d_1(a) = G_1(x, a) = 0, \dots, d_k(a) = G_k(x, a) = 0$, and, maybe the equation $G_{k+1}(x, a) = 0$.

Other application of the algorithm is to obtain for given polynomial $f(x)$ its "shift-free double" – polynomial $g(x)$ such that all roots of $g(x)$ are also the roots of $f(x)$ and the difference of any two roots of $g(x)$ is not integer (rational). The algorithm can be applied to solve the following commonly occurring in the theory of differential equations problem: select such roots α of polynomial $f_1(x)$ and β of polynomial $f_2(x)$ as $\alpha + \beta$ is integer (rational). One can see also the other applications of the algorithm.

In some special cases the algorithm can be simplified. For instance, the integration of rational function [Laz&Rio90] calls for the computation of $\gcd(u(x), v(x) - au'(x))$, where a is a parameter, $u(x)$ is squarefree and $\deg v(x) < \deg u(x)$. Only the roots of the resultant

$$\text{Res}_x(u(x), v(x) - au'(x)). \quad (11)$$

provide a nontrivial gcd. By means of squarefree factorization one can present the resultant (11) as

$$\prod_{i=1}^n r_i(a)^{i}. \quad (12)$$

It is proved in [Laz&Rio90] that for any α such that $r_i(\alpha) = 0$: $\gcd(u(x), v(x) - \alpha u'(x)) = S_i(x, \alpha)$, where $S_i(x, a)$ is i^{th} subresultant of the polynomials $u(x), v(x) - au'(x)$. Thus as soon as the subresultant chain is computed and the factorization (12) is obtained the answer can be written as

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

This approach is not acceptable in the general case. For example, $\text{Res}_x(x^2 - a^2, x^2 + a^2) = 4a^4$, $a = 0$ is a root of the multiplicity 4; but the degree of the corresponding gcd is equal to 2.

4 The algorithm

Let us describe briefly the algorithm to compute the gcd of the polynomials $u(x, a)$ and $v(x, a)$, which depend on a parameter a . We assume that $p(a)$ is either the zero polynomial or a squarefree polynomial of positive degree. We assume also that a pair $(d(a), G(x, a))$ is included in the returned list iff $d(a) \notin K \setminus \{0\}$.

algorithm GCDpar(u, v, p)

begin

Step 1 : Preliminary computations

$u := u \bmod p$; $v := v \bmod p$;

if $u = 0$ **then** return (p, v) ; **fi**

if $v = 0$ **then** return (p, u) ; **fi**

Step 2 : Investigation of the contents

$C_u := \text{cont}_x u$; $C_v := \text{cont}_x v$;

$u := \text{pp}_x u$; $v := \text{pp}_x v$;

if $p(a)$ is the zero polynomial **then**

$C_u := \text{SQfree } C_u$;

$C_v := \text{SQfree } C_v$

else

$C_u := \gcd(C_u, p)$;

$C_v := \gcd(C_v, p)$

fi;

$C := \gcd(C_u, C_v)$;

$\text{result} := (C, 0), (C_u/C, v), (C_v/C, u)$;

$p := p/\text{lcm}(C_u, C_v)$;

% $p(a)$ correction
% (all the considered values of a are excluded)

Step 3 : Simple cases

if $\deg_x u = 0 \vee \deg_x v = 0$ **then** return $\text{result}, (p, 1)$; **fi**
% either $u(x, a)$ or $v(x, a)$ is in K

Step 4 : Investigation of the leading coefficients

$\delta := \gcd(\text{lc}_x u, \text{lc}_x v)$;

if $p(a)$ is the zero polynomial **then** $\delta := \text{SQfree } \delta$

else $\delta := \gcd(\delta, p)$

fi;

if $\deg_a \delta > 0$ **then**

$\text{result} := \text{GCDpar}(u, v, \delta), \text{result}$;

$p := p/\delta$ % $p(a)$ correction

fi;

Step 5 : Investigation of the subresultant chain

construct the regular subresultant chain of the

polynomials $u(x, a), v(x, a)$:

$S_{n-1}, S_{n-2}, \dots, S_0$ ($n = \deg_x v(x, a)$)

and remove from it all subresultants S_i with $i \geq n$;

if the resultant chain is empty **then** return $\text{result}, (p, v)$;

fi

% v divides u

Let S_i be the subresultant of lowest degree in x

in the resultant chain $r := \text{lc}_x S_i$;

if $p(a)$ is the zero polynomial **then**

$r := \text{SQfree } r$;

$r := r/\gcd(r, \text{lcm}(C_u, C_v, \delta))$

else $r := \gcd(r, p)$

fi;

% all the values of a considered above are excluded

Step 6 : Final efforts

$p := p/r$;

$\text{result} := \text{result}, (p, S_i)$;

for $i := t + 1$ **to** $n - 1$ **do**

```

    h := gcd(r, lcxSi(x, a));
    w := r/h;
    r := h;
    result := (w, Si), result
  od;

  result := (r, v), result;
  return result
end

```

5 Implementation

The algorithm above was implemented in REDUCE. The program in Standard LISP contains about 600 lines. The examples below were obtained on IBM-PC/AT 286 running at 12MHz.

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

References

- [Abr71] Abramov, S.A. *On the summation of rational functions*. CMMP ¹ 11, 1(1971), 1071-1075.
- [Abr75] Abramov, S.A. *The rational component of the solution of a first-order linear recurrence relation with a rational right-hand side*. CMMP 15, 4(1975), 1035-1039.
- [Abr89] Abramov, S.A. *Rational solutions of linear difference and differential equations with polynomial coefficients*. CMMP 29, 11(1989), 1611-1620.
- [Del et al.] Della Dora, J., Dicrescenzo, C., Duval, D. *About a new method for computing in algebraic number fields*. LNCS 204(1985), 289-290.
- [Gosp78] Gosper, R.W. *Decision procedure for indefinite hypergeometric summation*. Proc. Nat. Acad. Sci. USA 75/1(1978), 40-42.
- [Hab48] Habicht, W. *Eine Verallgemeinerung des Sturmschen Wurzelzählverfahrens*. Comment. math. Helvetici, 21(1948), 99-116.
- [Laz&Rio90] Lazard, D., Rioboo, R. *Integration of rational functions: rational computation of the logarithmic part*. J.Symb.Comp. 9(1990), 113-115.
- [Loos83] Loos, R. *Generalized Polynomial remainder sequences*. in *Computer Algebra. Symbolic and algebraic computation*. New York: Springer-Verlag(1983), 115-138.
- [Trag76] Trager, B.M. *Algebraic factoring and rational function integration*. Proc. 1976 Symp. on Symbolic and Algebraic Computation, 219-226.
- [Waer53] van der Waerden, B.L. *Modern algebra*, vol.1. New York: Frederick Ungar, 1953.
- [Abr71] Abramov, S.A. *On the summation of ra-*

¹ "USSR Comput. maths and math. phys.", transl. of "Zl Vychislit. matem. i mat. fiz.", Pergamon press