Theoretical Mathematics & Applications, vol.3, no.3, 2013, 13-21
ISSN: 1792-9687 (print), 1792-9709 (online)
Scienpress Ltd, 2013

Parametric euclidean algorithm

Ali Ayad[1], Ali Fares[2] and Youssef Ayyad[3]

Abstract

In this paper, we deal with the computation of generic greatest common divisors (gcd) of a finite set of parametric univariate polynomials. We will describe a parametric version of the well-known euclidean algorithm for computing gcds of univariate polynomials. We introduce the notion of parametric greatest common divisor in order to uniformly describe the gcd of univariate polynomials depending on parameters. The main algorithm of the paper decomposes the parameters space into a finite number of constructible sets such that a gcd of the parametric univariate polynomials is given uniformly in each constructible set.

Mathematics Subject Classification: 68W30; 11Y16; 11C08; 11A05
Keywords: Symbolic computations; greatest common divisor of polynomials; euclidean algorithm

[1] Équipe Algèbre et Combinatoire, EDST, Faculté des sciences - Section 1, Université libanaise, Hadath, Liban.

[2] Équipe Algèbre et Combinatoire, EDST, Faculté des sciences - Section 1, Université libanaise, Hadath, Liban.

[3] Faculty of Sciences and Arts, IUL, Khaldeh, Lebanon.

Article Info: *Received* : December 20, 2012. *Revised* : April 30, 2013
Published online : September 1, 2013

1 Introduction

Consider k polynomials $f_1, \ldots, f_k \in \mathbb{Q}[u_1, \ldots, u_t][X]$ with polynomial coefficients in the variables $u_1, \ldots, u_t$ over $\mathbb{Q}$. When we look at $u_1, \ldots, u_t$ as parameters, we consider $f_1, \ldots, f_k$ as parametric univariate polynomials. Parameters take values from the space $\mathcal{P} = \overline{\mathbb{Q}}^t$ which we call the parameters space, where $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$.

We begin the paper by introducing the problem with some notations and we show the result of the main algorithm. For a polynomial $g \in \mathbb{Q}(u_1, \ldots, u_t)[X]$ and a value $a = (a_1, \ldots, a_t) \in \mathcal{P}$, we denote by G (in capital letter if there is no confusion on a) the polynomial of $\overline{\mathbb{Q}}[X]$ obtained by specialization of u by a in the coefficients of g if their denominators do not vanish at a, i.e., $G = g(a_1, \ldots, a_t, X) \in \overline{\mathbb{Q}}[X]$.

For $k = 2$, if we look at f_1 and f_2 as univariate polynomials with coefficients in the fraction field $\mathbb{Q}(u_1, \ldots, u_t)$ of the ring $\mathbb{Q}[u_1, \ldots, u_t]$ and if we compute the sequence

$$\{r_0, r_1, \ldots, r_s, r_{s+1} = 0\} \subset \mathbb{Q}(u_1, \ldots, u_t)[X]$$

of remainders by successive euclidean divisions of the polynomials $r_0 = f_1$ and $r_1 = f_2$ in $\mathbb{Q}(u_1, \ldots, u_t)[X]$, i.e., for any $2 \leq i \leq s+1$, r_i is the remainder of the euclidean division of r_{i-2} by r_{i-1} in $\mathbb{Q}(u_1, \ldots, u_t)[X]$. This sequence does not give the gcd of F_1 and F_2 in $\overline{\mathbb{Q}}[X]$ for all specializations $a \in \mathcal{P}$ of the parameters for both following reasons:

Problem 1: Zeros of the denominators of the coefficients of $r_0, r_1, \ldots, r_s$ are not covered. This means that if a is a such zero, the sequence does not calculate a gcd of F_1 and F_2.

Problem 2: Even for a value $a \in \mathcal{P}$ which does not vanish any denominator of the coefficients of $r_2, \ldots, r_s$, the polynomial $R_s \in \overline{\mathbb{Q}}[X]$ is not necessarily a gcd of F_1 and F_2. However r_s is a gcd of f_1 and f_2 in $\mathbb{Q}(u_1, \ldots, u_t)[X]$.

Example 1.1. Consider the two parametric univariate polynomials

$$r_0 = f_1 = uX^2 + X - 1 \quad \text{and} \quad r_1 = f_2 = vX + 1,$$

where u and v are parameters. By the successive euclidean division of r_0 by r_1 in $\mathbb{Q}(u, v)[X]$, we get $r_2 = -\frac{1}{v}(1 - \frac{u}{v}) - 1$ and $r_3 = 0$. Then it is obvious that for arbitrary values of u and $v = 0$, r_2 is not defined. Moreover, for $(u, v) = (2, 1)$, then $R_2 = 0$ and $F_2 = X + 1$ is a gcd of $F_1 = 2X^2 + X - 1$ and F_2, i.e., F_2 divides F_1.

The euclidean algorithm is known to be the oldest algorithm for computing the greatest common divisor (gcd) of two univariate polynomials [9, 6, 3]. There are different versions of this algorithm for computing gcd of several polynomials in one or several variables. The extended euclidean algorithm expresses the gcd as a linear combination of the input polynomials. Different algorithms deal with the computation of gcds depending on different models for representing polynomials: sparse representation (only non-zero monomials are represented with their coefficients) [8, 10], dense representation (all monomials up to a certain degree are represented with their coefficients, including those which are zeroes) [3, 4, 7] and straight-line programs (polynomials are given by their evaluations) [5]. In [1], there is an algorithm for computing gcds of two univariate polynomials with one parameter.

In order to compute the gcd of the polynomials $F_1, \ldots, F_k \in \overline{\mathbb{Q}}[X]$ uniformly in the values a of the parameters in $\mathcal{P}$, we introduce the notion of parametric greatest common divisors:

Definition 1.2. *A parametric greatest common divisor (pgcd) of the set $\{f_1, \ldots, f_k\}$ is a couple (W, g) where W is a constructible subset of $\mathcal{P}$ and $g \in \mathbb{Q}[u_1, \ldots, u_t][X]$ is a parametric univariate polynomial such that for any $a \in \mathcal{P}$, the polynomial G is a gcd of the polynomials $F_1, \ldots, F_k$ in $\overline{\mathbb{Q}}[X]$.*

The main algorithm of the paper is given in the following theorem.

Theorem 1.3. *For a set $\{f_1, \ldots, f_k\} \subset \mathbb{Q}[u_1, \ldots, u_t][X]$ of parametric univariate polynomials, the algorithm computes a finite number of pgcd (W_1, g_1), $\ldots, (W_N, g_N)$ such that the sets $W_1, \ldots, W_N$ form a partition of the parameters space $\mathcal{P}$.*

2 Parametric gcds

To avoid the problem 1, we compute a sequence of pseudo-remainders of successive euclidean divisions:

Definition 2.1. *Let $f_1, f_2 \in \mathbb{Q}[u_1, \ldots, u_t][X]$ be two parametric univariate polynomials. Let $m_1 = \deg_X(f_1)$ and $m_2 = \deg_X(f_2)$.*

- *The pseudo-division of f_1 by f_2 is defined to be the euclidean division of $lc(f_2)^{m_1-m_2+1} f_1$ by f_2 in $\mathbb{Q}(u_1, \ldots, u_t)[X]$, where*

  $$0 \neq lc(f_2) \in \mathbb{Q}[u_1, \ldots, u_t]$$

  is the leading coefficient of f_2. Then there exist unique polynomials $q, r \in \mathbb{Q}[u_1, \ldots, u_t][X]$ such that

  $$lc(f_2)^{m_1-m_2+1} f_1 = q f_2 + r \quad \text{and} \quad \deg_X(r) < \deg_X(f_2),$$

  q is called the pseudo-quotient and r is the pseudo-remainder (denoted by $Prem(f_1, f_2)$) of the pseudo-division of f_1 by f_2.

- *The sequence of pseudo-remainders of successive pseudo-divisions applicated to $\tilde{r}_0 = f_1$ and $\tilde{r}_1 = f_2$ is the sequence*

  $$\{\tilde{r}_0, \tilde{r}_1, \ldots, \tilde{r}_s, \tilde{r}_{s+1} = 0\}$$

  where for any $2 \leq i \leq s+1$, $\tilde{r}_i$ is the pseudo-remainder of the pseudo-division of $\tilde{r}_{i-2}$ by $\tilde{r}_{i-1}$.

The following lemma proves that the sequence of pseudo-remainders also computes gcds.

Proposition 2.2. *Let $f_1, f_2 \in \mathbb{Q}[u_1, \ldots, u_t][X]$ be two parametric univariate polynomials. Let $\{\tilde{r}_0, \tilde{r}_1, \ldots, \tilde{r}_s, \tilde{r}_{s+1} = 0\}$ be the sequence of pseudo-remainders of successive pseudo-divisions of $\tilde{r}_0 = f_1$ by $\tilde{r}_1 = f_2$. Then $\tilde{r}_s$ is a gcd of f_1 and f_2 in $\mathbb{Q}[u_1, \ldots, u_t][X]$ and for any $a \in \mathcal{P}$ which does not vanish any leading coefficient of the polynomials in the sequence, the polynomial $\tilde{R}_s \in \overline{\mathbb{Q}}[X]$ is a gcd of F_1 and F_2.*

Proof. It is deduced from Theorem 6.62 of [9]. □

Example 2.3. Consider the two parametric univariate polynomials

$$\tilde{r}_0 = f_1 = X^3 + uX^2 + vX + 1 \quad \text{and} \quad \tilde{r}_1 = f_2 = X^2 - uX - 1.$$

By the successive pseudo-division of $\tilde{r}_0$ by $\tilde{r}_1$, we get

$$\begin{cases} \tilde{r}_2 = (2u^2 + v + 1)X + (2u + 1), \\ \tilde{r}_3 = 2u^3 - 2u^2v + 2u^2 - v^2 + uv + 5u - 2v, \\ \tilde{r}_4 = 0. \end{cases}$$

By proposition 2.2, $\tilde{r}_3$ is a gcd of f_1 and f_2 in $\mathbb{Q}[u, v][X]$. But for $(u, v) = (0, 0)$, then $\tilde{R}_3 = 0$ and $\tilde{R}_2 = X + 1$ is a gcd of $F_1 = X^3 + 1$ and $F_2 = X^2 - 1$.

The problem 2 can be avoided by truncations of polynomials.

Definition 2.4. *Let $g = g_m X^m + \cdots + g_0 \in \mathbb{Q}[u_1, \ldots, u_t][X]$ be a non-zero parametric univariate polynomial of degree m w.r.t. X.*

- *For any $0 \le i \le m$, the truncation of g at i, denoted by $Tru_i(g)$, is the polynomial*

$$Tru_i(g) = g_i X^i + \cdots + g_0 \in \mathbb{Q}[u_1, \ldots, u_t][X].$$

- *The set of truncations of g, denoted by $Tru\,(g)$, is the finite subset of $\mathbb{Q}[u_1, \ldots, u_t][X]$ defined recursively by:*

$$Tru\,(g) = \begin{cases} \{g\} & \text{if} \quad g_m = lc(g) \in \mathbb{Q}, \\ \{g\} \cup Tru\,(Tru_{m-1}(g)) & \text{else.} \end{cases}$$

If $g_i \notin \mathbb{Q}$ for all $0 \le i \le m$, then we add 0 to $Tru\,(g)$.

Example 2.5. Consider the parametric univariate polynomials:

$$g = uX^4 + uvX^3 + 3X^2 - u^4X + 1 \quad \text{and} \quad h = u^3X^2 + uv^2X + v^2 + 1.$$

Then

$$\begin{cases} Tru(g) = \{g, Tru_3(g), Tru_2(g)\}, \text{ where} \\ Tru_3(g) = uvX^3 + 3X^2 - u^4X + 1, \\ Tru_2(g) = 3X^2 - u^4X + 1, \end{cases}$$

and

$$\begin{cases} Tru(h) = \{h, Tru_1(h), Tru_0(h), 0\}, \text{ where} \\ Tru_1(h) = uv^2X + v^2 + 1, \\ Tru_0(h) = v^2 + 1. \end{cases}$$

Definition 2.6. *[2]*
Let $f_1, f_2 \in \mathbb{Q}[u_1, \ldots, u_t][X]$ be two parametric univariate polynomials.

- *For each nonzero polynomial $\tilde{r}_0 \in Tru\,(f_1)$, we associate a tree of pseudo-remainder sequences of $\tilde{r}_0$ by f_2, denoted by $TPrems(\tilde{r}_0, f_2)$. The root of this tree contains $\tilde{r}_0$. The sons of $\tilde{r}_0$ contain the elements of $Tru(f_2)$. Each node N contains a polynomial $Pol(N) \in \mathbb{Q}[u_1, \ldots, u_t][X]$. A node N is a leaf of the tree if $Pol(N) = 0$. If N is not a leaf, the sons of N contain the elements of the set of truncations of $Prem(Pol(p(N)), Pol(N))$ where $p(N)$ is the parent of N.*

- *The set of all the trees associated to the nonzero elements of $Tru\,(f_1)$ is called the forest of pseudo-remainder sequences of f_1 by f_2, it is denoted by $T(f_1, f_2)$.*

Remark 2.7. *Each tree $TPrems(\tilde{r}_0, f_2)$ in the definition 2.6 terminates since the transition from a level to another one in the tree is performed by a pseudo-division then the degrees of the polynomials w.r.t. X decrease. Thus we have a finite number of leaves in the tree.*

Example 2.8. Return to example 2.3 and take the same parametric univariate polynomials f_1 and f_2. We have $Tru(f_1) = \{f_1\}$ and $Tru(f_2) = \{f_2\}$, then the forest $T(f_1, f_2)$ contains only one tree which is $TPrems(\tilde{r}_0, f_2)$ with root $\tilde{r}_0 = f_1$, this root has $\tilde{r}_1 = f_2$ as its unique son. But $Prem(\tilde{r}_0, \tilde{r}_1) = (2u^2 + v + 1)X + (2u + 1)$, then the sons of $\tilde{r}_1$ are the elements of

$$Tru\big(Prem(\tilde{r}_0, \tilde{r}_1)\big) = \Big\{(2u^2 + v + 1)X + (2u + 1),\ (2u + 1), 0\Big\}.$$

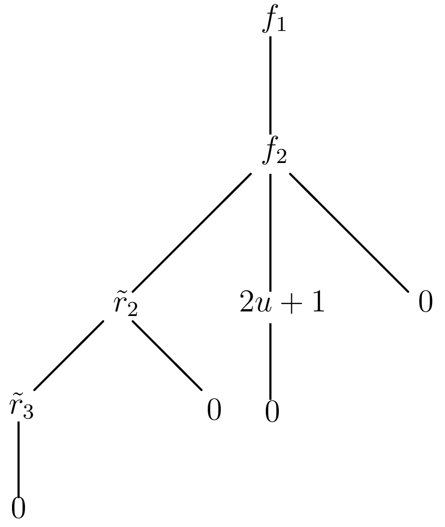
- If $\tilde{r}_2 = (2u^2 + v + 1)X + (2u + 1)$ is a son of $\tilde{r}_1$ then

$$Prem(\tilde{r}_1, \tilde{r}_2) = 2u^3 - 2u^2v + 2u^2 - v^2 + uv + 5u - 2v.$$

  Hence the sons of $\tilde{r}_2$ are $\tilde{r}_3 = 2u^3 - 2u^2v + 2u^2 - v^2 + uv + 5u - 2v$ and 0.

- If $\tilde{r}_2 = (2u + 1)$ is a son of $\tilde{r}_1$ then $Prem(\tilde{r}_1, \tilde{r}_2) = 0$.

The forest $T(f_1, f_2)$ is described in the following graph:



Definition 2.9. *Let $f_1, f_2 \in \mathbb{Q}[u_1, \ldots, u_t][X]$ be two parametric univariate polynomials. Let $\tilde{r}_0 \in Tru\,(f_1) \setminus \{0\}$ and $TPrems(\tilde{r}_0, f_2)$ the tree with root contains $\tilde{r}_0$. For each leaf L of $TPrems(\tilde{r}_0, f_2)$, we consider the unique path*

$$P_L = \{\tilde{r}_0, \tilde{r}_1, \ldots, \tilde{r}_s, \tilde{r}_{s+1} = Pol(L) = 0\}$$

from the root $\tilde{r}_0$ to L where $\tilde{r}_1 \in Tru\,(f_2)$ is a son of $\tilde{r}_0$ and we associate to L a constructible subset W_L of $\mathcal{P}$ defined by the following quantifier-free formula:

$$\bigwedge_{2 \le i \le s+1} \Big[\deg_X(\tilde{r}_i) = \deg_X\big(Prem(\tilde{r}_{i-2}, \tilde{r}_{i-1})\big) \Big].$$

Corollary 2.10. *Let $f_1, f_2 \in \mathbb{Q}[u_1, \ldots, u_t][X]$ be two parametric univariate polynomials. The constructible sets W_L where L are the leaves of the forest $T(f_1, f_2)$ form a partition of $\mathcal{P}$. Moreover, for every leaf L of $T(f_1, f_2)$, the path*

$$P_L = \{\tilde{r}_0, \tilde{r}_1, \ldots, \tilde{r}_s, \tilde{r}_{s+1} = Pol(L) = 0\}$$

is a parametric pseudo-remainder sequence of f_1 and f_2, i.e., for any $a \in W_L$, the set $\{\tilde{R}_0, \tilde{R}_1, \ldots, \tilde{R}_s, \tilde{R}_{s+1} = Pol(L) = 0\} \subset \overline{\mathbb{Q}}[X]$ is the sequence of pseudo-remainders of F_1 and F_2. In particular, $0 \neq \tilde{R}_s \in \overline{\mathbb{Q}}[X]$ is a gcd of F_1 and F_2, i.e., $(W_L, \tilde{r}_s)$ is a pgcd of f_1 and f_2.

Proof. It is deduced from proposition 2.2. □

Example 2.11. Return to Example 2.8. The forest $T(f_1, f_2)$ contains 4 leaves, then we get 4 pgcds $(W_1, g_1), (W_2, g_2), (W_3, g_3), (W_4, g_4)$ of f_1 and f_2 as follows:

$$\mathcal{P} = W_1 \cup W_2 \cup W_3 \cup W_4,$$

$$\begin{cases} W_1 = \{2u^2 + v + 1 \neq 0, g_1 \neq 0\}, \\ g_1 = 2u^3 - 2u^2v + 2u^2 - v^2 + uv + 5u - 2v, \end{cases}$$

$$\begin{cases} W_2 = \{2u^2 + v + 1 \neq 0, g_1 = 0\}, \\ g_2 = (2u^2 + v + 1)X + 2u + 1, \end{cases}$$

$$\begin{cases} W_3 = \{2u^2 + v + 1 = 0, 2u + 1 \neq 0\}, \\ g_3 = 2u + 1, \end{cases}$$

$$\begin{cases} W_4 = \{2u^2 + v + 1 = 0, 2u + 1 = 0\}, \\ g_4 = f_2. \end{cases}$$

Corollary 2.12. *Let $f_1, \ldots, f_k \in \mathbb{Q}[u_1, \ldots, u_t][X]$ be k parametric univariate polynomials where $k \geq 3$. One can compute a finite number of pgcd $(\mathcal{V}, g)$ of the set $\{f_1, \ldots, f_k\}$ such that the constructible sets $\mathcal{V}$ form a partition of $\mathcal{P}$ and $g \in \mathbb{Q}[u_1, \ldots, u_t][X]$.*

Proof. The proof is done by induction on k:

- The case $k = 2$ is exactly the corollary 2.10.

- Suppose that at the $(k-1)$-th step of the induction, we have a partition of $\mathcal{P}$ into a finite number of pgcd (V, h) of the set $\{f_1, \ldots, f_{k-1}\}$ where $h \in \mathbb{Q}[u_1, \ldots, u_t][X]$. For each pgcd (V, h), we compute the forest $T(h, f_k)$ as in the corollary 2.10 and for each leaf L of this forest, we take the following constructible set $\mathcal{V}_L = V \cap W_L$ where W_L is the constructible set associated to L in $T(h, f_k)$ (see Definition 2.9). The sets $\mathcal{V}_L$ where L are the leaves of $T(h, f_k)$ for all pgcd (V, h) of $\{f_1, \ldots, f_{k-1}\}$ form a partition of $\mathcal{P}$. Moreover, for each leaf L in $T(h, f_k)$, the couple $(\mathcal{V}_L, g)$ is a pgcd of the set $\{f_1, \ldots, f_k\}$ where $g = Pol(p(L)) \in \mathbb{Q}[u_1, \ldots, u_t][X]$. □

References

[1] S. A. Abramov and K. Yu. Kvashenko, On the greatest common divisor of polynomials which depend on a parameter, *Proceedings of the 1993 international symposium on Symbolic and algebraic computation*, (1993), 152 - 156.

[2] S. Basu, R. Pollack and M-F. Roy, *Algorithms in real algebraic geometry*, Springer, New York, 2003.

[3] W. S. Brown, On Euclid's algorithm and the computation of polynomial greatest common divisors, *J. ACM 18*, **4**, (1971), 478 - 504.

[4] G. E. Collins, Subresultants and reduced polynomial remainder sequences, *J. ACM*, **14**, (1967), 128 - 142.

[5] E. Kaltofen, Greatest common divisors of polynomials given by straight-line programs, *Journal of the ACM (JACM)*, **35** (1), (1988), 231 - 264.

[6] D.E. Knuth, *The Art of Computer Programming, Vol. 2: Seminumerical Algorithms*, Addison-Wesley, Reading, Mass., 3rd edition, 1998.

[7] J. Moss, and D.Y.Y. YUN, The EZ-GCD algorithm, *Proceedings of the 1973 ACM National Conference*, ACM, New York, (1973), 159 - 166.

[8] D. A. Plaisted, Sparse complex polynomials and polynomial reducibility. *J. Comput. Syst. Sci*, **14**, (1977), 210 - 221.

[9] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, Cambridge University Press, 1999.

[10] R. E. Zippel, Probabilistic algorithms for sparse polynomials, in Proceedings of the EUROSAM'79, *Lecture Notes on Computer Science*, Springer-Verlag, New York, **72**, (1979), 216 - 226.