Degree bounds and lifting techniques for triangular sets

Éric Schost, Laboratoire GAGE, École polytechnique
91128 Palaiseau, France
Eric.Schost@polytechnique.fr

ABSTRACT

We study the representation of the solutions of a polynomial system by triangular sets, and concentrate on the positive-dimensional case. We reduce to dimension zero by placing the free variables in the base-field, so the solutions can be represented by triangular sets with coefficients in a rational function field. First, we give bounds on the degree of these coefficients; then we show how to apply lifting techniques in this context, and point out the role played by the evaluation properties of the input system. Our algorithms are implemented in Magma; we present two applications.

1. MAIN RESULTS

We first define triangular sets over a ring A. A *triangular set* is a family of polynomials $T = (T_1, \ldots, T_n)$ in $A[X_1, \ldots, X_n]$ such that, for $k \leq n$: T_k depends only on $(X_1, \ldots, X_k)$, T_k is *monic* of degree $d_k > 0$ in X_k and T_k has degree in X_j less than d_j, for $j < k$. We let (T) denote the ideal generated by T. Let now $\mathcal{K}$ be a field, $\mathcal{V} \subset \mathbb{A}^n(\overline{\mathcal{K}})$ a *zero-dimensional* algebraic set defined over $\mathcal{K}$; a family $\{T^1, \ldots, T^P\}$ of triangular sets with coefficients in $\mathcal{K}$ *represents* the zeros of $\mathcal{V}$ if $\mathcal{I}(\mathcal{V}) = \cap_{i \leq P}(T^i)$, and if for $i \neq j$, T^i and T^j have no common zero. Then all (T^i) are radical ideals.

Our definition is inspired by that of reduced triangular sets in [18]. If $\mathcal{V}$ is irreducible, the family we seek exists, is unique and reduced to a single triangular set; then $\prod_{k \leq n} \deg_{X_k} T_k$ is the cardinality of $\mathcal{V}$. If $\mathcal{V}$ is not irreducible, a family $\{T^1, \ldots, T^P\}$ satisfying our conditions exists but is not unique [18, Prop. 2 and Rem. 1]; then $\sum_{i \leq P} \prod_{k \leq n} \deg_{X_k} T_k^i$ is the cardinality of $\mathcal{V}$. If X_1 separates the points in $\mathcal{V}$, we obtain a representation by primitive element, called geometric resolution after [12, 10, 11, 13].

For a positive dimensional variety $\mathcal{V} \subset \mathbb{A}^N(\overline{\mathcal{K}})$, several notions of triangular sets exist [16, 19, 3, 6, 24]. In this situation, *we choose to reduce to dimension zero*, by considering a projection of $\mathcal{V}$ on a suitable linear space L. We require the projection $\mathcal{V} \to L$ to be *dominant with generically finite fibers*. As a motivation, note that many questions in polynomial systems solving are of parametric nature: the systems come with distinguished variables, some *parameters*, and admit a finite number of solutions for a generic value of the parameters. Such situations are zero-dimensional over the field of functions on the parameter-space L.

We formalize this situation the following way. We consider a m-dimensional variety $\mathcal{V} \subset \mathbb{A}^{m+n}(\overline{\mathcal{K}})$, defined over $\mathcal{K}$. Let $\{\mathcal{V}_i\}_{i \in I}$ denote the $\mathcal{K}$-irreducible components of $\mathcal{V}$, and π the projection $\mathbb{A}^{m+n}(\overline{\mathcal{K}}) \to \mathbb{A}^m(\overline{\mathcal{K}})$. Our main assumption, already done in [22], is that the image by π of each $\mathcal{V}_i$ is dense in $\mathbb{A}^m(\overline{\mathcal{K}})$. Then the fibers of π are generically finite.

We denote by $P = P_1, \ldots, P_m$ the first m coordinates, and by $X = X_1, \ldots, X_n$ the last coordinates in $\mathbb{A}^{m+n}(\overline{\mathcal{K}})$; the variables P are called *parameters*. Let $\mathcal{I} \subset \overline{\mathcal{K}}[P, X]$ be the radical ideal defining $\mathcal{V}$, $\mathcal{I}_P$ its extension in $\overline{\mathcal{K}}(P)[X]$ and A_P the quotient $\overline{\mathcal{K}}(P)[X]/\mathcal{I}_P$. Our first assumption implies that A_P is a finite dimensional $\overline{\mathcal{K}}(P)$-algebra. Our second assumption is that the extension $\overline{\mathcal{K}}(P) \to A_P$ is separable. By [14, Prop. 1], its dimension is the generic number of points in the fibers of $\pi_{|\mathcal{V}}$, which will be denoted by $\deg \pi$.

We call *generic zeros* of $\mathcal{V}$ the roots of $\mathcal{I}_P$. Since they are in finite number, they can be represented by a family of triangular sets in $\mathcal{K}(P)[X]$. If $\{T^1, \ldots, T^P\}$ is such a family, $\sum_{i \leq P} \prod_{k \leq n} \deg_{X_k} T_k^i$ equals $\deg \pi$ by the above discussion.

Our first result is a bound on the degrees in $(P_1, \ldots, P_m)$ of the coefficients of such triangular sets, using the geometric notion of degree introduced in [14].

THEOREM 1. *Let $\mathcal{W}$ be the reunion of some of the irreducible components of $\mathcal{V}$, defined over $\mathcal{K}$, such that the generic zeros of $\mathcal{W}$ can be represented by a single triangular set $T = (T_1, \ldots, T_n)$, with $T_k \in \mathcal{K}(P)[X]$ for $k \leq n$. For $k \leq n$, denote by $\mathcal{W}_k \subset \mathbb{A}^{m+k}(\overline{\mathcal{K}})$ the projection of $\mathcal{W}$ on $\mathbb{A}^{m+k}(\overline{\mathcal{K}})$ and by $\mathcal{D}_k$ its degree. Then all coefficients of T_k are rational functions in $\mathcal{K}(P)$ of degree at most*

$$(2k^2 + 4k + 3)^{k+1}\mathcal{D}_k^{2k+3}.$$

This is in the continuity of the results of Gallo-Mishra [7] and Szanto [24] for Ritt-Wu's and Kalkbrener's unmixed representations. If $\mathcal{V}$ is given as the zero-set of a system of n equations of degree d, Gallo-Mishra's bound is $2n(8n)^{2n}d(d+1)^{4n^2}$ and Szanto's is $d^{O(n^2)}$.

With this notation, the Bézout inequality of [14] implies that $\mathcal{D}_k$ is at most d^n for all k. Thus according to Theorem 1, in a worst-case scenario the degrees of the coefficients in the triangular set $(T_1, \ldots, T_n)$ are bounded by $81d^{5n}$ for T_1, $6859d^{7n}$ for T_2, $\ldots$, $(2n^2+n+3)^{n+1}d^{n^2+3n}$ for T_n. This improves the previous results, which gave the same bounds for *all* T_k; yet we do not know if these bounds are sharp.

Another new feature is that our bounds are given in terms of the intrinsic geometric quantities $\mathcal{D}_k$, which may be bounded *a priori*. In the example presented in Section 4.2, the Bézout bound is 1024, but an *a priori* estimate based on the semantics of the problem gives $\mathcal{D}_k \leq 80$.

The second part of this article presents lifting techniques for triangular sets. We restrict the context to a variety $\mathcal{V}$ given as the zero-set of a system $F = F_1, \ldots, F_n$ with indeterminates $(P, X) = (P_1, \ldots, P_m, X_1, \ldots, X_n)$, with the additional assumption that the Jacobian determinant w.r.t. X is invertible on an open subset of $\mathcal{V}$. Then the previous two assumptions are satisfied, and we want to compute triangular sets in $\mathcal{K}(P)[X]$ that represent the generic zeros of $\mathcal{V}$.

The underlying paradigm is that solving a zero-dimensional system over $\mathcal{K}$ by means of triangular sets is a well-solved task. Thus, the basic idea is first to specialize the indeterminates P in the system F, and solve the corresponding system in the remaining variables X, by means of triangular sets in $\mathcal{K}[X]$. A lifting process then produces triangular sets with coefficients in a formal power series ring, from which we can recover the required information.

We do not give a full algorithm. Difficulties arise when recombining factorized triangular sets, so our first contribution treats the case when $\mathcal{V}$ is irreducible: its generic zeros are represented by a single triangular set $T = (T_1, \ldots, T_n)$, and we propose an algorithm that computes $T_1, \ldots, T_k$ for any k. If $\mathcal{V}$ is not irreducible, we compute the *minimal polynomial* of X_1 in A_P, which can be read off triangular sets.

The *complexity of evaluation* of the system F plays a crucial role here: F is given by a *Straight-Line Program* of size L. In the sequel, $M(d, m)$ is the number of monomials of degree at most d in m variables, and C a universal constant, see Section 3.2. The algorithms are probabilistic in the choice of the points $\mathbf{p}$, $\mathbf{p}'$ below: the choices leading to an error are enclosed in a strict algebraic subset of $\mathbb{A}^{2m}(\overline{\mathcal{K}})$. The degree analysis of this subset is done for Theorem 3 in [23, Ch. 18, 19], and has to be done for Theorem 2.

The following results were improved from an earlier version thanks to the anonymous referees' comments. All complexities are stated in terms of number of operations in $\mathcal{K}$.

Theorem 2. *Assume that $\mathcal{V}$ is irreducible. Let $\mathbf{p}, \mathbf{p}'$ be generic enough points in $\mathcal{K}^m$; assume that a description of the zeros of the systems $F(\mathbf{p}, X)$, $F(\mathbf{p}', X)$ by triangular sets is available. Let T be the triangular set in $\mathcal{K}(P)[X]$ that represents the generic zeros of $\mathcal{V}$, choose $k \leq n$ and let $\mathfrak{D}_k$ be the maximal degree in P of the coefficients of $T_1, \ldots, T_k$. Then $T_1, \ldots, T_k$ can be computed by a probabilistic algorithm in time polynomial in $L, C^n, \deg \pi, M(\mathfrak{D}_k, m)$.*

Theorem 3. *Let $\mathbf{p}, \mathbf{p}'$ be generic enough points in $\mathcal{K}^m$, and assume that a description of the zeros of the systems $F(\mathbf{p}, X)$, $F(\mathbf{p}', X)$ by triangular sets which define prime ideals is available. Let $M_1 \in \mathcal{K}(P)[X_1]$ be the minimal polynomial of X_1 in A_P, and $\mathfrak{D}_1$ the maximal degree in P of its coefficients. Then M_1 can be computed by a probabilistic algorithm in time polynomial in $L, C^n, \deg \pi, M(\mathfrak{D}_1, m)$.*

This work was greatly motivated by applications. The first accounts for computations done in [9] to study genus 2 curves with (2,2)-split Jacobian, which occur frequently in number theory. The second shows how to compute the modular equations for hyperelliptic curves defined in [8, 23] with a view towards applications in cryptography; our result is now used within Magma's hyperelliptic curve package [1].

Comparison with primitive elements techniques.

The present results are in the continuation of [22], which focuses on a representation by primitive elements, under the same hypotheses. Caution must be taken when comparing the two approaches. They answer different needs; as such, their complexities cannot be compared directly, since they are stated in terms of different quantities.

Assume for simplicity that the generic zeros of $\mathcal{V}$ are represented by a single triangular set. The degree bound in a geometric resolution is *linear* in the degree of $\mathcal{V}$, see Proposition 1 below. On the other hand, using a primitive element, we cannot take into account the degrees of the *projections* of $\mathcal{V}$, which can be arbitrarily smaller than the degree of $\mathcal{V}$. This refinement makes the interest of the triangular representation, using results such as Theorem 1.

Consider now the algorithmic aspect. The algorithm in [22] computes a generic geometric resolution in time polynomial in $L, \deg \pi, M(\deg \mathcal{V}, m)$, where $\deg \mathcal{V}$ is the degree of $\mathcal{V}$. Here, using Theorem 1, the complexity in Theorems 2 and 3 is seen to depend on the degree of the *projections* of $\mathcal{V}$ on the spaces of coordinates $(P, X_1, \ldots, X_k)$ for Theorem 2, or (P, X_1) for Theorem 3, but *not on the degree of $\mathcal{V}$ itself*, which can be arbitrarily bigger.

Thus, the present approach takes more refined complexity measures into account. It will prove of interest for structured problems, when a partial information (e.g. a minimal polynomial) is wanted: the computational cost will not depend on the whole degree of $\mathcal{V}$, as when using a primitive element, but only on that of a suitable projection, which might turn out to be smaller. The applications in Section 4 are examples of this phenomenon, and illustrate the practical interest of our approach in this situation. Their study inspired this work in the first place.

Related results.

In dimension zero, a landmark paper for the representation by triangular sets is [18]. In arbitrary dimension, several notions and algorithms exist, see [16, 19, 3, 6, 24], and [4] for a comparison of some of them. Our choice to reduce the question to dimension zero over a field of rational functions yields algorithms with good complexity, and easy to implement. Yet, our output is not as strong as for instance [19, 6], since it is only *generically* valid.

An important feature of our algorithms is the representation of the input system by *evaluation*. This approach proved successful for solving systems by primitive element techniques, in a series of articles by the TERA group, see [12, 10, 11, 13] and references therein. In particular the article [15], with a similar approach but under more restrictive hypotheses, inspired [22] and the present work. Finally, parallel arithmetic circuits are used for triangular sets in [24].

Notation.

The letter T denotes a triangular set $(T_1, \ldots, T_n)$. A family of triangular sets is denoted with superscripts as $T^1, \ldots, T^P$, each T^i being a triangular set $(T_1^i, \ldots, T_n^i)$. The letter X stands for $X_1, \ldots, X_n$, and P for $P_1, \ldots, P_m$. Bold letters denote matrices or vectors. Finally, $\mathcal{I}_P$ is an ideal in $\overline{\mathcal{K}}(P)[X]$, and A_P the corresponding quotient algebra.

2. DEGREE BOUNDS

Representation by primitive elements.

The following is a variation on the Primitive Element Theorem. The version we use is a slight extension of [22, Prop. 2], and applies under the assumptions of Section 1; it is inspired by [12, 21].

PROPOSITION 1. *There exists $(u_1, \ldots, u_n) \in \overline{\mathcal{K}}^n$ such that $u_0 := \sum_{i=1}^n u_i X_i$ generates A_P. Besides, there exists some polynomials $V, V_1, \ldots, V_n$ in $\overline{\mathcal{K}}[P][U]$ such that*

- *the total degrees of $V, V_1, \ldots, V_n$, seen in $\overline{\mathcal{K}}[P, U]$, are bounded by $\deg \mathcal{V}$;*
- *$V'(u_0)$ is invertible in A_P, the relations*

  $$V(u_0) = 0, \quad V'(u_0)X_i = V_i(u_0) \ (1 \le i \le n)$$

  hold in A_P, so the ideal $\mathcal{I}_P + (U - u_0)$ coincides with

  $$V(U), V'(U)X_1 - V_1(U), \ldots, V'(U)X_n - V_n(U) \ .$$

Effective Bézout bound.

The following is Lemma 5 in [17]; similar results can be seen in [10], originating from [12]. As pointed out by a referee, a bound similar to Theorem 1 can be obtained without this result, by working out an explicit division procedure.

PROPOSITION 2. *Let $\mathfrak{K}$ be a field, and $(F_1, \ldots, F_N)$ a regular sequence in $\mathfrak{K}[Y_1, \ldots, Y_N]$. Let d be a bound on the degrees of the polynomials F, and δ the maximum of the degrees of the varieties $\mathcal{V}(F_1, \ldots, F_i)$, for $i = 1, \ldots, N-1$. For $i = 0, \ldots, N-1$, let B_i be the quotient*

$$\mathfrak{K}[Y_1, \ldots, Y_N]/(F_1, \ldots, F_{N-i}).$$

Assume that the extension $\mathfrak{K}[Y_1, \ldots, Y_i] \to B_i$ is integral and that the jacobian of $(F_1, \ldots, F_{N-i})$ w.r.t. $(Y_{i+1}, \ldots, Y_N)$ is a non-zero divisor in B_i. Then if H belongs to $(F_1, \ldots, F_N)$, there exists polynomials $(Q_1, \ldots, Q_N)$ in $\mathfrak{K}[Y_1, \ldots, Y_N]$ such that $H = Q_1F_1 + \cdots + Q_NF_N$, and, for $i = 1, \ldots, N$, $\deg Q_iF_i \le 2N^2d\delta + \delta \max\{\deg H, d\}$.

Proof of Theorem 1.

Let $\mathcal{W}$ be the reunion of some of the irreducible components of $\mathcal{V}$, such that the generic zeros of $\mathcal{W}$ can be represented by a single triangular set $T = (T_1, \ldots, T_n)$. For $k \le n$, denote by $\mathcal{W}_k \subset \mathbb{A}^{m+k}(\overline{\mathcal{K}})$ the projection of $\mathcal{W}$ on $\mathbb{A}^{m+k}(\overline{\mathcal{K}})$ and by $\mathcal{D}_k$ its degree. We now prove that all coefficients in T_k are of degree bounded by $(2k^2 + 4k + 3)^{k+1}\mathcal{D}_k^{2k+3}$.

Let $\mathcal{J} \subset \overline{\mathcal{K}}[P, X]$ be the ideal defining $\mathcal{W}$, $\mathcal{J}_P$ its extension in $\overline{\mathcal{K}}(P)[X]$, and B_P the algebra $\overline{\mathcal{K}}(P)[X]/\mathcal{J}_P$. Since A_P is a separable extension of $\overline{\mathcal{K}}(P)$, so is B_P. Also, by definition of T, $\mathcal{J}_P$ is the ideal generated by $T = (T_1, \ldots, T_n)$ in $\overline{\mathcal{K}}(P)[X]$.

Denote by $X_{\le k}$ the variables $X_1, \ldots, X_k$, $\mathcal{J}_{\le k} \subset \overline{\mathcal{K}}[P, X_{\le k}]$ the ideal defining $\mathcal{W}_k$, that is, $\mathcal{J} \cap \overline{\mathcal{K}}[P, X_{\le k}]$, and $\mathcal{J}_{P,\le k}$ its extension in $\overline{\mathcal{K}}(P)[X_{\le k}]$. Under our first assumption that none of the prime components of $\mathcal{I}$ contains a polynomial in $\overline{\mathcal{K}}[P]$, it is a routine check that $\mathcal{J}_{P,\le k} = \mathcal{J}_P \cap \overline{\mathcal{K}}(P)[X_{\le k}]$, i.e. the ideal generated by $(T_1, \ldots, T_k)$ in $\overline{\mathcal{K}}(P)[X_{\le k}]$. Besides, since $\overline{\mathcal{K}}(P) \to B_P$ is separable, it is also the case for $\overline{\mathcal{K}}(P) \to \overline{\mathcal{K}}(P)[X_{\le k}]/\mathcal{J}_{P,\le k}$.

Thus $\mathcal{W}_k$ satisfies the hypotheses of Proposition 1, so, using a new variable U, there exist scalars $u_1, \ldots, u_k$ in $\overline{\mathcal{K}}^k$, and polynomials $V, V_1, \ldots, V_k$ such that the ideal generated by T_k and $U - \sum_{i=1}^k u_k X_k$ in $\overline{\mathcal{K}}(P)[X_{\le k}, U]$ coincides with

$$V(U), V'(U)X_k - V_k(U), \ldots, V'(U)X_1 - V_1(U) \ .$$

Let us consider the systems

$$\mathcal{S} = \ V(U), V'(U)X_k - V_k(U), \ldots, V'(U)X_1 - V_1(U) \ ,$$

and for $0 \le i \le k$,

$$\mathcal{S}_i = \ V(U), V'(U)X_k - V_k(U), \ldots, V'(U)X_{i+1} - V_{i+1}(U) \ ,$$

in $\overline{\mathcal{K}}(P)[X_{\le k}, U]$. We check that the hypotheses of Proposition 2 are satisfied for $\mathcal{S}$, with $\mathfrak{K} = \overline{\mathcal{K}}(P)$, $N = k + 1$, and $Y_1, \ldots, Y_N = X_1, \ldots, X_k, U$. By Proposition 1, $V'(U)$ is invertible modulo $V(U)$. Thus modulo $V(U)$, each equation $V'(U)X_j - V_j(U)$ can be written $X_j - W_j(U)$, for some polynomial $W_j(U)$ in $\overline{\mathcal{K}}(P)[U]$.

This shows that $\mathcal{S}$ is a regular sequence. For i in $0, \ldots, k$, the ring B_i in Proposition 2 is $\overline{\mathcal{K}}(P)[X_{\le k}, U]/\mathcal{S}_i$, which is an integral extension of $\overline{\mathcal{K}}(P)[X_1, \ldots, X_i]$. Finally, the jacobian determinant of $\mathcal{S}_i$ with respect to $X_{i+1}, \ldots, X_k, U$ is the $(k-i)$-th power of $V'(U)$, so it is invertible in B_i. Consequently, the hypotheses of Proposition 2 are satisfied. Since the variables P are in the basefield $\mathfrak{K} = \overline{\mathcal{K}}(P)$, we estimate all degrees in terms of the variables $(X_{\le k}, U)$ only. By Proposition 1, the degrees of all polynomials in $\mathcal{S}$ are bounded by $\mathcal{D}_k$. The varieties $\mathcal{V}(\mathcal{S}_i)$ are cylinders built upon zero-dimensional varieties of degree at most $\mathcal{D}_k$ over $\overline{\mathfrak{K}}$, so their degree over $\overline{\mathfrak{K}}$ is at most $\mathcal{D}_k$.

All polynomials $T_1, \ldots, T_k$ belong to the ideal generated by $\mathcal{S}$. Consequently, for $i \le k$, there exist some polynomials $Q_{0,i}, \ldots, Q_{k,i}$ in $\overline{\mathcal{K}}(P)[X_{\le k}, U]$ such that the equality

$$T_i = Q_{0,i}V(U) + \sum_{j=1}^{k} Q_{j,i} \ V'(U)X_i - V_i(U) \qquad (1)$$

holds in $\overline{\mathcal{K}}(P)[X_{\le k}, U]$.

Let us fix i, and apply Proposition 2. Our Conventions on the elements of a triangular set show that the degree of T_i in $X_1, \ldots, X_k$ is at most $\mathcal{D}_k$. Proposition 2 then shows that the degree in $X_1, \ldots, X_k$ of each summand in (1) can be taken less than $2(k+1)^2\mathcal{D}_k^2 + \mathcal{D}_k^2 = (2k^2+4k+3)\mathcal{D}_k^2$.

The conclusion is now similar to that of [7]. Writing $T_i = X_i^{d_i} + R_i$, with $\deg_{X_i} R_i < d_i$, identity (1) can be rewritten

$$X_i^{d_i} = -R_i + Q_{0,i}V(U) + \sum_{j=1}^{k} Q_{j,i} \ \ V'(U)X_i - V_i(U) \ .$$

This in turn can be rewritten as a linear system in the coefficients of $R_i, Q_{0,i}, \ldots, Q_{k,i}$. Let G be the number of monomials in $k+1$ variables of degree at most $(2k^2+4k+3)\mathcal{D}_k^2$, and let $G' \leq G$ be the number of unknown coefficients in R_i. This system can be written $MA = B$, where A is the vector of $(k+1)G+G'$ unknowns, and B is the zero vector, except for one entry equal to 1, corresponding to the coefficient of $X_i^{d_i}$. The matrix M has G rows and $(k+1)G+G'$ columns, and its entries are either the constant 1, or the coefficients of $V, V', V_1, \ldots, V_n$. These are polynomials in $(P_1, \ldots, P_m)$ of degree at most $\mathcal{D}_k$, by Proposition 1.

The coefficients of R_i are uniquely determined: if there were two possible choices for R_i, then their difference would yield a polynomial in the ideal generated by the system $\mathcal{S}$ of degree less than d_i in X_i, an impossibility. Consequently, by Rouché-Fontené's Theorem, the coefficients of R_i can be expressed as quotients of determinants of size at most G, with entries that are polynomials in $P_1, \ldots, P_m$ of degree at most $\mathcal{D}_k$. Then their numerators and denominators have degree at most $G\mathcal{D}_k$, which is bounded by $(2k^2+4k+3)^{k+1}\mathcal{D}_k^{2k+3}$. This concludes the proof of Theorem 1.

3. LIFTING TECHNIQUES

We now present some lifting techniques for triangular sets. This requires a stronger assumption than before: $\mathcal{V}$ is now supposed to be defined by some polynomials $F = F_1, \ldots, F_n$ in $\mathcal{K}[P, X]$, where $P = P_1, \ldots, P_m$ and $X = X_1, \ldots, X_n$. Furthermore, we assume that the jacobian determinant of F with respect to X is invertible on an open subset of $\mathcal{V}$. For complexity statements, we assume that F is given by a Straight-Line Program that performs L operations.

From the invertibility of the jacobian, Lazard's lemma [5] as proved in [20] implies that $\mathcal{V}$ satisfies the assumptions of Section 1, so the generic zeros of $\mathcal{V}$ can be represented by triangular sets. To be specific, we denote by $T^1, \ldots, T^P$ a family of triangular sets in $\mathcal{K}(P)[X]$ that represent the generic zeros of $\mathcal{V}$ and define prime ideals in $\mathcal{K}(P)[X]$.

In the sequel, given $\mathbf{p}$ in $\mathbb{A}^m(\overline{\mathcal{K}})$, $F(\mathbf{p}, X)$ denotes the system F where the variables P are evaluated at $\mathbf{p}$; then there remain n equations in the n unknowns X. The "specialization" of a triangular set $T \in \mathcal{K}(P)[X]$ at $\mathbf{p}$ denotes the triangular set $T \in \overline{\mathcal{K}}[X]$, obtained by specializing all coefficients of T at $\mathbf{p}$, if $\mathbf{p}$ cancels none of their denominators.

Here is the description of a could-be lifting process. Choose a generic value $\mathbf{p}$ in $\mathbb{A}^m(\overline{\mathcal{K}})$, and compute a family of triangular sets that represent the solutions of $F(\mathbf{p}, X)$. Apply a lifting process, to compute triangular sets with coefficients in the formal power series ring centered at $\mathbf{p}$. When the precision of the power series is high enough, use a rational reconstruction process to recover the requested information. For the introduction of lifting techniques in the context of polynomial systems solving, see [12, 11, 10, 15, 13].

Recovering completely $T^1, \ldots, T^P$ using such techniques requires delicate recombinations of factorized triangular sets. We will not treat the general case here: we present probabilistic algorithms to treat the case when $\mathcal{V}$ is irreducible, and, in the general case, to recover the minimal polynomial of the variable X_1 (which comes from the first polynomials of each triangular set). We refer to [23] for estimates on the error probability for the minimal polynomial computation.

We now specify the genericity conditions imposed on the specialization value $\mathbf{p}$. There exists an hypersurface Δ of $\mathbb{A}^m(\overline{\mathcal{K}})$ such that, for $\mathbf{p}$ not in Δ: (H_1) all coefficients in $T^1, \ldots, T^P$ can be specialized at $\mathbf{p}$, and (H_2) the jacobian of $F(\mathbf{p}, X)$ is invertible on all solutions of $F(\mathbf{p}, X)$.

In the sequel, we assume that we are given a point $\mathbf{p}$ outside Δ with coordinates in $\mathcal{K}$; randomly choosing this point is our first probabilistic aspect. The following condition is a consequence of the above assumptions; since we do not give the proof of this implication, we take this as a new assumption on $\mathbf{p}$, called H_3: all solutions of $F(\mathbf{p}, X)$ are described by the specialization of $T^1, \ldots, T^P$ at $\mathbf{p}$ and if $i \neq j$, the specializations of T^i and T^j at $\mathbf{p}$ have no common zero.

In 3.2, we recall some lifting techniques from in [22], that enable the lifting of the specializations of $T^1, \ldots, T^P$ at $\mathbf{p}$. Yet, the solutions of $F(\mathbf{p}, X)$ may not be given as the specialization of $T^1, \ldots, T^P$, since they may be more factorized. Thus in 3.3, we show that the lifting techniques presented in 3.2 can be applied independently to each factor of the specializations of $T^1, \ldots, T^P$. In 3.4, we treat the case when $\mathcal{V}$ is irreducible. In 3.5, we drop the irreducibility assumption, and show how to recover the minimal polynomial of X_1 modulo $\mathcal{I}_P$.

3.1 Additional subroutines

Initial resolution.

The first task is to compute a family of triangular sets $r^1, \ldots, r^Q$ which represent the solutions of $F(\mathbf{p}, X)$; this is called `Solve(F,p)`. In Subsection 3.5, we also ask that all triangular sets $r^1, \ldots, r^Q$ define prime ideals. To this effect, we may use the zero-dimensional solving procedures of [18, 6, 4] ... In the sequel, *we do not take the cost of this phase into account*, all the more as the cost of the lifting phase is predominant in practice.

Rational Reconstruction.

At the end of the lifting process, we need to recover some rational functions in $P = P_1, \ldots, P_m$ from their power series expansion. More precisely, if c is a formal power series in P of precision $2^{\kappa+1}$, we look for a rational function C with denominators of degree at most 2^κ of which c is the power series expansion. Finding such a rational function, if it exists, amounts to solve a linear system for the coefficients of C. This is done in time polynomial in $M(2^\kappa, m)$.

3.2 Lifting step

We now present the lifting techniques of [22]. Let $T = (T_1, \dots, T_n)$ be one the triangular sets $T^1, \dots, T^P$. Up to a change of variables, we can assume that the specialization value $\mathbf{p}$ is $(0, \dots, 0)$. We denote by A the power series ring $\mathcal{K}[[P_1, \dots, P_m]]$, and $\mathfrak{m}$ its maximal ideal, so $A/\mathfrak{m} = \mathcal{K}$.

Since T generates a prime, hence radical, ideal in $\mathcal{K}(P)[X]$, there exists a $n \times n$ matrix $\mathbf{A}$ with entries in $\mathcal{K}(P)[X]$ such that $\mathbf{F} = \mathbf{AT}$, where $\mathbf{T}$ is the vector with entries $T_1, \dots, T_n$, and $\mathbf{F}$ is the vector $F_1, \dots, F_n$. Assumption H_1 on $\mathbf{p}$ shows that all coefficients in T admit power series expansions in A. Since all polynomials in T are monic in their main variable, the denominators in $\mathbf{A}$ are products of those in T, so they all admit power series expansions in A.

We now see $F, T, \mathbf{A}$ with coefficients in A, and denote $T \mod \mathfrak{m}$ by $t = (t_1, \dots, t_n)$, that is, T with all coefficients specialized at $\mathbf{p}$. The hypotheses we now use are the following. The first is a consequence of H_2 and H_3, and the second comes from the above discussion.

- H'_1 : The jacobian determinant of F with respect to X is invertible in the quotient $\mathcal{K}[X]/(t_1, \dots, t_n)$.
- H'_2 : There exists a $n \times n$ matrix $\mathbf{A}$ with entries in $A[X]$ such that the equality $\mathbf{F} = \mathbf{AT}$ holds.

For $k > 0$, denote by A_k the ring $A/\mathfrak{m}^k$, so that $A_1 = A/\mathfrak{m} = \mathcal{K}$. We want to compute the images of T in the rings $A_{2^\kappa}[X]$, for $\kappa \geq 0$. This amounts to compute the powers series expansions of all coefficients of T in $\mathcal{K}[[P_1, \dots, P_m]]$ at successive precisions 2^κ. The initial value is $t = T \mod \mathfrak{m}$, which we assume to be known.

Let $\kappa \geq 0$ be given, and suppose that we know a triangular set $\tau = (\tau_1, \dots, \tau_n)$ such that $\tau = T \mod \mathfrak{m}^{2^\kappa}$. Using τ, we want to compute $T \mod \mathfrak{m}^{2^{\kappa+1}}$. We formalize our assumption by seeing τ as a triangular set in $A_{2^{\kappa+1}}[X]$ such that $T = \tau \mod \mathfrak{m}^{2^\kappa} \cdot A_{2^{\kappa+1}}[X]$. Since τ is a triangular set, all τ_j are monic, so $\deg_{X_j} T_j = \deg_{X_j} \tau_j$ for $j \leq n$.

Let Q_κ be $A_{2^{\kappa+1}}[X]/(\tau_1, \dots, \tau_n)$. Then Q_κ is a free $A_{2^{\kappa+1}}$-module, with a canonical monomial basis. We denote by $\mathbf{Jac}(\tau)$ and $\mathbf{Jac}(\mathbf{F}_\kappa)$ the jacobian matrices of τ and $\mathbf{F}$ computed in the matrix algebra over Q_κ, and $\mathbf{F}_\kappa$ the image of $\mathbf{F}$ in Q_κ. In [22], we prove the following.

Proposition 3. *The matrix $\mathbf{Jac}(\mathbf{F}_\kappa)$ is invertible in the matrix algebra over Q_κ. Let then $\delta = (\delta_1, \dots, \delta_n)$ be the product $\mathbf{Jac}(\tau)\mathbf{Jac}(\mathbf{F}_\kappa)^{-1}\mathbf{F}_\kappa$ evaluated over the ring Q_κ, and $\widetilde{\delta}$ its canonical preimage in $A_{2^{\kappa+1}}[X]$. Then the equality $T = \tau + \widetilde{\delta}$ holds in $A_{2^{\kappa+1}}[X]$. Besides, it is enough to compute the inverse of $\mathbf{Jac}(\mathbf{F}_\kappa)$ modulo $\mathfrak{m}^{2^\kappa}$.*

This result shows how to compute the new approximation $T \mod \mathfrak{m}^{2^{\kappa+1}}$, which can be used instead of τ for the next lifting step. In the sequel, given F, p and τ, we will denote `Lift(t,F,p)` the subroutine which performs the operations above, and outputs $T \mod \mathfrak{m}^{2^{\kappa+1}}$.

Example.

Let us take one parameter P_1, two variables X_1, X_2 and

$$F_1 : 2X_1^2 - P_1 + 1 - X_1X_2^2P_1 - X_1X_2^2 - X_2X_1^3 + X_1X_2P_1 - X_1X_2$$

$$F_2 : X_2^2P_1 + X_2^2 - X_1 + X_2X_1^2 - X_2P_1 + X_2.$$

This system is constructed so that its solutions can be represented by the following triangular set in $\mathbb{Q}(P_1)[X_1, X_2]$.

$$T_1 = X_1^2 - P_1 + 1, \quad T_2 = X_2^2 - X_1/(P_1 + 1).$$

To compute T_1, T_2, we choose the specialization value $P_1 = 0$, and solve the specialized system. This gives:

$$t_1 = X_1^2 + 1, \quad t_2 = X_2^2 - X_1.$$

Here $\kappa = 0$, $2^{\kappa+1} = 2$, so the base-ring A_2 is $\mathbb{Q}[[P_1]]/(P_1^2)$; $\tau = (X_1^2 + 1, X_2^2 - X_1)$ and all computations are done over $Q_0 = A_2[X_1, X_2]/(\tau_1, \tau_2)$. The jacobian matrix of τ is

$$\mathbf{Jac}(\tau) = \begin{matrix} 2X_1 & 0 \\ -1 & 2X_2 \end{matrix} \quad ,$$

the inverse of the jacobian matrix of F, $\mathbf{Jac}(\mathbf{F}_\kappa)^{-1}$, is

$$\frac{1}{8} \begin{matrix} 2P_1X_2 + (-2P_1 - 4)X_1 & 2P_1X_1X_2 + 2P_1 + 4 \\ (P_1 - 2)X_2 + 2P_1 - 4 & (5P_1 - 6)X_1X_2 - 4X_1 \end{matrix} \quad ,$$

and the image of F in Q_0, denoted $\mathbf{F}_\kappa$, is

$$(P_1X_1X_2, \quad -P_1X_2 + P_1X_1).$$

Then we apply Proposition 3: we compute the value $\delta = (-P_1, P_1X_1)$, so the approximation at precision P_1^2 is

$$X_1^2 + 1 - P_1, \quad X_2^2 - X_1 + P_1X_1.$$

This is indeed the expansion of T_1, T_2 at precision P_1^2. The terms in $\mathbf{Jac}(\mathbf{F}_\kappa)^{-1}$ of degree in $P_1 > 0$ are not used, since $\mathbf{F}_\kappa$ has valuation 1 in P_1; this is the last statement in Proposition 3.

Complexity.

We let C be a universal constant such that, for any ring R and any triangular set T, the operations $+, \times,$ and $\div$ when it is possible, can be done modulo T in a numbers of operations in R polynomial in C^n and $\prod_{i \leq n} \deg_{X_i} T_i$. The inverse of the determinant of $\mathbf{Jac}(\mathbf{F}_\kappa)$ is computed by induction on κ by Hensel's Lemma [25, Ch. 9], using multiplications in Q_κ: the only inversion is done for $\kappa = 0$, and can be done in $\mathcal{K}[X]/(t_1, \dots, t_n)$, according to Proposition 3.

An operation $+, \times$ in Q_κ takes a number of operations in $A_{2^{\kappa+1}}$ polynomial in $C^n, \prod_{i \leq n} \deg_{X_i} \tau_i$. In terms of operations in $\mathcal{K}$, an operation in $A_{2^{\kappa+1}}$ has a cost polynomial in $M(2^{\kappa+1}, m)$, the number of monomials of degree $\leq 2^{\kappa+1}$ in m variables. Since $\deg_{X_i} \tau_i = \deg_{X_i} T_i$, the number of operations in $\mathcal{K}$ is polynomial in $C^n, \prod_{i \leq n} \deg_{X_i} T_i, M(2^{\kappa+1}, m)$.

Computing $\mathbf{Jac}(\mathbf{F}_\kappa)$ and $\mathbf{F}_\kappa$ requires to evaluate the system F and its jacobian matrix in Q_κ. Since we assume that F is given by a Straight-Line Program that performs L operations, this cost is $O(nL)$ operations in Q_κ [13]. The other operations are linear algebra with matrices of size n over Q_κ, which can be done in $n^{O(1)} \in O(C^n)$ operations in Q_κ. Finally, the total cost of procedure `Lift`, in operations in $\mathcal{K}$, is polynomial in $L, C^n, \prod_{i \leq n} \deg_{X_i} T_i, M(2^{\kappa+1}, m)$.

3.3 Factorized lifting

In practice, we cannot ensure that the resolution of the system $F(\mathbf{p}, X)$ is given as the specialization of $T^1, \dots, T^P$ at $\mathbf{p}$, since it may be more factorized. Thus, we now prove that the lifting can be applied to any factor of $t = T \mod \mathfrak{m}$.

Proposition 4. *Let r be a triangular set in $\mathcal{K}[X]$ such that the ideal generated by r contains t. Then there exists a triangular set R in $A[X]$ such that $R \mod \mathfrak{m} = r$ and the ideal generated by R contains T. The successive approximations $R \mod \mathfrak{m}^{2^k}$ can be computed using Proposition 3.*

Proof. First consider a particular case: we suppose that there exists $J \leq n$ such that the following holds. Let B denote $A[X_1, \dots, X_{J-1}]/(T_1, \dots, T_{J-1})$ and $\mathfrak{n}$ the ideal of B induced by $\mathfrak{m} + (T_1, \dots, T_{J-1})$. Thus, the quotient $B/\mathfrak{n}$ is $\mathcal{K}[X_1, \dots, X_{J-1}]/(t_1, \dots, t_{J-1})$. Our assumption is:

- $r_1, \dots, r_{J-1} = t_1, \dots, t_{J-1}$;
- there exists a polynomial q_J in $B/\mathfrak{n}\,[X_J]$ such that $t_J = q_J r_J$ holds in $B/\mathfrak{n}\,[X_J]$;
- for j in $J+1, \dots, n$, we see t_j as a polynomial in the variables $X_{J+1}, \dots, X_j$ with coefficients in $B/\mathfrak{n}\,[X_J]$, and assume that r_j is obtained by reducing all these coefficients modulo r_J.

Since A is complete with respect to the $\mathfrak{m}$-adic topology, B is complete with respect to the $\mathfrak{n}$-adic topology. Hypotheses H'_1 and H'_2 imply that the derivative of t_J w.r.t. X_j is invertible in $B/\mathfrak{n}\,[X_J]/(t_J)$. Hensel's Lemma then shows that there exists Q_J and R_J in B such that $T_J = Q_J R_J$ holds in $B[X_J]$ and $r_J = R_J \mod \mathfrak{n}$. The polynomial R_J is defined in $B[X_J]$, but we may identify it to its canonical preimage in $A[X_1, \dots, X_J] \subset A[X_1, \dots, X_n]$.

For $j < J$, we define $R_j = T_j$. For $j > J$, we define R_j as follows. We see T_j as polynomial in the variables $X_{J+1}, \dots, X_j$ with coefficients in $B[X_J]$, and define R_j by reducing all these coefficients modulo R_J. As such, this polynomial is a multivariate polynomial in $X_{J+1}, \dots, X_j$ with coefficients in $A[X_1, \dots, X_J]$ modulo $T_1, \dots, T_{J-1}, R_J$, but as above, we may identify it with its canonical preimages in $A[X_1, \dots, X_n]$. Through this identification, $r = R \mod \mathfrak{m}$.

We then prove the existence of a matrix $\mathbf{B}$ such that the equality $\mathbf{T} = \mathbf{B}\mathbf{R}$ holds, by successively constructing its lines. For $j < J$, we have $T_j = R_j$, so we take a line composed only of 0's, with 1 at entry j. Let us now take $j = J$. The equality $T_J = Q_J R_J$ in $B[X_J]$ can be rewritten in $A[X_1, \dots, X_J]$ as $T_J = Q_J R_J + S_J$, where S_J is in the ideal $(T_1, \dots, T_{J-1}) = (R_1, \dots, R_{J-1})$, and R_J is seen in $A[X_1, \dots, X_J]$. This enables to define the J-th line of $\mathbf{B}$. Finally, we take $j > J$. Then R_j is such that $R_j = T_j$ with all coefficients reduced modulo R_J in $B[X_J]$. Thus, $T_j = R_j + s_j$, where s_j is in the ideal generated by R_J in $B[X_J, \dots, X_j]$. From the definition of B, this can be rewritten as $T_j = R_j + S_j$ in $A[X_1, \dots, X_j]$, where S_j is in the ideal $(T_1, \dots, T_{J-1}, R_J) = (R_1, \dots, R_J)$. This enables to complete the definition of $\mathbf{B}$.

We now turn to the proposition itself. Let J be the least integer such that $r_J \neq t_J$. If $r = t$, we take $J = n + 1$. We prove by induction on J that if T satisfies hypotheses H'_1, H'_2, and $t = T \mod \mathfrak{m}$ belongs to the ideal generated by r, then there exists a triangular set R such that $r = R \mod \mathfrak{m}$, and a $n \times n$ matrix $\mathbf{B}$ with entries in $A[X]$ such that $\mathbf{T} = \mathbf{B}\mathbf{R}$. We call this property $P(J)$; $P(n+1)$ is obvious, so we suppose that $J \leq n$ and that P is proved for $J+1, \dots, n+1$.

Since t_J is in the ideal generated by r, it is easy to deduce that r_J divides t_J in $\mathcal{K}[X_1, \dots, X_{J-1}]/(t_1, \dots, t_{J-1})[X_J]$. We then define a triangular set s in $\mathcal{K}[X_1, \dots, X_n]$ as follows. We take $s_1, \dots, s_J = r_1, \dots, r_J$, and for $j > J$ we define s_j as t_j with all coefficient reduced modulo s_J. Thus T and s satisfy the hypotheses of the previous paragraphs, which enables to define a triangular set S and a matrix $\mathbf{B}$ such that $\mathbf{T} = \mathbf{B}\mathbf{S}$ and $s = S \mod \mathfrak{m}$.

The triangular set S satisfies H'_1 and H'_2. For $j > J$, $s_j - t_j$ is in the ideal generated by r. Since t_j is in this ideal, s_j is in this ideal too. Consequently, we can apply our induction argument on S and r, since now s and r coincide at least up to level J. This shows the existence of a triangular set R and a matrix $\mathbf{B}'$ such that $\mathbf{S} = \mathbf{B}'\mathbf{R}$, and $R \mod \mathfrak{m} = r$. Thus, $\mathbf{T} = \mathbf{B}\mathbf{B}'\mathbf{R}$. This shows $P(J)$, which gives the first part of the proposition. We have $\mathbf{F} = \mathbf{A}\mathbf{B}\mathbf{B}'\mathbf{R}$, which gives H'_2 for R. It is easy to check that R satisfies H'_1, so Proposition 3 applies to R.

3.4 The irreducible case

We now assume that $\mathcal{V}$ is irreducible. Then its generic zeros can be described by a single triangular set T. We fix $k \leq n$, and show how to compute $(T_1, \dots, T_k)$ by lifting techniques.

By assumption H_3, the specialization of T at $\mathbf{p}$ gives a description of the solutions of the system $F(\mathbf{p}, X)$. Yet, the specialized system may not define an irreducible set, and could be represented by more than one triangular set. Thus, we explicitly require that `Solve(F,p)` outputs a *single* triangular set, which *must* then be the specialization of T at $\mathbf{p}$. Then the algorithm is straightforward:

```
r <- Solve(F,p)
while not(Finished) do
  r <- Lift(r,F,p)
  Finished,R1,...,Rk <- Stop(r)
end while
return R1,...,Rk
```

The subroutine `Stop` first tries to compute a rational reconstruction of all the coefficients in $r_1, \dots, r_k$, yielding polynomials $R_1, \dots, R_k$. Even if the reconstruction is possible, it might not coincide with $T_1, \dots, T_k$, if we have stopped the lifting too early. So we choose a witness value $\mathbf{p}'$, which must satisfy the same conditions as $\mathbf{p}$, and compute a description $t'_1, \dots, t'_n$ of the solutions of the system $F(\mathbf{p}, X)$. `Stop` tests if the specialization of $R_1, \dots, R_k$ at $\mathbf{p}'$ is $t'_1, \dots, t'_k$. If the reconstruction is possible and R passes the test, `Stop` outputs `true` and R; else it returns `false`. The choices of , $\mathbf{p}, \mathbf{p}'$ that lead to an error belong to a proper algebraic set of $\mathbb{A}^{2m}(\overline{\mathcal{K}})$.

For such lifting techniques, the whole cost is equivalent to the cost of the last lifting step. Let $\mathfrak{D}_k$ be the maximal degree in P of the coefficients in $T_1, \dots, T_k$. Then the lifting must be run to precision 2^{p+1}, with $p = \lceil \log_2(\mathfrak{D}_k) \rceil$. From the analysis of Subsection 3.2, the cost of the last lifting step is polynomial in $L, C^n, \prod_{i \le n} \deg_{X_i} T_i, M(2^{p+1}, m)$. The product of the degrees is the number of generic solutions, i.e. $\deg \pi$ (see the introduction); since $M(2^{p+1}, m)$ is polynomial in $M(\mathfrak{D}_k, m)$, the cost of the lifting is polynomial in $L, C^n, \deg \pi, M(\mathfrak{D}_k, m)$. From Subsection 3.1, the cost of the rational reconstruction fits into this bound, so Theorem 2 is proved.

3.5 Computing a minimal polynomial

Let us drop the irreducibility assumption, and let $M_1 \in \mathcal{K}(P)[X_1]$ be the minimal polynomial of X_1 modulo $\mathcal{I}_P$. We now show how to compute M_1 by lifting techniques.

The introduction mentions the use of primitive element techniques for this question (X_1 is not necessarily a primitive element of A_P); we now relate this to triangular sets. The first polynomials of each triangular set, $T_1^1, \dots, T_1^P$, may not be all distinct. Without loss of generality, assume that $T_1^1, \dots, T_1^p$ are representatives of the distinct polynomials among them, for some $p \le P$. Since $T^1, \dots, T^p$ define prime ideals, $T_1^1, \dots, T_1^p$ are irreducible, so their product is M_1.

We need a new assumption on $\mathbf{p}$. We denote by $\mathcal{V}_{\mathbf{p}}$ the zero-set of $F(\mathbf{p}, X)$, and by m_1 the minimal polynomial of X_1 modulo $\mathcal{I}(\mathcal{V}_{\mathbf{p}})$. Then we make the following assumption, denoted H_4, on $\mathbf{p}$, which is satisfied on an open subset of $\mathbb{A}^m(\overline{\mathcal{K}})$: m_1 is the specialization of M_1 at $\mathbf{p}$.

Let $r^1, \dots, r^Q$ be triangular sets that describe the solutions of $F(\mathbf{p}, X)$, and define prime ideals in $\mathcal{K}[X]$. By assumption H_3, $T^1, \dots, T^P$ can be specialized at $\mathbf{p}$, and their specializations $t^1, \dots, t^P$ also describe the solutions of $F(\mathbf{p}, X)$. Besides, H_3 shows that the intersection of the ideals generated by $t^1, \dots, t^P$ is actually their product. Then for $i \le Q$, there exists j such that t^j is in the ideal defined by r^i, so Proposition 3 shows that the lifting process can be applied to r^i. Let thus $R^1, \dots, R^Q$ be triangular sets with coefficients in $\mathcal{K}[[P]]$ such that, for $i \le Q$, $R^i \mod \mathfrak{m} = r^i$, and there exists j such that T^j is contained in the ideal generated by R^i. In this case, we see that R_1^i divides T_1^j.

The polynomials T_1^j and M_1 are actually in $\mathcal{K}(P)[X_1]$, so if we see them in $\mathcal{K}[[P]][X_1]$, their coefficients are the Taylor expansions of some rational functions. This is likely not the case for the polynomials R_1^i, but we can still recover M_1.

Proposition 5. *Reorder $r^1, \dots, r^Q$ so that $r_1^1, \dots, r_1^q$ are representatives of the distinct polynomials in $r_1^1, \dots, r_1^Q$, for some $q \le Q$. Then $\prod_{i \le q} R_1^i = M_1$ in $\mathcal{K}[[P]][X_1]$.*

Proof. We first show that $R_1^1, \dots, R_1^Q$ are irreducible in the factorial ring $\mathcal{K}[[P]][X_1]$. Suppose that $R_1^i = GH$ in $\mathcal{K}[[P]][X_1]$. Since R_1^i is monic, we may suppose that G and H are monic. Then $r_1^i = (G \mod \mathfrak{m})(H \mod \mathfrak{m})$. Since r_1^i is irreducible, it follows that for instance $G \mod \mathfrak{m}$ is a unit. Since G is monic, G is the constant 1, so R_1^i is irreducible.

The product $\prod_{i \le q} r_1^i$ is the minimal polynomial of X_1 modulo $\mathcal{I}(\mathcal{V}_{\mathbf{p}})$, that is m_1. The corresponding $R_1^1, \dots, R_1^q$ are all pairwise distinct, hence pairwise coprime, since they are irreducible. Since each of them divides one of the polynomials T_1^j, each of them divides M_1. Thus $\prod_{i \le q} R_1^i$ divides M_1. The degree of $\prod_{i \le q} R_1^i$ is the degree of $\prod_{i \le q} r_1^i$, that is the degree of m_1. By hypothesis H_4, it coincides with the degree of M_1. Thus, $\prod_{i \le q} R_1^i = M_1$.

This gives the following algorithm to compute M_1:

```
r^1,..,r^Q <- Solve(F,p)
## r^1,..,r^Q are chosen to define prime ideals.
## we reorder them and take q so that
## r^1_1,..,r^q_1 are a set of representatives of
## the distinct polynomials among r^1_1,..,r^Q_1.
while not(Finished) do
  for i in [1..q] do r^i <- Lift(r^i,F,p)
  Finished,M <- Stop(r^1,..,r^q)
end while
return M
```

The subroutine Stop computes the product of all polynomials r_1^i, and if possible, a rational reconstruction of all coefficients of the product. This gives a polynomial M, on which we apply a probabilistic check: as before, we test whether M specializes on the minimal polynomial of X_1 for a randomly chosen witness $\mathbf{p}'$.

Let $\mathfrak{D}_1$ be the maximal degree in P of the coefficients in M_1, and $p = \lceil \log_2(\mathfrak{D}_1) \rceil$. As in Subsection 3.4, the complexity is polynomial in $L, C^n, M(\mathfrak{D}_1, m)$ and $\sum_{i \le q} \prod_{j \le n} \deg_{X_j} r_j^i$. This last sum is at most the number of generic solutions of the system F, i.e. $\deg \pi$. This proves Theorem 3.

4. APPLICATIONS

We present two applications of our algorithms, from number theory and cryptography. Our Magma [1] implementation outperformed the built-in functions on these examples; the probabilistic aspect was not a problem: problem-specific arguments show that our output is correct. Our computations were done on a Compaq XP/1000 EV6 from the MEDICIS resource center [2].

4.1 Genus 2 curves with (2,2)-split Jacobian

Genus 2 curves with Jacobian (2,2)-isogeneous to a product of elliptic curves appear frequently in number theory: current rank and torsion records are obtained for such curves. In [9], we give an explicit classification of such situations, using the algorithms presented here. We now describe part of the necessary computations.

Isomorphism classes of genus 2 (resp. elliptic) curves are classified by the Igusa invariants j_1, j_2, j_3 (resp. by their j-invariant). There exists a polynomial $T(J_1, J_2, J_3)$ such that a genus 2 curve has (2,2)-split Jacobian if and only if its Igusa invariants cancel T; then the j-invariants of the elliptic curves are given by a polynomial of degree 2, whose coefficients are rational functions of j_1, j_2, j_3.

A genus 2 curve with (2,2)-split Jacobian admits the equation $y^2 = x^6 + ax^4 + bx^2 + 1$; its Igusa invariants are rational functions $J_1(a,b), J_2(a,b), J_3(a,b)$. The underlying elliptic curves are isomorphic to the curves $y^2 = x^3 + ax^2 + bx + 1$; their j-invariant is a rational function $J(a,b)$.

Let F be the system $\{j - J(a,b), j_i - J_i(a,b)\,(i \leq 3)\}$ in $\mathbb{Q}[j_1, j_2, j_3, j, a, b]$ and take j_1, j_2 for parameters: we work in $\mathbb{Q}(j_1, j_2)[j_3, j, a, b]$ modulo the ideal generated by F after canceling denominators. This ideal is prime of dimension zero, so its solutions are represented by a triangular set in $\mathbb{Q}(j_1, j_2)[j_3, j, a, b]$. The first polynomial $T_1 \in \mathbb{Q}(j_1, j_2)[j_3]$ is the relation T mentioned above. The second polynomial $T_2 \in \mathbb{Q}(j_1, j_2)[j_3, j]$ gives j in terms of j_1, j_2, j_3 when the denominators of its coefficients do not vanish.

We use the algorithm of Section 3.4. T_1 is computed in 22 sec., and T_1, T_2 in 140 sec. As a comparison, using the algorithm of [22], a representation by primitive element requires more than 400 sec. — see [23, Ch. 16, 20, 25] for details. This illustrates the interest of our "triangular" approach, when only a partial information is wanted.

4.2 Modular equations

In [8, 23], *modular equations* in high genus are defined. For a hyperelliptic curve C, and a prime ℓ, we study the ℓ-torsion divisors in the Jacobian of C: over a finite field, this enables to compute the cardinality of the Jacobian, a question of primary importance for hyperelliptic cryptosystems [8].

The ℓ-torsion divisors form a finite group G_ℓ, and are solutions of an algebraic system, in suitable coordinates. We define t_ℓ as a well-chosen function defined on G_ℓ, and the modular equation is the minimal polynomial Ξ_ℓ of t_ℓ in G_ℓ. It behaves like a revolvent: in [8], it is shown how to use its factorization patterns for cardinality determination.

Computing Ξ_ℓ for a generic curve is done following Section 3.5. We treated the 3-torsion in genus 2; the corresponding system has 3 equations in 3 unknowns X_1, X_2, X_3 and 3 parameters P_1, P_2, P_3 which parameterize curves of genus 2. The output $\Xi_3 \in \mathbb{Q}(P_1, P_2, P_3)[T]$ is computed within 4.5 h.; for comparison, it takes more than 20 h. to compute a representation by primitive element. Our result is used within Magma's hyperelliptic curves package `CrvHyp`.

5. REFERENCES

[1] http://www.maths.usyd.edu.au:8000/u/magma/.

[2] http://www.medicis.polytechnique.fr/.

[3] P. Aubry. *Ensembles triangulaires de polynômes et résolution de systèmes algébriques. Implantation en Axiom.* PhD thesis, Université Paris VI, 1999.

[4] P. Aubry, D. Lazard, and M. Moreno Maza. On the theories of triangular sets. *J. Symb. Comp.*, 28(1,2):45–124, 1999.

[5] F. Boulier, D. Lazard, F. Ollivier, and M. Petitot. Representation for the radical of a finitely generated differential ideal. In *Proceedings ISSAC '95*, pages 158–166. ACM Press, 1995.

[6] S. Dellière. *Triangularisation de systèmes constructibles — Application à l'évaluation dynamique.* PhD thesis, Université de Limoges, 1999.

[7] G. Gallo and B. Mishra. Efficient algorithms and bounds for Wu-Ritt characteristic sets. In *Proceedings MEGA '90.* Birkhäuser, 1990.

[8] P. Gaudry. *Algorithmique des courbes hyperelliptiques et applications à la cryptologie.* PhD thesis, École polytechnique, 2000.

[9] P. Gaudry and É. Schost. On the invariants of the quotients of the Jacobian of a curve of genus 2. In *Proceedings AAECC 14*, LNCS, 2001.

[10] M. Giusti, K. Hägele, J. Heintz, J. E. Morais, J. L. Montaña, and L. M. Pardo. Lower bounds for Diophantine approximation. Number 117,118 in J. of Pure and App. Algebra, pages 277–317, 1997.

[11] M. Giusti, J. Heintz, J. E. Morais, J. Morgenstern, and L. M. Pardo. Straight-line programs in geometric elimination theory. *J. of Pure and App. Algebra*, 124:101–146, 1998.

[12] M. Giusti, J. Heintz, J. E. Morais, and L. M. Pardo. When polynomial equation systems can be solved fast ? In *Proceedings AAECC 11*, LNCS, 1995.

[13] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *J. Complexity*, 17(1):154–211, 2001.

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

[15] J. Heintz, T. Krick, S. Puddu, J. Sabia, and A. Waissbein. Deformation techniques for efficient polynomial equation solving. *J. Complexity*, 16:70–109, 2000.

[16] M. Kalkbrener. *Three contributions to elimination theory.* PhD thesis, Kepler University, Linz, 1991.

[17] T. Krick, J. Sabia, and P. Solernó. On intrinsic bounds in the Nullstellensatz. *AAECC Journal*, 8:125–134, 1997.

[18] D. Lazard. Solving zero-dimensional algebraic systems. *J. Symb. Comp.*, 13:117–133, 1992.

[19] M. Moreno Maza. *Calculs de pgcd au-dessus des tours d'extensions simples et résolution des systèmes d'équations algébriques.* PhD thesis, Université Paris VI, 1997.

[20] S. Morrison. The differential ideal $[P] : M^\infty$. *J. Symb Comp.*, 28:631–656, 1999.

[21] J. Sabia and P. Solernó. Bounds for traces in complete intersections and degrees in the Nullstellensatz. *AAECC Journal*, 6:353–376, 1996.

[22] É. Schost. Computing parametric geometric resolutions. Preprint École polytechnique, 2000.

[23] É. Schost. *Sur la résolution des systèmes polynomiaux à paramètres.* PhD thesis, École polytechnique, 2000.

[24] A. Szanto. *Computation with polynomial systems.* PhD thesis, Cornell University, 1999.

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