Rational Univariate Representations of Bivariate Systems and Applications

Yacine Bouzidi
INRIA Nancy Grand Est
LORIA, Nancy, France
Yacine.Bouzidi@inria.fr

Sylvain Lazard
INRIA Nancy Grand Est
LORIA, Nancy, France
Sylvain.Lazard@inria.fr

Marc Pouget
INRIA Nancy Grand Est
LORIA, Nancy, France
Marc.Pouget@inria.fr

Fabrice Rouillier
INRIA Paris-Rocquencourt
IMJ, Paris, France
Fabrice.Rouillier@inria.fr

ABSTRACT

We address the problem of solving systems of two bivariate polynomials of total degree at most d with integer coefficients of maximum bitsize τ. We suppose known a linear separating form (that is a linear combination of the variables that takes different values at distinct solutions of the system) and focus on the computation of a Rational Univariate Representation (RUR).

We present an algorithm for computing a RUR with worst-case bit complexity in $\widetilde{O}_B(d^7 + d^6\tau)$ and bound the bitsize of its coefficients by $\widetilde{O}(d^2 + d\tau)$ (where O_B refers to bit complexities and $\widetilde{O}$ to complexities where polylogarithmic factors are omitted). We show in addition that isolating boxes of the solutions of the system can be computed from the RUR with $\widetilde{O}_B(d^8+d^7\tau)$ bit operations. Finally, we show how a RUR can be used to evaluate the sign of a bivariate polynomial (of degree at most d and bitsize at most τ) at one real solution of the system in $\widetilde{O}_B(d^8 + d^7\tau)$ bit operations and at all the $\Theta(d^2)$ solutions in only $O(d)$ times that for one solution.

Categories and Subject Descriptors

F.2 [**Analysis of Algorithms and Problem Complexity**]: Nonnumerical Algorithms and Problems

Keywords

Bivariate system; Rational univariate representation

1. INTRODUCTION

There exists many algorithms, in the literature, for "solving" algebraic systems of equations. Some focus on computing "*formal solutions*" such as rational parameterizations, Gröbner bases, and triangular sets, others focus on isolating the solutions. By isolating the solution, we mean computing isolating axis-parallel boxes sets such that every real solution lies in a unique box and conversely. In this paper, we focus on the worst-case bit complexity of these methods (in the RAM model) for systems of **two bivariate polynomials of total degree d with integer coefficients of bitsize τ.**

For isolating the real solutions of systems of two bivariate polynomials, the algorithm with best known bit complexity was recently analyzed by Emeliyanenko and Sagraloff [9]. They solve the problem in $\widetilde{O}_B(d^8+d^7\tau)$ bit operations (where $\widetilde{O}$ refers to complexities where polylogarithmic factors are omitted and O_B refers to bit complexities). Furthermore, the isolating boxes can easily be refined because the algorithm computes the univariate polynomials that correspond to the projections of the solutions on each axis (that is, the resultants of the two input polynomials with respect to each of the variables).

Other widespread approaches that solve systems are those that compute rational parameterizations of the (complex) solutions. Recall that such a rational parameterization is a set of univariate polynomials and associated rational one-to-one mappings that send the roots of the univariate polynomials to the solutions of the system. The algorithm with the best known complexity for solving such systems via rational parameterizations was, in essence, first introduced by Gonzalez-Vega and El Kahoui [11]. The algorithm first applies a generic linear change of variables to the input polynomials, computes a rational parameterization using the subresultant sequence of the sheared polynomials and finally computes the isolating boxes of the solutions. Its initial bit complexity of $\widetilde{O}_B(d^{16} + d^{14}\tau^2)$ was improved by Diochnos et al. [8, Theorem 19] to (i) $\widetilde{O}_B(d^{10} + d^9\tau)$ for computing a generic shear (i.e., a separating linear form), to (ii) $\widetilde{O}_B(d^7+d^6\tau)$ for computing a rational parameterization and to (iii) $\widetilde{O}_B(d^{10} + d^9\tau)$ for the isolation phase with a modification of the initial algorithm.[1]

Main results. We addressed in [4] the first phase of the above algorithm and proved that a separating linear form

[1]The complexity of the isolation phase in [8, Theorem 19] is stated as $\widetilde{O}_B(d^{12}+d^{10}\tau^2)$ but it trivially decreases to $\widetilde{O}_B(d^{10}+d^9\tau)$ with the recent result of Sagraloff [17] which improves the complexity of isolating the real roots of a univariate polynomial.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
ISSAC'13, June 26–29, 2013, Boston, Massachusetts, USA.
Copyright 2013 ACM 978-1-4503-2059-7/13/06 ...$15.00.

can be computed in $\widetilde{O}_B(d^8+d^7\tau+d^5\tau^2)$ bit operations.[2] We address in this paper the second and third phase of the above algorithm, that is the computation of a rational parameterization and the isolation of the solutions of the system. We also consider an important related problem, namely, the evaluation of the sign of a polynomial at a real solution of a system, referred to as the *sign_at* operation.

We first show that the Rational Univariate Representation (RUR for short) of Rouillier [15] (i) can be expressed with simple polynomial formulas, that (ii) it has a total bitsize which is asymptotically smaller than that of Gonzalez-Vega and El Kahoui by a factor d, and that (iii) it can be computed with the same complexity, that is $\widetilde{O}_B(d^7+d^6\tau)$ (Theorem 13). Namely, we prove that the RUR consists of four polynomials of degree $O(d^2)$ and bitsize $\widetilde{O}(d^2+d\tau)$ (instead of $O(d)$ polynomials with the same asymptotic degree and bitsize for Gonzalez-Vega and El Kahoui parameterization).

For the next two applications, we focus for simplicity on a parameterization given by the RUR as defined in [15], but the complexity results also hold for the one defined in [11].

We show that, given a RUR, isolating boxes of the solutions of the system can be computed with $\widetilde{O}_B(d^8+d^7\tau)$ bit operations (Proposition 16). This decreases by a factor d^2 the best known complexity for the isolation phase of the algorithm (see the discussion above). Globally, this bounds the overall bit complexity of all three phases of the algorithm by $\widetilde{O}_B(d^8+d^7\tau)$, if $\tau \in \widetilde{O}(d^2)$.

Finally, we show how a RUR can be used to perform efficiently the *sign_at* operation. Given a polynomial F of total degree at most d with integer coefficients of bitsize at most τ, we show that the sign of F at one real solution of the system can be computed in $\widetilde{O}_B(d^8+d^7\tau)$ bit operations, while the complexity of computing its sign at all the $\Theta(d^2)$ solutions of the system is only $O(d)$ times that for one real solution (Theorem 19). This improves the best known complexities of $\widetilde{O}_B(d^{10}+d^9\tau)$ and $\widetilde{O}_B(d^{12}+d^{11}\tau)$ for these respective problems (see [8, Th. 14 & Cor. 24] with the improvement of [17] for the root isolation).

2. NOTATION AND PRELIMINARIES

The bitsize of an integer p is the number of bits needed to represent it, that is $\lfloor \log p \rfloor + 1$ (log refer to the logarithm in base 2). For rational numbers, we refer to the bitsize as to the maximum bitsize of its numerator and denominator. The bitsize of a polynomial with integer or rational coefficients is the *maximum* bitsize of its coefficients.

We denote by $\mathbb{D}$ a unique factorization domain, typically $\mathbb{Z}[X,Y]$, $\mathbb{Z}[X]$ or $\mathbb{Z}$. We also denote by $\mathbb{F}$ a field, typically $\mathbb{Q}$, $\mathbb{C}$. For any polynomial $P \in \mathbb{D}[X]$, let $Lc_X(P)$ denote its leading coefficient with respect to the variable X (or simply $Lc(P)$ in the univariate case), $d_X(P)$ its degree with respect to X, and $\overline{P}$ its squarefree part. The ideal generated by two polynomials P and Q is denoted $\langle P,Q\rangle$, and the affine variety of an ideal I is denoted by $V(I)$. The solutions are always considered in the algebraic closure of the fraction field of $\mathbb{D}$, unless specified otherwise. For a point $\sigma \in V(I)$, $\mu_I(\sigma)$ denotes the multiplicity of σ in I. For simplicity, we refer indifferently to the ideal $\langle P,Q\rangle$ and to the corresponding system of polynomials.

[2]This improves the previous complexity $\widetilde{O}_B(d^{10}+d^9\tau)$ by a factor $\min(d^2, \frac{d^4}{\tau})$ if $\tau \in \widetilde{O}(d^4)$.

We finally introduce the following notation which are extensively used throughout the paper. Given the two input polynomials P and Q, we consider the "generic" change of variables $X = T - SY$, and we define the "sheared" polynomials $P(T-SY,Y)$, $Q(T-SY,Y)$, and their resultant with respect to Y,

$$R(T,S) = Res_Y(P(T-SY,Y), Q(T-SY,Y)). \quad (1)$$

We introduce

$$\begin{array}{c} L_P(S) = Lc_Y(P(T-SY,Y)) \\ L_Q(S) = Lc_Y(Q(T-SY,Y)), \quad L_R(S) = Lc_T(R(T,S)) \end{array} \quad (2)$$

and remark that these polynomials do not depend on T.

Complexity. In the sequel, we often consider the gcd of two univariate polynomials P and Q and the gcd-free part of P with respect to Q, that is, the divisor D of P such that $P = \gcd(P,Q)D$. Note that when $Q = P'$, D is the squarefree part $\overline{P}$ of P.

LEMMA 1 ([2, REMARK 10.19]). *Two polynomials P, Q in $\mathbb{Z}[X]$ with maximum degree d and bitsize at most τ have a gcd (in $\mathbb{Q}[X]$ or in $\mathbb{Z}[X]$) with coefficients of bitsize in $\widetilde{O}(d+\tau)$ which can be computed with $\widetilde{O}_B(d^2\tau)$ bit operations. The same bounds hold for the bitsize and the computation of the gcd-free part of P with respect to Q. If P and Q are in $\mathbb{Q}[X]$ and there exists $c \in \mathbb{Z}$ of bitsize in $O(\tau)$ such that cP and cQ are in $\mathbb{Z}[X]$ with coefficients of bitsize in $O(\tau)$, then the same results also hold.*

We now state a bound on the complexity of evaluating a univariate polynomial which is straightforward and ought to be known, even though we were not able to find a proper reference for it (see [3] for details).

LEMMA 2. *Let a be a rational of bitsize τ_a, the evaluation at a of a univariate polynomial f of degree d and rational coefficients of bitsize τ can be done in $\widetilde{O}_B(d(\tau+\tau_a))$ bit operations, while the value $f(a)$ has bitsize in $O(\tau + d\tau_a)$.*

As we often use the "sheared" polynomials $P(T-SY,Y)$ and $Q(T-SY,Y)$ we also recall some related complexities.

LEMMA 3 ([4, LEMMA 5]). *Let $P,Q \in \mathbb{Z}[X,Y]$ of total degree d and maximum bitsize τ. The sheared polynomials $P(T-SY,Y)$ and $Q(T-SY,Y)$ can be expanded in $\widetilde{O}_B(d^4+d^3\tau)$ and their bitsizes are in $\widetilde{O}(d+\tau)$. The resultant $R(T,S)$ can be computed in $\widetilde{O}_B(d^7+d^6\tau)$ bit operations; its degree is at most $2d^2$ in each variable and its bitsize is in $\widetilde{O}(d^2+d\tau)$.*

3. RATIONAL UNIV. REPRESENTATIONS

The idea of this section is to express the polynomials of a RUR of two polynomials in terms of a resultant defined from these polynomials. Given a separating form, this yields a new algorithm to compute a RUR (Section 3.1) and it also enables us to derive the bitsize of the polynomials of a RUR (Section 3.2). Throughout this section we assume that the two input polynomials P and Q are coprime in $\mathbb{Z}[X,Y]$, that their maximum total degree d is at least 2 and that their coefficients have maximum bitsize τ. We first recall the definition and main properties of Rational Univariate Representations. In the following, for any polynomial $v \in \mathbb{Q}[X,Y]$ and $\sigma = (\alpha,\beta) \in \mathbb{C}^2$, we denote by $v(\sigma)$ the image of σ by the polynomial function v (e.g. $X(\alpha,\beta) = \alpha$).

Definition 4 ([15]). *Let $I \subset \mathbb{Q}[X,Y]$ be a zero-dimensional ideal, $V(I) = \{\sigma \in \mathbb{C}^2, v(\sigma) = 0, \forall v \in I\}$ its associated variety, and a linear form $T = X + aY$ with $a \in \mathbb{Q}$. The RUR-candidate of I associated to $X + aY$ (or simply, to a), denoted $RUR_{I,a}$, is the following set of four univariate polynomials in $\mathbb{Q}[T]$*

$$f_{I,a}(T) = \prod_{\sigma \in V(I)} (T - X(\sigma) - aY(\sigma))^{\mu_I(\sigma)} \tag{3}$$

$$f_{I,a,v}(T) = \sum_{\sigma \in V(I)} \mu_I(\sigma) v(\sigma) \prod_{\varsigma \in V(I), \varsigma \neq \sigma} (T - X(\varsigma) - aY(\varsigma))$$
$$\text{for } v \in \{1, X, Y\}.$$

If $(X,Y) \mapsto X + aY$ is injective on $V(I)$, we say that the linear form $X + aY$ separates $V(I)$ (or is separating for I), $RUR_{I,a}$ is called a RUR (the RUR of I associated to a) and it defines a bijection between $V(I)$ and $V(f_{I,a}) = \{\gamma \in \mathbb{C}, f_{I,a}(\gamma) = 0\}$:

$$\begin{array}{ccc} V(I) & \to & V(f_{I,a}) \\ (\alpha, \beta) & \mapsto & \alpha + a\beta \\ \left(\frac{f_{I,a,X}}{f_{I,a,1}}(\gamma), \frac{f_{I,a,Y}}{f_{I,a,1}}(\gamma)\right) & \leftarrow\!\shortmid & \gamma \end{array}$$

Moreover, this bijection preserves the real roots and the multiplicities.

3.1 RUR computation

We show here that the polynomials of a RUR can be expressed as combinations of specializations of the resultant R and its partial derivatives. The seminal idea has already been used by several authors in various contexts (see e.g. [6, 1, 18]) for computing rational parameterizations of the radical of a given zero-dimensional ideal and mainly for bounding the size of a Chow form. Based on the same idea but keeping track of multiplicities, we present a simple new formulation for the polynomials of a RUR, given a separating form.

Proposition 5. *For any $a \in \mathbb{Q}$ such that $L_P(a)L_Q(a) \neq 0$ and such that $X + aY$ is a separating form of $\langle P, Q\rangle$, the RUR of $\langle P, Q\rangle$ associated to a is as follows:*

$$f_{I,a}(T) = \frac{R(T,a)}{L_R(a)}$$
$$f_{I,a,1}(T) = \frac{f'_{I,a}(T)}{\gcd(f_{I,a}(T), f'_{I,a}(T))}$$
$$f_{I,a,Y}(T) = \frac{\frac{\partial R}{\partial S}(T,a) - f_{I,a}(T)\frac{\partial L_R}{\partial S}(a)}{L_R(a)\gcd(f_{I,a}(T), f'_{I,a}(T))}$$
$$f_{I,a,X}(T) = Tf_{I,a,1}(T) - d_T(f_{I,a})f_{I,a}(T) - af_{I,a,Y}(T).$$

We postpone the proof of Proposition 5 and first analyze the complexity of the computation of the expressions therein. Note that a separating form $X + aY$ as in Proposition 5, with $0 \leqslant a < 2d^4$, can be computed in $\widetilde{O}_B(d^8 + d^7\tau + d^5\tau^2)$ [4] or $\widetilde{O}_B(d^{10} + d^9\tau)$ [8] bit operations.

Proposition 6. *Computing the polynomials in Proposition 5 can be done with $\widetilde{O}_B(d^7 + d^6(\tau + \tau_a))$ bit operations, where τ_a is the bitsize of a.*

Proof. According to Lemma 3, the resultant $R(T,S)$ of $P(T - SY, Y)$ and $Q(T - SY, Y)$ with respect to Y has degree $O(d^2)$ in T and S, has bitsize in $\widetilde{O}(d(d+\tau))$, and can be computed in $\widetilde{O}_B(d^6(d+\tau))$ bit operations. Specializing $R(T,S)$ at $S = a$ can be done by evaluating $O(d^2)$ polynomials in S, each of degree in $O(d^2)$ and bitsize in $\widetilde{O}(d^2 + d\tau)$. By Lemma 2, each of the $O(d^2)$ evaluations can be done in $\widetilde{O}_B(d^2(d^2 + d\tau + \tau_a))$ bit operations and each result has bitsize in $\widetilde{O}(d^2 + d\tau + d^2\tau_a)$. Hence, $R(T,a)$ and $f_{I,a}(T)$ have degree in $O(d^2)$, bitsize in $\widetilde{O}(d^2 + d\tau + d^2\tau_a)$, and they can be computed with $\widetilde{O}_B(d^4(d^2 + d\tau + \tau_a))$ bit operations.

The complexity of computing the numerators of $f_{I,a,1}(T)$ and $f_{I,a,Y}(T)$ is clearly dominated by the computation of $\frac{\partial R}{\partial S}(T,a)$. Indeed, computing the derivative $\frac{\partial R}{\partial S}(T,S)$ can trivially be done in $O(d^4)$ arithmetic operations of complexity $\widetilde{O}_B(d^2 + d\tau)$, that is in $\widetilde{O}_B(d^6 + d^5\tau)$. Then, as for $R(T,a)$, $\frac{\partial R}{\partial S}(T,a)$ has degree in $O(d^2)$, bitsize in $\widetilde{O}(d^2 + d\tau + d^2\tau_a)$, and it can be computed within the same complexity as the computation of $R(T,a)$.

On the other hand, since $f_{I,a}(T)$ and $f'_{I,a}(T)$ have degree in $O(d^2)$ and bitsize in $\widetilde{O}(d^2 + d\tau + d^2\tau_a)$, and $f_{I,a}(T) = \frac{R(T,a)}{L_R(a)}$, one can multiply these two polynomials by the product of $L_R(a)$ and the denominator of the rational a to the power of $d_S(R(T,S))$ which is an integer of bitsize in $O(d^2\tau_a)$, to obtain polynomials with coefficients in $\mathbb{Z}$. Hence, according to Lemma 1, their gcd can be computed with $\widetilde{O}_B(d^4(d^2 + d\tau + d^2\tau_a))$ bit operations, and has bitsize in the same class of complexity.

$f_{I,a,1}(T)$ and $f_{I,a,Y}(T)$ are then obtained by dividing the numerators by the above gcd which can be done with $\widetilde{O}_B(d^4(d^2 + d\tau + d^2\tau_a))$ bit operations, according to [20, Theorem 9.6 and subsequent discussion]. Finally, computing $f_{I,a,X}(T)$ can be done within the same complexity as for $f_{I,a,1}(T)$ and $f_{I,a,Y}(T)$ since it is dominated by the computation of the squarefree part of $f_{I,a}(T)$.

The overall complexity is thus that of computing the resultant which is in $\widetilde{O}_B(d^6(d+\tau))$ plus that of computing the above gcd and Euclidean division which is in $\widetilde{O}_B(d^4(d^2 + d\tau + d^2\tau_a))$. This gives a total of $\widetilde{O}_B(d^7 + d^6(\tau + \tau_a))$. □

Proof of Proposition 5. Proposition 5 expresses the polynomials $f_{I,a}$ and $f_{I,a,v}$ of a RUR in terms of specializations (by $S = a$) of the resultant $R(T,S)$ and its partial derivatives. Since the specializations are done after considering the derivatives of R, we study the relations between these entities before specializing S by a.

For that purpose, we introduce the following polynomials which are exactly the polynomials $f_{I,a}$ and $f_{I,a,v}$ of (3) where the parameter a is replaced by the variable S. These polynomials can be seen as the RUR polynomials of the ideal I with respect to a "generic" linear form $X + SY$.

$$f_I(T,S) = \prod_{\sigma \in V(I)} (T - X(\sigma) - SY(\sigma))^{\mu_I(\sigma)} \tag{4}$$

$$f_{I,v}(T,S) = \sum_{\sigma \in V(I)} \mu_I(\sigma) v(\sigma) \prod_{\varsigma \in V(I), \varsigma \neq \sigma} (T - X(\varsigma) - SY(\varsigma))$$
$$\text{for } v \in \{1, X, Y\}.$$

These polynomials are obviously in $\mathbb{C}[T,S]$, but they are actually in $\mathbb{Q}[T,S]$ because, when S is specialized at any rational value a, the specialized polynomials are those of $RUR_{I,a}$ which are known to be in $\mathbb{Q}[T]$ (see e.g. [15]). We express the derivatives of $f_I(T,S)$ in terms of $f_{I,v}(T,S)$, in Lemma 7, and show that $f_I(T,S)$ is the monic form of the

resultant $R(T,S)$, seen as a polynomial in T, in Lemma 9. Let

$$g_I(T,S) = \prod_{\sigma\in V(I)} (T - X(\sigma) - SY(\sigma))^{\mu_I(\sigma)-1}.$$

LEMMA 7. *We have*

$$\frac{\partial f_I}{\partial T}(T,S) = g_I(T,S) f_{I,1}(T,S), \tag{5}$$

$$\frac{\partial f_I}{\partial S}(T,S) = g_I(T,S) f_{I,Y}(T,S). \tag{6}$$

PROOF. It is straightforward that the derivative of f_I with respect to T is $\sum_{\sigma\in V(I)} \mu_I(\sigma)(T-X(\sigma)-SY(\sigma))^{\mu_I(\sigma)-1} \prod_{\varsigma\in V(I),\varsigma\neq\sigma}(T - X(\varsigma) - SY(\sigma))^{\mu_I(\varsigma)}$, which can be rewritten as the product of $\prod_{\sigma\in V(I)}(T - X(\sigma) - SY(\sigma))^{\mu_I(\sigma)-1}$ and $\sum_{\sigma\in V(I)} \mu_I(\sigma) \prod_{\varsigma\in V(I),\varsigma\neq\sigma}(T - X(\varsigma) - SY(\varsigma))$ which is exactly the product of $g_I(T,S)$ and $f_{I,1}(T,S)$.

The expression of the derivative of f_I with respect to S is similar to that with respect to T except that the derivative of $T-X(\sigma)-SY(\sigma)$ is now $Y(\sigma)$ instead of 1. It follows that $\frac{\partial f_I}{\partial S}$ is the product of $\prod_{\sigma\in V(I)}(T-X(\sigma)-SY(\sigma))^{\mu_I(\sigma)-1}$ and $\sum_{\sigma\in V(I)} \mu_I(\sigma)Y(\sigma) \prod_{\varsigma\in V(I),\varsigma\neq\sigma}(T - X(\varsigma) - SY(\varsigma))$ which is the product of $g_I(T,S)$ and $f_{I,Y}(T,S)$. □

For the proof of Lemma 9, we will use the following lemma which states that when two polynomials have no common solution at infinity in some direction, the roots of their resultant with respect to this direction are the projections of the solutions of the system with cumulated multiplicities.

LEMMA 8 ([5, PROP. 2 AND 5]). *Let $P,Q \in \mathbb{F}[X,Y]$ defining a zero-dimensional ideal $I = \langle P,Q\rangle$, such that their leading terms $Lc_Y(P)$ and $Lc_Y(Q)$ do not have common roots. Then $Res_Y(P,Q) = c\prod_{\sigma\in V(I)}(X - X(\sigma))^{\mu_I(\sigma)}$ where c is nonzero in $\mathbb{F}$.*

LEMMA 9. *$R(T,S) = L_R(S)f_I(T,S)$ and, for any $a \in \mathbb{Q}$, $L_P(a)L_Q(a) \neq 0$ implies that $L_R(a) \neq 0$.*

PROOF. The proof is organized as follows. We first prove that for any rational a such that $L_P(a)L_Q(a)$ does not vanish, $R(T,a) = c(a)f_I(T,a)$ where $c(a) \in \mathbb{Q}$ is a nonzero constant depending on a. This is true for infinitely many values of a and, since $R(T,S)$ and $f_I(T,S)$ are polynomials, we can deduce that $R(T,S) = L_R(S)f_I(T,S)$. This will also implies the second statement of the lemma since, if $L_P(a)L_Q(a) \neq 0$, then $R(T,a) = c(a)f_I(T,a) = L_R(a)f_I(T,a)$ with $c(a) \neq 0$, thus $L_R(a) \neq 0$ (since $f_I(T,a)$ is monic).

Since a is such that $L_P(a)L_Q(a) \neq 0$, the resultant $R(T,S)$ can be specialized at $S = a$: $R(T,a)$ is equal to the resultant of $P(T - aY,Y)$ and $Q(T - aY,Y)$ with respect to Y[2, Proposition 4.20]. The polynomials $P(T - aY,Y)$ and $Q(T - aY,Y)$ satisfy the hypotheses of Lemma 8: first, their leading coefficients (in Y) do not depend on T, hence they have no common root in $\mathbb{Q}[T]$; second, the polynomials $P(T - aY,Y)$ and $Q(T - aY,Y)$ are coprime because $P(X,Y)$ and $Q(X,Y)$ are coprime by assumption and the change of variables $(X,Y) \mapsto (T = X + aY,Y)$ is a one-to-one mapping. Hence Lemma 8 yields that $R(T,a) = c(a)\prod_{\sigma\in V(I_a)}(T-T(\sigma))^{\mu_{I_a}(\sigma)}$, where $c(a) \in \mathbb{Q}$ is a nonzero constant depending on a, and I_a is the ideal generated by $P(T - aY,Y)$ and $Q(T - aY,Y)$.

We now observe that $\prod_{\sigma\in V(I_a)}(T - T(\sigma))^{\mu_{I_a}(\sigma)}$ is equal to $f_I(T,a) = \prod_{\sigma\in V(I)}(T - X(\sigma) - aY(\sigma))^{\mu_I(\sigma)}$ since any solution (α,β) of $P(X,Y)$ is in one-to-one correspondence with the solution $(\alpha+a\beta,\beta)$ of $P(T-aY,Y)$ (and similarly for Q) and the multiplicities of the solutions also match, i.e. $\mu_I(\sigma) = \mu_{I_a}(\sigma_a)$ when σ and σ_a are in correspondence through the mapping [10, §3.3 Prop. 3 and Thm. 3]. Hence,

$$L_P(a)L_Q(a) \neq 0 \Rightarrow R(T,a) = c(a)f_I(T,a) \text{ with } c(a) \neq 0. \tag{7}$$

Since there is finitely many values of rational a such that $L_P(a)L_Q(a)L_R(a) = 0$ and since $f_I(T,S)$ is monic with respect to T, (7) implies that $R(T,S)$ and $f_I(T,S)$ have the same degree in T, say D. We write these polynomials as

$$\begin{aligned} R(T,S) &= L_R(S)T^D + \sum_{i=0}^{D-1} r_i(S)T^i, \\ f_I(T,S) &= T^D + \sum_{i=0}^{D-1} f_i(S)T^i. \end{aligned} \tag{8}$$

If a is such that $L_P(a)L_Q(a)L_R(a) \neq 0$, (7) and (8) imply that $L_R(a) = c(a)$ and $r_i(a) = L_R(a)f_i(a)$, for all i. These equalities hold for infinitely many values of a, and $r_i(S), L_R(S)$ and $f_i(S)$ are polynomials in S, thus $r_i(S) = L_R(S)f_i(S)$ and, by (8), $R(T,S) = L_R(S)f_I(T,S)$. □

PROOF OF PROPOSITION 5. Lemma 9 immediately gives the first formula. Equation 5 states that $f_{I,1}(T,S)g_I(T,S) = \frac{\partial f_I(T,S)}{\partial T}$, withs $g_I(T,S) = \prod_{\sigma\in V(I)}(T-X(\sigma)-SY(\sigma))^{\mu_I(\sigma)-1}$. In addition, g_I being monic in T, it never identically vanishes when S is specialized, thus the preceding formula yields after specialization: $f_{I,a,1}(T) = \frac{f'_{I,a}(T)}{g_I(T,a)}$. Furthermore, $g_I(T,a) = \gcd(f_{I,a}(T), f'_{I,a}(T))$. Indeed, $f_{I,a}(T) = \prod_{\sigma\in V(I)}(T-X(\sigma)-aY(\sigma))^{\mu_I(\sigma)}$ and all values $X(\sigma) + aY(\sigma)$, for $\sigma \in V(I)$, are pairwise distinct since $X + aY$ is a separating form, thus the gcd of $f_{I,a}(T)$ and its derivative is $g_I(T,a) = \prod_{\sigma\in V(I)}(T - X(\sigma) - aY(\sigma))^{\mu_I(\sigma)-1}$. This proves the formula for $f_{I,a,1}$.

Concerning the third equation, Lemma 9 together with Equation 6 implies:

$$\begin{aligned} f_{I,Y}(T,S) &= \frac{\frac{\partial f_I(T,S)}{\partial S}}{g_I(T,S)} = \frac{\frac{\partial (R(T,S)/L_R(S))}{\partial S}}{g_I(T,S)} \\ &= \frac{\frac{\partial R(T,S)}{\partial S} - f_I(T,S)\frac{\partial L_R(S)}{\partial S}}{L_R(S)g_I(T,S)}. \end{aligned}$$

As argued above, when specialized, $g_I(T,a)$ is equal to the gcd of $f_{I,a}(T)$ and $f'_{I,a}(T)$), and it does not identically vanish. By Lemma 9, $L_R(a)$ does not vanish either, and the formula for $f_{I,a,Y}$ follows.

It remains to compute $f_{I,a,X}$. Definition 4 implies that, for any root γ of $f_{I,a}$: $\gamma = \frac{f_{I,a,X}}{f_{I,a,1}}(\gamma) + a\frac{f_{I,a,Y}}{f_{I,a,1}}(\gamma)$, and thus $f_{I,a,X}(\gamma) + af_{I,a,Y}(\gamma) - \gamma f_{I,a,1}(\gamma) = 0$. Replacing γ by T, we have that the polynomial $f_{I,a,X}(T) + af_{I,a,Y}(T) - Tf_{I,a,1}(T)$ vanishes at every root of $f_{I,a}$, thus the square-free part of $f_{I,a}$ divides that polynomial. In other words, $f_{I,a,X}(T) = Tf_{I,a,1}(T) - af_{I,a,Y}(T) \bmod \overline{f_{I,a}(T)}$. We now compute $Tf_{I,a,1}(T)$ and $af_{I,a,Y}(T)$ modulo $\overline{f_{I,a}(T)}$.

Equation (3) implies that $f_{I,a,v}(T)$ is equal to $T^{\#V(I)-1}\sum_{\sigma\in V(I)} \mu_I(\sigma)v(\sigma)$ plus some terms of lower degree in T, and that the degree of $\overline{f_{I,a}(T)}$ is $\#V(I)$ (since $X + aY$ is a separating form). First, for $v = Y$, this implies that $d_T(f_{I,a,Y}) < d_T(\overline{f_{I,a}})$, and thus that $af_{I,a,Y}(T)$ is already reduced modulo $\overline{f_{I,a}(T)}$. Second, for $v = 1$, $\sum_{\sigma\in V(I)} \mu_I(\sigma)$ is nonzero and equal to $d_T(f_{I,a})$. Thus, $Tf_{I,a,1}(T)$ and

$\overline{f_{I,a}(T)}$ are both of degree $\#V(I)$, and their leading coefficients are $d_T(f_{I,a})$ and 1, respectively. Hence $T f_{I,a,1}(T)$ mod $\overline{f_{I,a}(T)} = T f_{I,a,1}(T) - d_T(f_{I,a})\overline{f_{I,a}(T)}$. We thus obtain the last equation of Proposition 5. $\square$

3.2 RUR bitsize

We prove here a new bound on the bitsize of the coefficients of the polynomials of a RUR. This bound is interesting in its own right and is instrumental for our analysis of the complexity of computing isolating boxes of the solutions of the input system, as well as for performing *sign_at* evaluations. Note that we state our bound for RUR-*candidates*, that is even when the linear form $X + aY$ is not separating. In this paper, we only use this result when the form is separating but the general result is interesting in a probabilistic context when a RUR-candidate is computed with a random linear form.

PROPOSITION 10. *Let $P, Q \in \mathbb{Z}[X, Y]$ be two coprime polynomials of total degree at most d and maximum bitsize τ, and let a be a rational of bitsize τ_a. The polynomials of the RUR-candidate of $\langle P, Q\rangle$ associated to a have bitsize in $\widetilde{O}(d^2\tau_a + d\tau)$. Moreover, there exists an integer of bitsize in $\widetilde{O}(d^2\tau_a + d\tau)$ such that the product of this integer with the polynomials of the RUR-candidate yields polynomials with integer coefficients.*

Before proving Proposition 10, we state a corollary of Mignotte's lemma [13, Theorem 4bis]. We also introduce a notion of primitive part for polynomials in $\mathbb{Q}[X, Y]$ and some of its properties.

LEMMA 11. *Let $P \in \mathbb{Z}[X, Y]$ be of degree at most d in each variable with coefficients bitsize at most τ. If $P = Q_1Q_2$ with Q_1, Q_2 in $\mathbb{Z}[X, Y]$, then the bitsize of Q_i, $i = 1, 2$, is in $\widetilde{O}(d + \tau)$.*

Primitive part. Consider a polynomial P in $\mathbb{Q}[X, Y]$ of degree at most d in each variable. It can be written $P = \sum_{i,j=0}^{d} \frac{a_{ij}}{b_{ij}} X^iY^j$ with a_{ij} and b_{ij} coprime in $\mathbb{Z}$ for all i, j. We define the *primitive part* of P, denoted $pp(P)$, as P divided by the gcd of the a_{ij} and multiplied by the least common multiple (lcm) of the b_{ij}. (Note that this definition is not entirely standard since we do not consider contents that are polynomials in X or in Y.) We also denote by τ_P the bitsize of P (that is, the maximum bitsize of all the a_{ij} and b_{ij}). We prove three properties of the primitive part which will be useful in the proof.

LEMMA 12. *For any two polynomials P and Q in $\mathbb{Q}[X, Y]$, we have the following properties: (i) $pp(PQ) = pp(P)\,pp(Q)$. (ii) If P is monic then $\tau_P \leqslant \tau_{pp(P)}$ and, more generally, if P has one coefficient, ξ, of bitsize τ_ξ, then $\tau_P \leqslant \tau_\xi + \tau_{pp(P)}$. (iii) If P has coefficients in $\mathbb{Z}$, then $\tau_{pp(P)} \leqslant \tau_P$.*

PROOF. Gauss Lemma states that if two univariate polynomials with integer coefficients are primitive, so is their product. This lemma can straightforwardly be extended to be used in our context by applying a change of variables of the form $X^iY^j \to Z^{ik+j}$ with $k > 2\max(d_Y(P), d_Y(Q))$. Thus, if P and Q in $\mathbb{Q}[X, Y]$ are primitive (i.e., each of them has integer coefficients whose common gcd is 1), their product is primitive. It follows that $pp(PQ) = pp(P)\,pp(Q)$ because, writing $P = \alpha\, pp(P)$ and $Q = \beta\, pp(Q)$, we have $pp(PQ) = pp(\alpha\, pp(P)\,\beta\, pp(Q)) = pp(pp(P)\,pp(Q))$ which is equal to $pp(P)\,pp(Q)$ since the product of two primitive polynomials is primitive.

Second, if $P \in \mathbb{Q}[X, Y]$ has one coefficient, ξ, of bitsize τ_ξ, then $\tau_P \leqslant \tau_\xi + \tau_{pp(P)}$. Indeed, We have $P = \xi\frac{P}{\xi}$ thus $\tau_P \leqslant \tau_\xi + \tau_{\frac{P}{\xi}}$. Since $\frac{P}{\xi}$ has one of its coefficients equal to 1, its primitive part is $\frac{P}{\xi}$ multiplied by an integer (the lcm of the denominators), thus $\tau_{\frac{P}{\xi}} \leqslant \tau_{pp(\frac{P}{\xi})}$ and $pp(\frac{P}{\xi}) = pp(P)$ by definition, which implies the claim.

Third, if P has coefficients in $\mathbb{Z}$, then $\tau_{pp(P)} \leqslant \tau_P$ since $pp(P)$ is equal to P divided by an integer (the gcd of the integer coefficients). $\square$

PROOF OF PROPOSITION 10. The idea of the proof is to use the equations of Lemmas 9 and 7 which say, roughly speaking, that the polynomials of the RUR-candidate before specialization at $S = a$ are factors of the resultant $R(T, S)$ and some of its derivatives. The bounds are then derived using Lemma 11. More formally, we prove that the polynomials $f_I, f_{I,v} \in \mathbb{Q}[T, S]$, $v \in \{1, X, Y\}$ (see Equation (4)) have bitsize in $\widetilde{O}(d^2 + d\tau)$. We then specialize these polynomials at $S = a$ which yields the result.

Bitsize of f_I. We apply Lemma 11 to the primitive part of both sides of the equation $R(T, S) = L_R(S)f_I(T, S)$ of Lemma 9, where $R, L_R \in \mathbb{Z}[T, S]$, $f_I \in \mathbb{Q}[T, S]$ is monic with respect to T (see Equation (4)). By Lemma 3, R has bitsize in $\widetilde{O}(d(d+\tau))$ and degree at most $2d^2$ in each variable. Note that this directly implies that, when $L_R(a) \neq 0$, the bitsize of $f_{I,a}(T) = f_I(T, a) = R(T, a)/L_R(a)$ is in $\widetilde{O}(d^2\tau_a + d\tau)$. For any value of $L_R(a)$, we show that $f_I(T, S)$ has bitsize in $\widetilde{O}(d^2 + d\tau)$ and we specialize S by a afterward. Indeed, Lemma 12 implies that $pp(R)$ also has bitsize $\widetilde{O}(d(d + \tau))$. Since f_I is monic, $\tau_{f_I} \leqslant \tau_{pp(f_I)}$ which is, by Lemma 11, in $\widetilde{O}(d^2 + d\tau)$. Hence, f_I has bitsize in $\widetilde{O}(d^2 + d\tau)$ and its degree in each variable is at most that of R, that is $2d^2$.

Moreover, since f_I is monic (in T), the corresponding coefficient of $pp(f_I)$ is equal to the lcm of the denominators of the coefficients of f_I, which we denote by Lcm_{f_I}. It follows that $\tau_{Lcm_{f_I}} \leqslant \tau_{pp(f_I)}$ which we proved is in $\widetilde{O}(d^2 + d\tau)$.

Bitsize of $f_{I,v}$, $v \in \{1, Y\}$. We consider the equations of Lemma 7. These equations can be written as $\frac{\partial f_I}{\partial u}(T, S) = g_I(T, S)f_{I,v}(T, S)$ where u is T or S, and v is 1 or Y, respectively. We first bound the bitsize of one coefficient, ξ, of $f_{I,v}$ so that we can apply Lemma 12 which states that $\tau_{f_{I,v}} \leqslant \tau_\xi + \tau_{pp(f_{I,v})}$. We consider the leading coefficient ξ of $f_{I,v}$ with respect to the lexicographic order (T, S). Since g_I is monic in T (see Lemma 7), the leading coefficient (with respect to the same ordering) of the product $g_I f_{I,v} = \frac{\partial f_I}{\partial u}$ is ξ which thus has bitsize in $\widetilde{O}(\tau_{f_I})$ (since it is bounded by τ_{f_I} plus the log of the degree of f_I). It follows that $\tau_{f_{I,v}}$ is in $\widetilde{O}(d^2 + d\tau + \tau_{pp(f_{I,v})})$.

We now take the primitive part of the above equation (of Lemma 7), which gives $pp(\frac{\partial f_I}{\partial u}(T, S)) = pp(g_I(T, S))\, pp(f_{I,v}(T, S))$. By Lemma 11, $\tau_{pp(f_{I,v})}$ is in $\widetilde{O}(d^2+\tau_{pp(\frac{\partial f_I}{\partial u})})$. In order to bound the bitsize of $pp(\frac{\partial f_I}{\partial u})$ we multiply $\frac{\partial f_I}{\partial u}$ by Lcm_{f_I} so that it has integer coefficients (multiplying by a constant does not change the primitive part). The bitsize of $pp(\frac{\partial f_I}{\partial u}) = pp(Lcm_{f_I}\frac{\partial f_I}{\partial u})$ is thus at most that of $Lcm_{f_I}\frac{\partial f_I}{\partial u}$ which is bounded by the sum of the bitsizes of Lcm_{f_I} and

$\frac{\partial f_I}{\partial u}$. We proved that $\tau_{Lcm_{f_I}}$ and τ_{f_I} are in $\widetilde{O}(d^2 + d\tau)$, thus the bitsize of $pp(\frac{\partial f_I}{\partial u})$ is in $\widetilde{O}(d^2 + d\tau)$. It follows that $\tau_{pp(f_{I,v})}$ and $\tau_{f_{I,v}}$ are also in $\widetilde{O}(d^2 + d\tau)$ for $v \in \{1, Y\}$.

Bitsize of $f_{I,X}$. We obtain the bound for $f_{I,X}$ by symmetry. Similarly as we proved that $f_{I,Y}$ has bitsize in $\widetilde{O}(d^2 + d\tau)$, we get, by exchanging the role of X and Y in Equation (4) and Lemma 7, that $\sum_{\sigma \in V(I)} \mu_I(\sigma) X(\sigma) \prod_{\varsigma \in V(I), \varsigma \neq \sigma} (T - Y(\varsigma) - SX(\varsigma))$ has bitsize in $\widetilde{O}(d^2 + d\tau)$. This polynomial is of degree $O(d^2)$ in T and S, thus after replacing S by $\frac{1}{S}$ and then T by $\frac{T}{S}$, the polynomial is of degree $O(d^2)$ in T and $\frac{1}{S}$. We multiply it by S to the power of $\frac{1}{S}$ and obtain $f_{I,X}$ which is thus of bitsize $\widetilde{O}(d^2 + d\tau)$.

Specialization at $S = a$. To bound the bitsize of the polynomials of $RUR_{I,a}$ (Definition 4), it remains to evaluate the polynomials f_I and $f_{I,v}$, $v \in \{1, X, Y\}$, at the rational value $S = a$ of bitsize τ_a. Since these polynomials have degree in S in $O(d^2)$ and bitsize in $\widetilde{O}(d^2 + d\tau)$, it is straightforward that their specializations at $S = a$ have bitsize in $\widetilde{O}(d^2 + d\tau + d^2\tau_a) = \widetilde{O}(d^2\tau_a + d\tau)$.

RUR-candidate with integer coefficients. With the above notation, we set $l = Lcm(Lcm_{f_I}, Lcm_{f_{I,v}}, v \in 1, X, Y)$. Similarly as above, it is straightforward to prove that l has bitsize in $\widetilde{O}(d^2 + d\tau)$ and that the product of l with f_I and $f_{I,v}$, $v \in \{1, X, Y\}$ yields polynomials with integer coefficients of bitsize in $\widetilde{O}(d^2 + d\tau)$. Moreover, by Equation 4, these polynomials have degree in S bounded by d^2, therefore, multiplying their specialization at a by $l \times denom(a)^{d^2}$ where $denom(a)$ is the denominator of a, yields polynomials with integer coefficients. This concludes the proof, since $l \times denom(a)^{d^2}$ has bitsize in $\widetilde{O}(d^2\tau_a + d\tau)$. $\square$

It is known that there exists a separating form $X + aY$ with a an integer in $O(d^4)$. Moreover, such a separating form, with $a < 2d^4$, can be computed in $\widetilde{O}_B(d^8 + d^7\tau + d^5\tau^2)$ bit operations [4]. As a direct consequence of Propositions 6 and 10, we get the following result.

THEOREM 13. *Let $P, Q \in \mathbb{Z}[X, Y]$ be two coprime bivariate polynomials of total degree at most d and maximum bitsize τ. Given a separating form $X + aY$ with integer a of bitsize[3] $\widetilde{O}(1)$, the RUR of $\langle P, Q\rangle$ associated to a can be computed using Proposition 5 with $\widetilde{O}_B(d^7 + d^6\tau)$ bit operations. Furthermore, the polynomials of this RUR have degree at most d^2 and bitsize in $\widetilde{O}(d^2 + d\tau)$.*

4. APPLICATIONS

In this section, we present two important applications of the RUR, that is, computing boxes with rational coordinates that isolate the real solutions of the system and evaluating the sign of a bivariate polynomial at these solutions. For simplicity we focus on a parameterization given by a RUR, but the complexity results also hold for the classical one via subresultants.

We start by recalling the complexity of isolating the real roots of a univariate polynomial. Here, f denotes a univariate polynomial of degree d with integer coefficients of bitsize at most τ.

[3]By abuse of notation, $\widetilde{O}(1)$ refers to O of any polylogarithmic function in d in τ.

LEMMA 14 ([17, THEOREM 10]). *Let f be squarefree. Isolating intervals of all the real roots of f can be computed and refined up to a width less than 2^{-L} with $\widetilde{O}_B(d^3\tau + d^2L)$ bit operations.*

LEMMA 15 ([16, THEOREM 4]). *Let the minimum root separation bound of f (or simply the separation bound of f) be the minimum distance between two different complex roots of f: $sep(f) = \min_{\{\gamma, \delta \text{ roots of } f,\ \gamma \neq \delta\}} |\gamma - \delta|$. One has $sep(f) > 1/(2d^{d/2+2}(d2^\tau + 1)^d)$, hence $sep(f) > 2^{-\widetilde{O}(d\tau)}$.*

4.1 Computation of isolating boxes

Given a RUR of the ideal I, $\{f_{I,a}, f_{I,a,1}, f_{I,a,X}, f_{I,a,Y}\}$, isolating boxes for the real solutions can be computed by first computing isolating intervals for the real roots of the univariate polynomial $f_{I,a}$ and then, evaluating the rational fractions $\frac{f_{I,a,X}}{f_{I,a,1}}$ and $\frac{f_{I,a,Y}}{f_{I,a,1}}$ by interval arithmetic. However, for the simplicity of the proof, instead of evaluating by interval each of these fractions of polynomials, we compute the product of its numerator with the inverted denominator modulo $f_{I,a}$, and then evaluate this resulting polynomial on the isolating intervals of the real roots of $f_{I,a}$ (note that we obtain the same complexity bound if we directly evaluate the fractions, but the proof is rather technical, although not difficult). When these isolating intervals are sufficiently refined, the computed boxes are necessarily disjoint and thus isolating. The following proposition analyzes the bit complexity of this algorithm.

PROPOSITION 16. *Given a RUR of $\langle P, Q\rangle$, isolating boxes for the solutions of $\langle P, Q\rangle$ can be computed in $\widetilde{O}_B(d^8 + d^7\tau)$ bit operations, where d bounds the total degree of P and Q, and τ bounds the bitsize of their coefficients.*

PROOF. For every real solution α of $I = \langle P, Q\rangle$, let $J_{X,\alpha} \times J_{Y,\alpha}$ be a box containing it. A sufficient condition for these boxes to be isolating is that the width of every interval $J_{X,\alpha}$ and $J_{Y,\alpha}$ is less than half the separation bound of the resultant of P and Q with respect to X and Y, respectively. Such a resultant has degree at most $2d^2$ and bitsize in $\widetilde{O}(d\tau)$, and we furthermore have an explicit upper bound on this bitsize which is $2d(\tau + \log 2d + 1) + \log(2d^2 + 1) + 1$ [2, Proposition 8.46]. Lemma 15 thus yields an explicit lower bound of $2^{-\varepsilon}$ with ε in $\widetilde{O}(d^3\tau)$ on the separating bound of such a resultant. It is thus sufficient to analyze the complexity of computing, for every α, a box $J_{X,\alpha} \times J_{Y,\alpha}$ that contains α and such that the widths of these intervals are smaller than half of $2^{-\varepsilon}$.[4] For technical reasons, we require that the interval widths are smaller than $2^{-\varepsilon'}$ with $\varepsilon' = \varepsilon + 2$.

Given a RUR $\{f_{I,a}, f_{I,a,1}, f_{I,a,X}, f_{I,a,Y}\}$ of I, we first show how to modify the rational mapping induced by this RUR into a polynomial one. Second, we bound, in terms of the width of J_γ, the side length of the box obtained by interval arithmetic as the image of J_γ through the mapping. We will then deduce an upper bound on the width of J_γ that ensures that the side length of its box image is less than $2^{-\varepsilon'}$, and the result will follow.

Polynomial mapping. Since $f_{I,a}$ and $f_{I,a,1}$ are coprime (see Proposition 5), the rational mapping can be transformed

[4]For clarity, we use an explicit bound for ε but the refinement can be stopped when all the boxes are pairwise disjoint, independently of their side length, and without changing the overall complexity.

into a polynomial one by replacing $\frac{1}{f_{I,a,1}}$ by $\frac{1}{f_{I,a,1}} \mod f_{I,a}$. This polynomial mapping still maps the real roots of $f_{I,a}$ to those of I, since $\frac{1}{f_{I,a,1}}$ and $\frac{1}{f_{I,a,1}} \mod f_{I,a}$ coincide when $f_{I,a}$ vanishes (by Bézout's identity). This mapping can be computed in $\widetilde{O}_B(d^6 + d^5\tau)$ bit operations and leads polynomials with degree less than $4d^2$ and bitsize in $\widetilde{O}(d^4 + d^3\tau)$. Indeed, $f_{I,a}$ and $\frac{1}{f_{I,a,1}}$ have degree at most d^2 and bitsize $\widetilde{O}(d^2+d\tau)$ (Theorem 13), thus $\frac{1}{f_{I,a,1}} \mod f_{I,a}$ has bitsize in $\widetilde{O}(d^2(d^2 + d\tau))$ and it can be computed with $\widetilde{O}_B((d^2)^2(d^2 + d\tau))$ bit operations [20, Corollaries 11.11(ii) & 6.52]. Thus, its product with $f_{I,a,X}$ or $f_{I,a,Y}$ can be computed in complexity $\widetilde{O}_B(d^2(d^4 + d^3\tau))$ [20, Corollary 8.27]. The result follows since the degree of the inverse modulo $f_{I,a}$ is less than that of $f_{I,a}$ and all the polynomials of the RUR have degrees at most d^2 by Theorem 13.

Width expansion through interval arithmetic evaluation. We consider here exact interval arithmetic, that is, interval arithmetic where operations on the interval boundaries are done exactly (with arbitrary precision). Let $J = [a, b]$ be an interval with rational endpoints such that $\max(|a|, |b|) \leqslant 2^\sigma$ and let $f \in \mathbb{Z}[T]$ be a polynomial of degree d_f with coefficients of bitsize τ_f. Denoting the width of J by $w(J) = |b - a|$, $f(J)$ can be evaluated by interval arithmetic into an interval $f_\square(J)$ whose width is at most $2^{\tau_f + d_f\sigma} d_f^2 w(J)$ (see [7, Lemma 8]). In other words, if $w(J) \leqslant 2^{-\varepsilon' - \tau_f - d_f\sigma - 2\log d_f}$, then $w(f_\square(J)) \leqslant 2^{-\varepsilon'}$.

Computing isolating boxes. We now apply the previous property on the polynomials of the mapping evaluated on isolating intervals of $f_{I,a}$. We denote by d_f and τ_f the maximum degree and bitsize of the polynomials of the mapping; as shown above $d_f < 4d^2$ and $\tau_f \in \widetilde{O}(d^4 + d^3\tau)$.

The polynomial $f_{I,a}$ has bitsize in $\widetilde{O}(d^2 + d\tau)$ (Theorem 13), thus, by Cauchy's bound (see e.g. [21, §6.2]) and considering intervals of isolation for $f_{I,a}$ of widths upper bounded by some constant, we have that the maximum absolute value of the boundaries of the isolating intervals are smaller than 2^σ with $\sigma = \widetilde{O}(d^2 + d\tau)$. Now, if all isolating intervals of $f_{I,a}$ are of width less than $2^{-\varepsilon' - \tau_f - d_f\sigma - 2\log d_f}$, the above property implies that the boxes evaluated by the polynomial mapping have side width less than $2^{-\varepsilon'}$ and are hence isolating. By Lemma 1, the squarefree part of $f_{I,a}$ has degree $O(d^2)$ and bitsize $\widetilde{O}(d^2 + d\tau)$. Lemma 14 thus implies that, for all the real roots of $f_{I,a}$, isolating intervals of width less than $2^{-\varepsilon' - \tau_f - d_f\sigma - 2\log d_f} = 2^{-\widetilde{O}(d^4 + d^3\tau)}$ can be computed with $\widetilde{O}_B(d^8 + d^7\tau)$ bit operations.

It remains to evaluate by interval arithmetic the polynomials of the mapping which have degree $O(d^2)$ and bitsize $\widetilde{O}(d^4 + d^3\tau)$ on each of these $O(d^2)$ isolating intervals whose endpoints have bitsize at most in $\widetilde{O}(d^4 + d^3\tau)$. By Lemma 2, this can be done with $\widetilde{O}_B(d^2 d^2(d^4 + d^3\tau))$ bit operations. Therefore, we can compute isolating boxes for the solutions of $\langle P, Q\rangle$ in $\widetilde{O}_B(d^8 + d^7\tau)$ bit operations. $\square$

4.2 Sign evaluation

This section addresses the problem of computing the sign ($+, -$ or 0) of a given polynomial F at the solutions of a bivariate system defined by two polynomials P and Q. We consider in the following that all input polynomials P, Q, and F are in $\mathbb{Z}[X, Y]$ and have degree at most d and coefficients of bitsize at most τ. We assume without loss of generality that the bound d is *even*.

Once the RUR $\{f_{I,a}, f_{I,a,1}, f_{I,a,X}, f_{I,a,Y}\}$ of $I = \langle P, Q\rangle$ is computed, we can use it to translate a bivariate sign computation into a univariate sign computation. Indeed, let $F(X, Y)$ be the polynomial to be evaluated at the solution (α, β) of I that is the image of the root γ of $f_{I,a}$ by the RUR mapping. We define the polynomial $f_F(T)$ roughly as the numerator of the rational fraction obtained by substituting $X = \frac{f_{I,a,X}(T)}{f_{I,a,1}(T)}$ and $Y = \frac{f_{I,a,Y}(T)}{f_{I,a,1}(T)}$ in the polynomial $F(X, Y)$, so that the sign of $F(\alpha, \beta)$ is the same as that of $f_F(\gamma)$.

LEMMA 17. *The primitive part of $f_F(T) = f_{I,a,1}^d(T)F(T - aY, Y)$, with $Y = \frac{f_{I,a,Y}(T)}{f_{I,a,1}(T)}$, has degree $O(d^3)$, bitsize in $\widetilde{O}(d^3 + d^2\tau)$, and it can be computed with $\widetilde{O}_B(d^7 + d^6\tau)$ bit operations. The sign of F at a real solution of $I = \langle P, Q\rangle$ is equal to the sign of $pp(f_F)$ at the corresponding root of $f_{I,a}$.*

PROOF. We first compute the polynomial $F(T - aY, Y)$ in the form $\sum_{i=0}^d a_i(T)Y^i$. Then, $f_F(T)$ is equal to $\sum_{i=0}^d a_i(T)$ $f_{I,a,Y}(T)^i f_{I,a,1}(T)^{d-i}$. Thus, computing an expanded form of $f_F(T)$ can be done by computing the $a_i(T)$, the powers $f_{I,a,Y}(T)^i$ and $f_{I,a,1}(T)^i$, and their appropriate products and sum.

Computing $a_i(T)$. According to Lemma 3, $F(T - SY, Y)$ can be expanded with $\widetilde{O}_B(d^4 + d^3\tau)$ bit operations and its bitsize is in $\widetilde{O}(d+\tau)$. Then, $F(T - aY, Y)$ is obtained by substituting S by a. Writing $F(T - SY, Y) = \sum_{i=0}^d f_i(T, Y)S^i$, this substitution amounts to compute for each i, a^i and $f_i(T, Y)a^i$ and then, summing all the $f_i(T, Y)a^i$. The dominating bit complexity is that of computing all the $f_i(T, Y)a^i$ and it is in $\widetilde{O}_B(d^4 + d^3\tau)$.

Computing $f_{I,a,Y}(T)^i$ and $f_{I,a,1}(T)^i$. $f_{I,a,Y}(T)$ has degree $O(d^2)$ and bitsize $\widetilde{O}(d^2 + d\tau)$ (by Theorem 13), thus $f_{I,a,Y}(T)^i$ has degree in $O(d^3)$ and bitsize in $\widetilde{O}(d^3 + d^2\tau)$. Computing all the $f_{I,a,Y}(T)^i$ can be done with $O(d)$ multiplications between these polynomials. Every multiplication can be done with $\widetilde{O}_B(d^3(d^3 + d^2\tau))$ bit operations [20, Corollary 8.27], thus all the multiplications can be done with $\widetilde{O}_B(d^4(d^3 + d^2\tau))$ bit operations in total. It follows that all the $f_{I,a,Y}(T)^i$, and similarly all the $f_{I,a,1}(T)^i$, can be computed using $\widetilde{O}_B(d^7 + d^6\tau)$ bit operations and their bitsize is in $\widetilde{O}(d^3 + d^2\tau)$.

Computing $f_F(T)$. Computing, for $i = 0, \ldots, d$, all $a_i(T)\, f_{I,a,Y}(T)^i\, f_{I,a,1}(T)^{d-i}$ amounts to multiplying $O(d)$ times, univariate polynomials of degree $O(d^3)$ and bitsize $\widetilde{O}(d^3 + d^2\tau)$, which can be done, similarly as above, with $\widetilde{O}(d^7 + d^6\tau)$ bit operations. Finally, their sum is the sum of d univariate polynomials of degree $O(d^3)$ and bitsize $\widetilde{O}(d^3 + d^2\tau)$, which can also be computed within the same bit complexity. Hence, $f_F(T)$ can be computed with $\widetilde{O}(d^7 + d^6\tau)$ bit operations and its coefficients have bitsize in $\widetilde{O}(d^3 + d^2\tau)$.

Primitive part of $f_F(T)$. By Proposition 10, there exists an integer r of bitsize in $\widetilde{O}(d^2 + d\tau)$ such that its product with the RUR polynomials gives polynomials in $\mathbb{Z}[T]$ of bitsize in $\widetilde{O}(d^2 + d\tau)$. We consider the polynomial $r^d f_F(T) = (r f_{I,a,1}(T))^d F(T - aY, Y)$ with $Y = \frac{r f_{I,a,Y}(T)}{r f_{I,a,1}(T)}$. This polynomial has its coefficients in $\mathbb{Z}$ since $r f_{I,a,Y}(T)$ and $r f_{I,a,1}(T)$

are in $\mathbb{Z}[T]$. Moreover, since $rf_{I,a,Y}(T)$ and $rf_{I,a,1}(T)$ have bitsize in $\widetilde{O}(d^2 + d\tau)$, $r^d f_F(T)$ can be computed, similarly as above, in $\widetilde{O}_B(d^7 + d^6\tau)$ and it has bitsize in $\widetilde{O}(d^3 + d^2\tau)$. The primitive part of $f_F(T)$ has also bitsize in $\widetilde{O}(d^3 + d^2\tau)$ (since it is smaller than or equal to that of $r^d f_F(T)$) and it can be computed from $r^d f_F(T)$ with $\widetilde{O}_B(d^3(d^3 + d^2\tau))$ bit operations by computing $O(d^3)$ gcd of coefficients of bitsize $\widetilde{O}(d^3 + d^2\tau)$ [21, §2.A.6].

Signs of F and f_F. By Definition 4, there is a one-to-one mapping between the roots of $f_{I,a}$ and those of $I = \langle P, Q\rangle$ that maps a root γ of $f_{I,a}$ to a solution $(\alpha, \beta) = (\frac{f_{I,a,X}(\gamma)}{f_{I,a,1}(\gamma)}, \frac{f_{I,a,Y}(\gamma)}{f_{I,a,1}(\gamma)})$ of I such that $\gamma = \alpha + a\beta$ and $f_{I,a,1}(\gamma) \neq 0$. For any such pair of γ and (α, β), $f_F(\gamma) = f^d_{I,a,1}(\gamma)F(\gamma - a\frac{f_{I,a,Y}(\gamma)}{f_{I,a,1}(\gamma)}, \frac{f_{I,a,Y}(\gamma)}{f_{I,a,1}(\gamma)})$ by definition of $f_F(T)$, and thus $f_F(\gamma) = f^d_{I,a,1}(\gamma)F(\alpha, \beta)$. It follows that $f_F(\gamma)$ and $F(\alpha, \beta)$ have the same sign since $f_{I,a,1}(\gamma) \neq 0$ and d is even by hypothesis. □

An algorithm for evaluating the sign of a univariate polynomial (here f_F) at the roots of a squarefree univariate polynomial (here $\overline{f_{I,a}}$) is analysed in [8, Corollary 5, Lemma 7]. The idea of this algorithm comes originally from [12], where the Cauchy index of two polynomials is computed by means of sign variations of a particular remainder sequence called the Sylvester-Habicht sequence. In [8], this approach is slightly adapted to deduce the sign from the Cauchy index ([21, Thm. 7.3]) and the bit complexity is given in terms of the two initial degrees and bitsizes. Unfortunately, the corresponding proof is problematic because the authors refer to two complexity results for computing parts of the Sylvester-Habicht sequences and none of them actually applies. Their approach is however correct in spirit and we state below a corrected (weaker) version of their complexity result, see [3] for details.

LEMMA 18. *Let $f \in \mathbb{Z}[X]$ be a squarefree polynomial of degree d_f and bitsize τ_f, and (a, b) be an isolating interval of one of its real roots γ with a and b distinct rationals of bitsize in $\widetilde{O}(d_f\tau_f)$ and $f(a)f(b) \neq 0$. Let $g \in \mathbb{Z}[X]$ be of degree d_g and bitsize τ_g. The sign of $g(\gamma)$ can be computed in $\widetilde{O}_B((d_f^3 + d_g^2)\tau_f + (d_f^2 + d_f d_g)\tau_g)$ bit operations. The sign of g at all the real roots of f can be computed with $\widetilde{O}_B((d_f^3 + d_f^2 d_g + d_g^2)\tau_f + (d_f^3 + d_f d_g)\tau_g)$ bit operations.*

THEOREM 19. *Given a RUR $\{f_{I,a}, f_{I,a,1}, f_{I,a,X}, f_{I,a,Y}\}$ of $I = \langle P, Q\rangle$ (satisfying the bounds of Theorem 13), the sign of F at a real solution of I can be computed with $\widetilde{O}_B(d^8 + d^7\tau)$ bit operations. The sign of F at all the solutions of I can be computed with $\widetilde{O}_B(d^9 + d^8\tau)$ bit operations.*

PROOF. By Lemma 17, the sign of F at the real solutions of I, is equal to the sign of $pp(f_F)$ at the corresponding roots of $pp(\overline{f_{I,a}})$. By Theorem 13 and Proposition 10, $f_{I,a}$ has degree at most d^2 and its primitive part has bitsize in $\widetilde{O}(d^2 + d\tau)$. Its primitive squarefree part $pp(\overline{f_{I,a}})$ can thus be computed in $\widetilde{O}_B(d^4(d^2 + d\tau))$ bit operations and has bitsize in $\widetilde{O}(d^2 + d\tau)$, by Lemma 1. By Lemmas 14 and 15, the isolating intervals (if not given) of $pp(\overline{f_{I,a}})$ can be computed in $\widetilde{O}_B((d^2)^3(d^2 + d\tau))$ bit operations with intervals boundaries of bitsize satisfying the hypotheses of Lemma 18. Applying this lemma then concludes the proof. □

5. REFERENCES

[1] M.-E. Alonso, E. Becker, M.-F. Roy, and T. Wörmann. Multiplicities and idempotents for zerodimensional systems. In *Algorithms in Algebraic Geometry and Applications*, vol. 143 of *Progress in Mathematics*, pp. 1–20, 1996.

[2] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in Real Algebraic Geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, 2006.

[3] Y. Bouzidi, S. Lazard, M. Pouget, and F. Rouillier. Rational Univariate Representations of Bivariate Systems and Applications. Research Report RR-8262, INRIA, 2013.

[4] Y. Bouzidi, S. Lazard, M. Pouget, and F. Rouillier. Separating linear forms for bivariate systems. In Proc. *ISSAC*, 2013.

[5] L. Busé, H. Khalil, and B. Mourrain. Resultant-based methods for plane curves intersection problems. In *Computer Algebra in Scientific Computing (CASC)*, vol. 3718 of *LNCS*, pp. 75–92, 2005.

[6] J. Canny. A new algebraic method for robot motion planning and real geometry. In Proc. *FoCS*, pp. 39–48, 1987.

[7] J. Cheng, S. Lazard, L. Peñaranda, M. Pouget, F. Rouillier, and E. Tsigaridas. On the topology of real algebraic plane curves. *Mathematics in Computer Science*, 4:113–137, 2010.

[8] D. I. Diochnos, I. Z. Emiris, and E. P. Tsigaridas. On the asymptotic and practical complexity of solving bivariate systems over the reals. *J. Symb. Comput.*, 44(7):818–835, 2009.

[9] P. Emeliyanenko and M. Sagraloff. On the complexity of solving a bivariate polynomial system. In Proc. *ISSAC*, pp. 154–161, 2012.

[10] W. Fulton. *Algebraic curves: an introduction to algebraic geometry*. 2008. `http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf`

[11] L. González-Vega and M. El Kahoui. An improved upper complexity bound for the topology computation of a real algebraic plane curve. *J. of Complexity*, 12(4):527–544, 1996.

[12] T. Lickteig and M.-F. Roy. Sylvester-Habicht Sequences and Fast Cauchy Index Computation. *J. Symb. Comput.*, 31(3):315–341, 2001.

[13] M. Mignotte. *Mathématiques pour le calcul formel*. Presses Universitaires de France, 1989.

[14] V. Y. Pan. Solving a polynomial equation: some history and recent progress. *SIAM Review*, 39(2):187–220, 1997.

[15] F. Rouillier. Solving zero-dimensional systems through the rational univariate representation. *J. of Applicable Algebra in Engineering, Communication and Computing*, 9(5):433–461, 1999.

[16] S. M. Rump. Polynomial minimum root separation. *Mathematics of Computation*, 33(145):327–336, 1979.

[17] M. Sagraloff. When Newton meets Descartes: A Simple and Fast Algorithm to Isolate the Real Roots of a Polynomial. In Proc. *ISSAC*, pp.297–304 2012.

[18] E. Schost. *Sur la Résolution des Systèmes Polynomiaux à Paramètres*. PhD thesis, Ecole Polytechnique, France, 2001.

[19] A. Schönhage. The fundamental theorem of algebra in terms of computational complexity. Manuscript, 1982.

[20] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge Univ. Press, Cambridge, U.K., 2003.

[21] C. Yap. *Fundamental Problems of Algorithmic Algebra*. Oxford University Press, Oxford-New York, 2000.