International Journal of Algebra, Vol. 4, 2010, no. 4, 173 - 188

Complexity of Algorithms for Computing Greatest Common Divisors of Parametric Univariate Polynomials

Ali Ayad

CEA LIST, Software Safety Laboratory
Point Courrier 94, Gif-sur-Yvette, F-91191 France
ayadali99100@hotmail.com
and
IRMAR, Campus de Beaulieu
Université Rennes 1, 35042, Rennes, France

Abstract

This paper presents a comparison between the complexity bounds of different algorithms for computing greatest common divisor of a finite set of parametric univariate polynomials. Each algorithm decomposes the parameters space into a finite number of constructible sets such that a greatest common divisor of the parametric univariate polynomials is given uniformly in each constructible set. The first one is a parametrization of the well-known euclidean algorithm, this is the worst case study: its complexity is exponential in the number k of the polynomials and the upper bound d on the degrees of the polynomials. The second algorithm comes from a paper of Grigoryev in 1989. The third algorithm is based on a parametrization of the well-known Gaussian elimination procedure for solving linear systems. The complexity of these two last algorithms is polynomial in k and d and exponential in the number r of the parameters. These algorithms are used to solve parametric univariate polynomial systems and to compute the multiplicities of roots of parametric univariate polynomials.

Mathematics Subject Classification: 11Y16, 11A05, 11C08, 11C20, 15A06

Keywords: Symbolic computations, Complexity analysis, Greatest common divisor of polynomials, Parametric Euclidean algorithm, linear algebraic systems, Parametric Gaussian elimination

1 Introduction

The euclidean algorithm is known to be the oldest algorithm for computing the greatest common divisor (GCD) of two univariate polynomials [15, 9, 3]. There are different versions of this algorithm for computing GCD of several polynomials in one or several variables. The extended euclidean GCD 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) [12, 16], dense representation (all monomials up to a certain degree are represented with their coefficients, including those which are zeroes) [3, 5, 11] and straight-line programs (polynomials are given by their evaluations) [8].

In this paper, we are interested in the complexity study of the computation of GCDs of parametric univariate polynomials given by dense representations. This will be uniform in the values of the parameters. In [1], there is an algorithm for computing GCDs of two univariate polynomials with one parameter. In this algorithm, GCDs are computed by sub-resultants without a complexity study. This approach is similar to that of Section 2.

We begin the paper by introducing the problem with some notations and we show the result of the main algorithms:

Let $\{f_1, \ldots, f_k\} \subset \mathbb{Q}[u_1, \ldots, u_r][X]$ be a set of parametric univariate polynomials. Their coefficients are polynomial functions on the parameters $u = (u_1, \ldots, u_r)$ with coefficients in the field $\mathbb{Q}$ of rational numbers. Parameters take values from the space $\mathcal{P} = \overline{\mathbb{Q}}^r$ which we call the parameters space, where $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$. In the sequel, let us adopt the following notation: for a polynomial $g \in \mathbb{Q}(u_1, \ldots, u_r)[X]$ and a value $a = (a_1, \ldots, a_r) \in \mathcal{P}$ of the parameters, we denote by $g^{(a)}$ the polynomial of $\overline{\mathbb{Q}}[X]$ which is obtained by specialization of u by a in the coefficients of g if their denominators do not vanish on a, i.e., $g^{(a)} = g(a_1, \ldots, a_r, X)$.

To compute the GCD of the polynomials $f_1^{(a)}, \ldots, f_k^{(a)} \in \overline{\mathbb{Q}}[X]$ uniformly in the values a of the parameters in $\mathcal{P}$, we introduce the notion of parametric greatest common divisors:

Definition 1.1 *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 $g \in \mathbb{Q}(u_1, \ldots, u_r)[X]$ is a parametric univariate polynomial with coefficients being rational functions on the parameters which satisfy the following properties:*

- *All coefficients of g in $\mathbb{Q}(u_1, \ldots, u_r)$ are well-defined on W.*
- *For any $a \in \mathcal{P}$, $g^{(a)}$ is a GCD of the polynomials $f_1^{(a)}, \ldots, f_k^{(a)}$ in $\overline{\mathbb{Q}}[X]$.*

The main goal of the algorithms of the paper is to cover all values of the parameters as follows:

Theorem 1.2 *For a set* $\{f_1, \ldots, f_k\} \subset \mathbb{Q}[u_1, \ldots, u_r][X]$ *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* $\mathcal{P}$.

These algorithms differ by the number of elements in the partition, the degrees of the PGCD, the equations and the inequations of the constructible sets w.r.t. u and their complexity bounds. We suppose that $f_1, \ldots, f_k$ are coded by dense representations. For the complexity analysis aims, we suppose that their degrees are bounded by an integer d (resp. δ) w.r.t. X (resp. u) and their binary lengths (i.e., the maximum of the binary lengths of their coefficients in $\mathbb{Q}$) are less than an integer M. Then we can write each f_i $(1 \leq i \leq k)$ in the form:

$$f_i = \sum_{0 \leq j \leq d} f_{ij} X^j \quad \text{where } f_{ij} \in \mathbb{Q}[u_1, \ldots, u_r],\ \deg(f_{ij}) \leq \delta.$$

and we consider the subset

$$\mathcal{U} = \mathcal{P} \setminus \{f_{ij} = 0, 1 \leq i \leq k, 0 \leq j \leq d\}.$$

The degree of a rational function $\frac{p}{q} \in \mathbb{Q}(u_1, \ldots, u_r)$ w.r.t. u is the maximum of those of p and q. Its binary length is the maximum of those of the coefficients of p and q in $\mathbb{Q}$.

Example 1.3 *For the two parametric univariate polynomials*

$$f_1 = X^3 + uX^2 + vX + 1 \quad \textit{and} \quad f_2 = X^2 - uX - 1,$$

the algorithm computes 4 *PGCD as follows:*

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

- $W_1 = \{2u^2+v+1 \neq 0, S \neq 0\}$, $g_1 = S = 2u^2(u-v+1)+uv+v^2+5u+2v$.
- $W_2 = \{2u^2 + v + 1 \neq 0, S = 0\}$, $g_2 = (2u^2 + v + 1)X + 2u + 1$.
- $W_3 = \{2u^2 + v + 1 = 0, 2u + 1 \neq 0\}$, $g_3 = 2u + 1$.
- $W_4 = \{2u^2 + v + 1 = 0, 2u + 1 = 0\}$, $g_4 = f_2$.

The paper is organized as follows: Section 2 describes a parametrization of the euclidean algorithm with a complete complexity analysis. Section 3 outlines an algorithm from a paper of Grigoryev in 1989 [6]. A parametrization of the well-known Gaussian elimination algorithm for solving parametric linear systems is given in Section 4. Based on this parametrization, we get a new algorithm for computing parametric GCDs. In this algorithm, PGCDs are expressed as linear combinations of the input polynomials. Applications of these algorithms include the resolution of parametric univariate algebraic systems (Section 5.1) and the computation of the multisets of the multiplicities of parametric univariate polynomials (Section 5.2).

2 Parametrization of the euclidean algorithm

First we consider the case of two parametric univariate polynomials, and we compute the sequence

$$(R_0, R_1, \ldots, R_s, R_{s+1} = 0) \subset \mathbb{Q}(u_1, \ldots, u_r)[X]$$

of remainders by successive euclidean divisions on the polynomials $R_0 = f_1$ and $R_1 = f_2$ in $\mathbb{Q}(u_1, \ldots, u_r)[X]$, 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}. This sequence does not give the GCD of $f_1^{(a)}, f_2^{(a)} \in \overline{\mathbb{Q}}[X]$ for all specializations $a \in \mathcal{U}$ of the parameters for both following reasons:

1. Zeros of the denominators of the coefficients of $R_0, R_1, \ldots, R_s$ are not covered.

2. Even for a value $a \in \mathcal{U}$ which does not vanish any denominator of the coefficients of $R_2, \ldots, R_s$, the polynomial $R_s^{(a)} \in \overline{\mathbb{Q}}[X]$ is not necessarily a GCD of $f_1^{(a)}$ and $f_2^{(a)}$ even if it is nonzero. However R_s is a GCD of f_1 and f_2 in $\mathbb{Q}(u_1, \ldots, u_r)[X]$.

The first problem can be avoided by the computation of a sequence of pseudo-remainders of successive euclidean divisions:

Definition 2.1 *Let $g, h \in \mathbb{Q}[u_1, \ldots, u_r][X]$ be two parametric univariate polynomials.*

- *The pseudo-division of g by h is the euclidean division of $lc(h)^{\deg(g)-\deg(h)+1}g$ by h in $\mathbb{Q}(u_1, \ldots, u_r)[X]$ where $0 \neq lc(h) \in \mathbb{Q}[u_1, \ldots, u_r]$ is the leading coefficient of h. Then there exist unique polynomials $Q, R \in \mathbb{Q}[u_1, \ldots, u_r][X]$ such that*

$$lc(h)^{\deg_X(g)-\deg_X(h)+1}g = Qh + R \quad \textit{and} \quad \deg_X(R) < \deg_X(h)$$

Q is called the pseudo-quotient and R is the pseudo-remainder (denoted by $Prem(g,h)$) of the pseudo-division of g by h.

- *The sequence of pseudo-remainders of successive pseudo-divisions applicated to $\tilde{R}_0 = g$ and $\tilde{R}_1 = h$ 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. This Lemma gives also bounds on the degrees and binary lengths of the polynomials of the sequence:

Lemma 2.2 *Let $g, h \in \mathbb{Q}[u_1, \ldots, u_r][X]$ be two parametric univariate polynomials of degrees $\leq d$ (resp. δ) w.r.t. X (resp. u) and binary lengths less than M. 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 $\tilde{R}_0 = g$ by $\tilde{R}_1 = h$. Then we have the following properties:*

- *$\tilde{R}_s$ is a GCD of g and h in $\mathbb{Q}[u_1, \ldots, u_r][X]$. For any $a \in \mathcal{U}$ which does not vanish any leading coefficient of the polynomials in the sequence, the polynomial $\tilde{R}_s^{(a)} \in \overline{\mathbb{Q}}[X]$ is a GCD of $g^{(a)}$ and $h^{(a)}$.*

- *For any $0 \leq i \leq s$, the degree of $\tilde{R}_i$ w.r.t. u is bounded by $O(d^2\delta)$ and its binary length is less than $O(Md^2 \log_2 d)$.*

The computation of this sequence is done by $O(\delta^2 d^9)$ operations in $\mathbb{Q}$ and $O(\delta^2 M^2 d^{13} \log_2^2 d)$ binary operations.

Proof. All these bounds are deduced from Theorems 6.54, 6.62 and Exercice 6.54 of [15]. □

The second problem can be avoided by truncations of polynomials:

Definition 2.3 *Let $g = g_m X^m + \cdots + g_0 \in \mathbb{Q}[u_1, \ldots, u_r][X]$ be a non-zero parametric univariate polynomial of degree m w.r.t. X.*

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

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

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

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

Definition 2.4 *[2] For each polynomial $R_0 \in Tru\,(f_1)$, we associate a tree of pseudo-remainder sequences of R_0 by f_2, denoted by $TRems(R_0, f_2)$. The root of this tree contains R_0. The sons of R_0 contain the elements of the set of truncations of f_2. Each node N contains a polynomial $Pol(N) \in \mathbb{Q}[u_1,\ldots,u_r][X]$. 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 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 2.5 *Each tree $TRems(R_0, f_2)$ in Definition 2.4 terminates since the transition from one level to another in the tree is performed by a pseudo-division then the degrees of polynomials w.r.t. X decrease. Thus we have a finite number of leaves in the tree.*

Definition 2.6 *Let $R_0 \in Tru\,(f_1)$ and $TRems(R_0, f_2)$ the tree with root contains R_0. For each leaf L of $TRems(R_0, f_2)$, we consider the unique path $C_L = \{R_0, R_1, \ldots, R_s, R_{s+1} = Pol(L) = 0\}$ from the root R_0 to L where $R_1 \in Tru\,(f_2)$ is a son of R_0 and we associate to L a constructible subset W_L of $\mathcal{P}$ defined by the following quantifier-free formula:*

$$\bigwedge_{2 \le i \le s+1} \deg_X(R_i) = \deg_X\,(Prem(R_{i-2}, R_{i-1})).$$

Theorem 2.7 *The constructible sets $\mathcal{W}_L = W_L \cap \mathcal{U}$ where L are the leaves of the forest $T(f_1, f_2)$ form a partition of $\mathcal{U}$. This partition satisfies the following properties:*

- *The number of leaves L of $T(f_1, f_2)$ is bounded by $(d+2)\,d!$ where $d!$ is the factorial of d.*

- *The degrees of equations and inequations which define each $\mathcal{W}_L$ w.r.t. u are bounded by $O(d^2\delta)$. Their binary lengths are less than $O(Md^2 \log_2 d)$.*

- *For any leaf L of $T(f_1, f_2)$, the path $C_L = \{R_0, R_1, \ldots, R_s, R_{s+1} = Pol(L) = 0\}$ is a parametric pseudo-remainder sequence of f_1 by f_2, i.e., for any $a \in W_L$, the sequence $(R_0^{(a)}, R_1^{(a)}, \ldots, R_s^{(a)}, R_{s+1} = Pol(L) = 0\} \subset \overline{\mathbb{Q}}[X]$ is the sequence of pseudo-remainders of $f_1^{(a)}$ by $f_2^{(a)}$. In particular, $0 \neq R_s^{(a)} \in \overline{\mathbb{Q}}[X]$ is a GCD of $f_1^{(a)}$ and $f_2^{(a)}$, i.e., (W_L, R_s) is a*

PGCD of f_1 and f_2. The degree of R_s w.r.t. u is bounded by $O(d^2\delta)$ and its binary length is less than $O(Md^2 \log_2 d)$.

The construction of the forest $T(f_1, f_2)$ is done by $\delta^2 d^{O(d)}$ operations in $\mathbb{Q}$ and $(M\delta)^2 d^{O(d)}$ binary operations.

Proof. The number of leaves L of $T(f_1, f_2)$ is proven by Remark 2.5 and the fact that for a polynomial $g \in \mathbb{Q}[u_1, \ldots, u_r][X]$ of degree m w.r.t. X, the number of elements of $Tru\,(g)$ is less than $(m+2)$. All other items are deduced from Lemma 2.2. □

In the general case, i.e., when $k \geq 2$, we get the following theorem:

Theorem 2.8 *One can compute at most $d^{(k-1)d}$ PGCD (W, g) of the set $\{f_1, \ldots, f_k\}$ such that the constructible sets W form a partition of $\mathcal{U}$ and $g \in \mathbb{Q}[u_1, \ldots, u_r][X]$. In addition, we have the following bounds:*

- *The degrees of g and the equations and inequations which define W w.r.t. u are bounded by $O(d^{(2k-2)}\delta)$. Their binary lengths are less than $O(Md^{(2k-2)} \log_2^{k-1} d)$.*

The computation of this partition is done by $\delta^2 d^{O(kd)}$ operations in $\mathbb{Q}$ and $(M\delta)^2 d^{O(kd)}$ binary operations.

Proof. The proof is done by induction on k:

- The case $k = 2$ is exactly Theorem 2.7.

- Suppose that at the $(k-1)$-th step of the induction, we have a partition of $\mathcal{U}$ into at most $d^{(k-2)d}$ PGCD (V, h) of the set $\{f_1, \ldots, f_{k-1}\}$ where the constructible sets V form a partition of $\mathcal{U}$ and $h \in \mathbb{Q}[u_1, \ldots, u_r][X]$. For each PGCD (V, h), we compute the forest $T(h, f_k)$ as in Theorem 2.7 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 2.6). 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 $\mathcal{U}$. Morever, 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 $g = Pol(p(L)) \in \mathbb{Q}[u_1, \ldots, u_r][X]$. The bounds on the degrees, the binary lengths and the total complexity are deduced from Theorem 2.7. □

3 Grigoryev algorithm

In 1989, Grigryev [6] describes an algorithm for computing PGCDs of parametric univariate polynomials based on the resolution of zero-dimensional polynomial systems by the elimination theory:

Theorem 3.1 *Let $\{f_1, \ldots, f_k\} \subset \mathbb{Q}[u_1, \ldots, u_r][X]$ be a set of parametric univariate polynomials as in the introduction. There is an algorithm which decomposes the set $\mathcal{U}$ into at most $k(\delta + d)^{O(r)}$ PGCD such that for each PGCD (W, g) among them, where W is a constructible subset of $\mathcal{U}$ and $g \in \mathbb{Q}[u_1, \ldots, u_r][X]$, the following bounds are satisfied:*

- *The degrees of the equations and inequations which define W w.r.t. u are bounded by $(\delta + d)^{O(1)}$. Their number is bounded by $k(\delta + d)^{O(r)}$ and their binary lengths are less than $(M + r)(\delta + d)^{O(1)}$.*
- *The degree of g w.r.t. $u_1, \ldots, u_r, X$ is bounded by $(\delta + d)^{O(1)}$.*
- *The binary length of g is less than $(M + r)(\delta + d)^{O(1)}$.*
- *The leading coefficient $lc_X(g) \in \mathbb{Q}[u_1, \ldots, u_r]$ of g w.r.t. X does not vanish on W.*

The number of arithmetic operations of this algorithm is bounded by $k^{O(1)}(\delta + d)^{O(r)}$ over $\mathbb{Q}$. Its binary complexity is bounded by $(kM)^{O(1)}(\delta + d)^{O(r)}$.

Proof. See Lemma 1 of [6]. □

4 A new algorithm

The idea behind this algorithm is based on the following lemma which gives a method to compute the GCD of univariate polynomials by solving linear systems:

Lemma 4.1 *Let K be a field and $h_1, \ldots h_k \in K[X]$ of degrees $\leq d$ and let $h \in K[X]$ be a GCD of $h_1, \ldots, h_k$. Then*

- *There exist polynomials $s_1, \ldots, s_k \in K[X]$ of degrees $< d$ such that $h = \sum_{1 \leq i \leq k} s_i h_i$.*
- *The degree of h is given by the formula:*

$$\deg(h) = \min \{ \deg(g);\ \exists s_1, \ldots, s_k \in K[X],\ \deg(s_i) < d,\ \forall 1 \leq i \leq k,$$

$$g = \sum_{1 \leq i \leq k} s_i h_i \neq 0 \}.$$

For any $0 \leq t \leq d$, we take the parametric linear system S_t defined by the following property:

$$\sum_{1 \leq i \leq k} s_i f_i \text{ is a monic polynomial of degree t and } \deg(s_i) < d.$$

We write each s_i in the form: $s_i = \sum_{0 \leq j < d} s_{ij} X^j$. Then S_t is defined by the following parametric linear equations:

$$\sum_{1 \leq i \leq k, 0 \leq j \leq m} s_{ij} f_{i,m-j} = \begin{cases} 0 & if \quad t < m < 2d \\ 1 & if \quad m = t \end{cases}$$

The unknowns of the system S_t are the variables s_{ij}, their number is equal to kd, the number of the equations of S_t is equal to $2d - t$. The degrees of the entries of S_t w.r.t. u are bounded by δ and their binary lengths are less than M.

Based on Lemma 4.1 and an algoritm for solving parametric linear systems from Section 4.1, we get the following theorem (see Section 4.2 for its demonstration):

Theorem 4.2 *There is an algorithm which for a given set $\{f_1, \ldots, f_k\} \subset \mathbb{Q}[u_1, \ldots, u_r][X]$ of parametric univariate polynomials decomposes the set $\mathcal{U}$ into at most $(d+1)$ PGCD such that for each PGCD (V, g) among them, where V is a constructible subset of $\mathcal{U}$ and $g \in \mathbb{Q}(u_1, \ldots, u_r)[X]$, the following bounds are satisfied:*

- *The degrees of g and the equations and inequations which define V w.r.t. u are bounded by $kd\delta$. Their binary lengths are less than kdM.*

The number of arithmetic operations of this algorithm is bounded by $(kd\delta)^{O(r)}$ over $\mathbb{Q}$. Its binary complexity is bounded by $M(kd\delta)^{O(r)}$.

4.1 Parametric Gaussian elimination

Parametric linear systems form a particular case of parametric polynomial systems where equations have degrees 1. Algorithms for solving parametric linear systems are given by Heintz [7] and Sit [14, 13]. In this subsection, we give an improved presentation of a parametrization of the well-known Gaussian algorithm with a study on the bounds of the outputs of the algorithm and a complete complexity analysis.

Let $Ax = b$ be a parametric linear system, where A is a $n \times n$ matrix, b is a n vector and $x = (x_1, \ldots, x_n)$ is the vector of the unknowns. We suppose

that all entries of A and b belong to $\mathbb{Q}[u_1, \ldots, u_r]$ with degrees bounded by δ and binary lengths less than M. Our goal is to study the dependancy of the solutions of the system from different values of the parameters. It is well-known that (non-parametric) linear systems can be only in one of the three states: no solutions, unique solution or infinite number of solutions. The set $\{det(A) \neq 0\} \subset \mathcal{P}$ defines the locus in the parameters space $\mathcal{P}$ where the associated systems have unique solution in $\overline{\mathbb{Q}}^n$ (where $det(A) \in \mathbb{Q}[u_1, \ldots, u_r]$ is the determinant of A). This solution is then given by Cramer's formulas as rational functions in the parameters:

$$x_j = \frac{\det(A_j)}{\det(A)} \in \mathbb{Q}(u_1, \ldots, u_r) \quad 1 \leq j \leq n$$

where A_j is the matrix obtained by replacing the j-th column of A by the vector b.

The parametrization of the Gaussian elimination procedure consists of performing ordinary Gaussian algorithm and separating steps where pivot Gaussian elements are non-zeros. The main theorem of this subsection is the following one:

Theorem 4.3 *There is an algorithm, called the parametric Gaussian algorithm which for a parametric linear system $Ax = b$ (with the above notations), products a partition of the parameters space $\mathcal{P}$ into $(n+1)$ constructible sets $\mathcal{U}_i$ $(0 \leq i \leq n)$ which satisfy the following properties:*

- *The rank of A is constant in each $\mathcal{U}_i$ and is equal to i, this means that for any $a \in \mathcal{U}_i$, $rk(A^{(a)}) = i$, where $A^{(a)}$ is the matrix obtained from A by specialization of its entries on a.*
- *For each $\mathcal{U}_i$, the algorithm computes $(n-i+1)$ vectors $Z_0, Z_1, \ldots, Z_{n-i} \in \mathbb{Q}(u_1, \ldots, u_r)^n$ where Z_0 is a generic particular solution of $Ax = b$ and $\{Z_1, \ldots, Z_{n-i}\}$ is a generic basis of the solution space of the associated parametric homogeneous system i.e., for all $a \in \mathcal{U}_i$, we have:*
  - *The denominators of the entries of $Z_0, Z_1, \ldots, Z_{n-i}$ dont vanish on a.*
  - *$Z_0^{(a)}$ is a particular solution of the system $A^{(a)}x = b^{(a)}$ and the set $\{Z_1^{(a)}, \ldots, Z_{n-i}^{(a)}\}$ is a basis of the associated homogeneous system $A^{(a)}x = 0$.*

The degrees of the equations and inequations which define $\mathcal{U}_i$ and the degrees of the entries of $Z_0, Z_1, \ldots, Z_{n-i}$ w.r.t. u are bounded by $n\delta$. Their binary lengths are less than nM. The total complexity of the algorithm is $(n\delta)^{O(r)}$ operations in $\mathbb{Q}$ and the total binary complexity is $M(n\delta)^{O(r)}$.

Proof. The algorithm constructs a set of couples $(C^{(i)}, A^{(i)})$, $0 \leq i \leq n$ where $C^{(0)} = \mathcal{P}$, $A^{(0)} = A$ and $C^{(i)}$ $(1 \leq i \leq n)$ is a constructible subset of $\mathcal{P}$ given by its equations and inequations and $A^{(i)} = \left(A^{(i)}_{s,t}\right)_{1 \leq s,t \leq n}$ is a $n \times n$ matrix with coefficients in $\mathbb{Q}[u_1, \ldots, u_r]$ obtained from A by linear row transformations and permutations. This matrix has the form:

$$A^{(i)} = \begin{pmatrix} A^{(i)}_{1,1} & \ldots & \ldots & \ldots & \ldots & \ldots & A^{(i)}_{1,n} \\ 0 & A^{(i)}_{2,2} & \ldots & \ldots & \ldots & \ldots & A^{(i)}_{2,n} \\ \vdots & 0 & \ddots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & 0 & A^{(i)}_{i,i} & \ldots & \ldots & A^{(i)}_{i,n} \\ \vdots & \vdots & \vdots & 0 & A^{(i)}_{i+1,i+1} & \ldots & A^{(i)}_{i+1,n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & A^{(i)}_{n,i+1} & \ldots & A^{(i)}_{n,n} \end{pmatrix}$$

such that for all $a \in C^{(i)}$,

$$A^{(i)}_{1,1}(a) \neq 0, \ldots, A^{(i)}_{i,i}(a) \neq 0.$$

We do this construction by induction on i. We suppose that at the i-th step, $C^{(i)}$ is defined by equations and inequations of the form $g = 0$ and $h \neq 0$ where $g, h \in \mathbb{Q}[u_1, \ldots, u_r]$ satisfy the following bounds:

- The degrees of g, h and $A^{(i)}_{s,t}$ $(1 \leq s, t \leq n)$ w.r.t. u are bounded by $i\delta$;
- The binary lengths of g, h and $A^{(i)}_{s,t}$ $(1 \leq s, t \leq n)$ are less than $i(M+1)$.

The $(i+1)$-th step consists to do the following:

- If $A^{(i)}_{i+1,i+1} \in \mathbb{Q}[u_1, \ldots, u_r]$ is linearly dependent of the polynomials g, we exchange the $(i+1)$-th row of $A^{(i)}$ by the $(i+2)$-th row and we test again if $A^{(i)}_{i+2,i+1}$ is linearly dependent of g and so on. Each test corresponds to solve a linear system with at most i unknowns and $\binom{r+i\delta}{r} \leq (i\delta)^r$ equations with coefficients in $\mathbb{Q}$. This resolution can be done with $(i\delta)^{O(r)}$ operations in $\mathbb{Q}$ [10]. Each of these operations is done on elements of binary lengths less than $i(M+1)$. Then each test is done by $(i\delta)^{O(r)}$ operations in $\mathbb{Q}$. Its binary complexity is bounded by $M(i\delta)^{O(r)}$.
- If all the polynomials $A^{(i)}_{s,t}$, $s \geq i+1$, $t \geq i+1$ (even after exchange of columns) are linearly dependent of the polynomials g then $A^{(i)}_{s,t}(a) = 0$ for all $a \in C^{(i)}$. In this case, the algorithm stops and does not consider

the next couple $(C^{(i+1)}, A^{(i+1)})$. The number of tests to do is equal to $(n-i)^2$. They are done by $n^2(i\delta)^{O(r)}$ operations in $\mathbb{Q}$ and with binary complexity bounded by $n^2 M(i\delta)^{O(r)}$.

- If there exist $s_0 \geq i+1$, $t_0 \geq i+1$ such that $A^{(i)}_{s_0,t_0}$ is linearly independent of the polynomials g then we take $C^{(i+1)} = C^{(i)} \cap \{A^{(i)}_{s_0,t_0} \neq 0\}$. After exchange of rows and columns, we put $A^{(i)}_{s_0,t_0}$ in the position $(i+1, i+1)$ and we apply the ordinary linear transformations on the rows $i+2, \ldots, n$ of the obtained matrix. This will make zeros the entries below $A^{(i)}_{s_0,t_0}$ (we say that $A^{(i)}_{s_0,t_0}$ is the parametric Gauss pivot, i.e., $A^{(i)}_{s_0,t_0}(a) \neq 0$ for all $a \in C^{(i+1)}$). Then $A^{(i+1)}$ is the obtained matrix which verifies the following property: $A^{(i+1)}_{i+1,i+1} = A^{(i)}_{s_0,t_0}$ does not vanish on $C^{(i+1)}$.

  By Bareiss's method (see e.g., [4, 2]), the polynomials $A^{(i+1)}_{s,t} \in \mathbb{Q}[u_1, \ldots, u_r]$ are $(i+1) \times (i+1)$ minors of the matrix A and are given by the formula:

$$A^{(i+1)}_{s,t} = \det \begin{pmatrix} A_{1,1} & \ldots & A_{1,i} & A_{1,t} \\ \vdots & & \vdots & \vdots \\ A_{i,1} & \ldots & A_{i,i} & A_{i,t} \\ A_{s,1} & \ldots & A_{s,i} & A_{s,t} \end{pmatrix}$$

  This proves the above induction bounds on the degrees of $A^{(i+1)}_{s,t}$ w.r.t. u and on their binary lengths.

The solutions of the system $Ax = b$ are then computed as usually, i.e., as in the case of non-parametric Gaussian eliminations. The total complexity of the algorithm is deduced from the above bounds by the fact that there is at most n steps in the algorithm. □

4.2 Proof of Theorem 4.2

We apply the algorithm of Theorem 4.3 to the parametric linear systems $S_0, \ldots, S_d$ of the beginning of Section 4. The algorithm computes constructible subsets $U_0, \ldots, U_d$ of $\mathcal{U}$ and rational functions

$$s_{0,i,j}, \ldots, s_{d,i,j} \in \mathbb{Q}(u_1, \ldots, u_r), \quad 1 \leq i \leq k,\ 0 \leq j < d.$$

which satisfy the following properties:

- The constructible sets $V_t = U_t \setminus \bigcup_{0 \leq t' < t} U_{t'}$ $(0 \leq t \leq d)$ form a partition of $\mathcal{U}$.

- For any $0 \leq t \leq d$, U_t is the consistent locus of the system S_t, i.e., for all $a \in U_t$, the system S_t specialized on a admits the vector

$$\left(s_{t,i,j}^{(a)}\right)_{1 \leq i \leq k,\, 0 \leq j < d} \in \overline{\mathbb{Q}}^{kd}$$

  as solution (in particular each $s_{t,i,j}$ is well-defined in U_t).

  Then by Lemma 4.1 for all $a \in V_t$, the monic polynomial $s_t^{(a)} \in \overline{\mathbb{Q}}[X]$ of degree t is a GCD of the polynomials $f_1^{(a)}, \ldots, f_k^{(a)} \in \overline{\mathbb{Q}}[X]$ where

$$s_t = \sum_{1 \leq i \leq k,\, 0 \leq j < d} s_{t,i,j} X^j f_i \in \mathbb{Q}(u_1, \ldots, u_r)[X].$$

- The degrees of the equations and inequations which define each V_t and s_t $(0 \leq t \leq d)$ w.r.t. u are bounded by $kd\delta$. Their binary lengths are less than kdM.

From the complexity bounds of Theorem 4.3, one can deduce those of Theorem 4.2. □

5 Applications

5.1 Solving algebraic systems of parametric univariate polynomials

A parametric algebraic system is a finite set of multivariate polynomials $f_1, \ldots, f_k \in \mathbb{Q}[u_1, \ldots, u_r][X_1, \ldots, X_n]$ with polynomial coefficients in the parameters $u_1, \ldots, u_r$ over $\mathbb{Q}$. Solving a parametric algebraic system returns to determine the values of the parameters in $\mathcal{P}$ for which the associated polynomial systems have solutions in $\overline{\mathbb{Q}}^n$ (we call them consistent systems). However, when the system is consistent, it is sometimes necessary to describe the set of its solutions uniformly in these values of the parameters (see Section 4.1 for the case of parametric linear systems, i.e., when the polynomials $f_1, \ldots, f_k$ have degrees 1 w.r.t. $X_1, \ldots, X_n$).

In the case $n = 1$, i.e., when we have to solve algebraic systems of parametric univariate equations with arbitrary degrees. Each algorithm for computing PGCDs gives a way to reduce the problem of solving $k \geq 2$ parametric univariate equations to that of just one parametric univariate equation. For a PGCD (W, g) of the set $\{f_1, \ldots, f_k\}$, if $deg_X(g) = 0$ and $g \neq 0$ then W is the set where $f_1, \ldots, f_k$ have no common roots in $\overline{\mathbb{Q}}$. In general, if $0 \neq lc_X(g) \in \mathbb{Q}$ then $deg_X(g)$ determines the number of common roots (counted with their multiplicities) of $f_1^{(a)}, \ldots, f_k^{(a)}$ for all $a \in W$.

5.2 Multiplicities of roots of parametric univariate polynomials

Let $G \in \mathbb{Q}[u_1, \ldots, u_r][X]$ be a parametric univariate polynomial of degree bounded by d (resp. δ) w.r.t. X (resp. u) and binary length less than M. We suppose that G is coded by dense representation.

The goal of this section is to compute the multiplicities of the roots of $G^{(a)}$ in $\overline{\mathbb{Q}}$ uniformly in the values a of the parameters in $\mathcal{P}$.

Definition 5.1 *Let K be a field and $g \in K[X]$ be a univariate polynomial with coefficients in K. The multiset of the multiplicities of g is the vector $(m_1, \ldots, m_s) \in \mathbb{N}^s$ where m_i is the multiplicity of a root of g in an algebraic extension $\overline{K}$ of K (there is no order on the integers of this multiset).*

Based on the fact that the multiplicities of the roots of G are given by the degree of the greatest common divisor of the successive derivatives of G w.r.t. X, we can use one of the algorithm of the above sections to compute uniformly the multiset of the multiplicities of G as follows:

Theorem 5.2 *Let G be a parametric univariate polynomial with the above notations. There is an algorithm which decomposes the parameters space $\mathcal{P}$ into at most $d(d+1)$ constructible sets such that for each set $\mathcal{V}$ among them, we have the following properties:*

- *The algorithm computes a vector $m = (m_1, \ldots, m_h) \in \mathbb{N}^h$ such that for any $a \in \mathcal{V}$, the vector m is the multiset of the multiplicities of the roots of the polynomial $G^{(a)} \in \overline{\mathbb{Q}}[X]$.*
- *The degrees of the equations and inequations which define $\mathcal{V}$ w.r.t. u are bounded by $d(d+1)\delta$. Their binary lengths are less than $d(d+1)M$.*

The number of arithmetic operations of this algorithm is bounded by $(d\delta)^{O(r)}$ over $\mathbb{Q}$. Its binary complexity is bounded by $M(d\delta)^{O(r)}$.

Proof. For any $1 \leq j \leq \deg_X(G) \leq d$, the algorithm of Theorem 4.2 computes parametric GCDs of the set $\{G, G', \ldots, G^{(j)}\} \subset \mathbb{Q}[u_1, \ldots, u_r][X]$ of successive derivatives of G w.r.t. X. This algorithm presents this GCD in the form:

$$A_{j,t}X^t + A_{j,t-1}X^{t-1} + \cdots + A_{j,0} \in \mathbb{Q}[u_1, \ldots, u_r][X]$$

such that $\deg_{u_1,\ldots,u_r}(A_{j,l}) \leq (j+1)d\delta$ for all $0 \leq l \leq t \leq d-j$. The degree of $\mathrm{GCD}(G, G', \ldots, G^{(j)})$ for all $1 \leq j \leq d$ determines the multiset of the multiplicities of the roots of G. The following constructible sets

$$\mathcal{V}_{j,l} := \{A_{j,l} *_{j,l} 0\} \subset \mathcal{P}$$

(where $*_{j,l} \in \{=, \neq\}$) form a partition of $\mathcal{P}$ such that the multiset of the multiplicities of the roots of G is constant in each one among them. The complexity bounds of the algorithm are deduced from those of the algorithm of Theorem 4.2. □

6 Conclusion

In this paper, we have dealt with the complexity of the computation of generic GCDs of a finite set of parametric univariate polynomials. We have presented three algorithms for solving this problem: the first algorithm (Section 2) has the worst complexity bound, the two other algorithms (Sections 3 and 4) are better because that their complexity bound is polynomial in k and d but they are still far from being implemented. A futur work is to improve these bounds by elaborating new efficient algorithms, easy to implement. One way to do that is to use the approach presented here, i.e., try to parametrize existing algorithms for computing GCDs and possibly intermediate algorithms.

ACKNOWLEDGEMENTS. We gratefully thank Professor Dimitry Grigoryev for his help in the redaction of this paper, and more generally for his suggestions about the approach presented here.

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] B. Buchberger, G. E. Collins, R. Loos and R. Albrecht, *Computer Algebra: Symbolic and Algebraic Computation*, Wien, Springer, 1983.

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

[6] D. Grigoryev, *Complexity of quantifier elimination in the theory of ordinary differential equations*, Lecture Notes Computer Science, vol. **378** (1989), 11 - 25.

[7] J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields*, Theor. Comput. Sci. **24, 3** (1983), 239 - 277.

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

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

[10] G. Matera and J.M.T. Torres, *The Space Complexity of Elimination Theory: Upper bounds*, Foundations of Computational Mathematics, FOCM'97, Springer Verlag, 1997, 267 - 276.

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

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

[13] W.Y. Sit, *An algorithm for solving parametric linear systems*, J. Symbolic Computation, **13** (1992), 353 - 394.

[14] W.Y. Sit, *A theory for parametric linear systems*, Proceedings of the 1991 international symposium on Symbolic and algebraic computation, Bonn, West Germany, 1991, 112 - 121.

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

[16] 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.

Received: June, 2009