Inversion of Parameterized Hypersurfaces by Means of Subresultants

Laurent Busé
INRIA, GALAAD,
2004 route des Lucioles, B.P. 93,
06902 Sophia-Antipolis cedex, France.
lbuse@sophia.inria.fr

Carlos D'Andrea
University of California at Berkeley,
1089 Evans Hall,
Berkeley, CA 94720 USA.
cdandrea@math.berkeley.edu

ABSTRACT

We present a subresultant-based algorithm for deciding if the parametrization of a toric hypersurface is invertible or not, and for computing the inverse of the parametrization in the case where it exists. The algorithm takes into account the monomial structure of the input polynomials.

Categories and Subject Descriptors

G.0 [**Mathematics of Computing**]: General

General Terms

Algorithms

Keywords

Multivariate Subresultants, Birational Maps.

1. INTRODUCTION

Let $\mathbb{K}$ be an algebraically closed field of characteristic zero. We will denote with $\mathbb{K}^*$ the multiplicative group of $\mathbb{K}$. Given a rational parametrization

$$\begin{array}{cccc} \phi: & \mathbb{K}^{*n} & -- > & \mathcal{V} \subset \mathbb{K}^{*n+1} \\ & (t_1,\ldots,t_n) & \mapsto & \left(\frac{p_1(t)}{q(t)},\ldots,\frac{p_{n+1}(t)}{q(t)}\right), \end{array} \quad (1)$$

where $p_i(t)$, $q(t) \in \mathbb{K}[t_1,\ldots,t_n]$ we would like to address the following questions:

- Decide if ϕ is invertible (properness problem).
- If ϕ is invertible, compute its inverse (inversion problem).

Both questions have been solved theoretically in [17] and algorithmically in [18] by means of Gröbner bases, and in [17] for the case of surfaces ($n = 2$) by using resultants. In this paper, we will give a general algorithmic method for the solution of both problems, which work in a general context, and is based on the theory of multivariate subresultants, as developed in [5, 21, 12]. We will show that if the input polynomials do not have common zeroes in a suitable compactification of the n th dimensional torus $\mathbb{K}^{*n}$, then we can convert both problems into a single one where we only have to deal with solving an over-determined system of $n+1$ equations with n unknowns. The theory of subresultants has shown to be useful in this situation, see [22].

Unirational algebraic varieties, specially rational curves and surfaces, are of interest in computer aided geometric design (see [15, 16] and the references therein). In low dimensions, the situation is very well-known. For plane curves, one can relate the properness and inversion problems to Lüroth's theorem, and there are different algorithmic procedures to solve them (see [15, 16, 19, 23]). In higher dimensions, there exists some algorithmic approaches based on u-resultants [6] and on Gröbner Basis in [18]. In [17], a general criteria is given and it turns to be effective for surfaces in $\mathbb{K}^3$.

Our approach essentially is the resultant-based method presented in [15, Chapter 15] for inverting a parametrized algebraic surface, and in [2, §5] where a similar approach is used for computing the inverse image of a point of a parametrization (note that these approaches do not require the knowledge of the implicit equation). We will show that we can perform the same operations with subresultant matrices instead of resultant matrices in the case where ϕ do not have base point in a certain toric variety. This will lead us to work with smaller and more compact matrices, as multivariate subresultants can essentially be computed as minors of resultant matrices [5].

2. THE CASE OF CURVES

Before dealing with the general case (1) we first describe our approach to properness and inversion problems in the case of curves ($n = 1$) for clarity; the tools we are going to use are quite standard.

Using the projective version (over $\mathbb{K}$) of (1), we suppose given a generically finite rational map

$$\phi : \mathbb{P}^1 \to \mathcal{V} \subset \mathbb{P}^2 : (t_1, t_2) \mapsto (p_1(t_1, t_2) : p_2(t_1, t_2) : q(t_1, t_2)),$$

where the homogeneous polynomials p_1, p_2 and q have the same degree $c \geq 1$. We assume moreover, but without loss of generality, that the $\gcd(p_1, p_2, q)$ is a constant, i.e. that ϕ does not have *base points*. Since ϕ is generically finite on the irreducible curve $\mathcal{V}$, we have the following well-known degree formula (see e.g. [10]): $d\deg(\mathcal{V}) = c$, where d denotes the

ISSAC'04, July 4–7, 2004, Santander, Spain.

degree of ϕ (i.e. the number of points in a generic fiber of ϕ).

Denoting with $(X_1 : X_2 : X_3)$ the homogeneous coordinates of $\mathbb{P}^2$, an affine (i.e. $X_3 = 1$) implicit equation of $\mathcal{V}$ is classically obtained by computing the resultant $\mathrm{Res}(qX_1 - p_1, qX_2 - p_2)$ eliminating both homogeneous variables t_1 and t_2. More precisely, if $C(X_1, X_2)$ denotes an affine implicit equation of $\mathcal{V}$ we have, with $k \in \mathbb{K}^*$:

$$\mathrm{Res}(qX_1 - p_1, qX_2 - p_2) = kC(X_1, X_2)^d. \qquad (2)$$

This resultant can be computed as the determinant of a square matrix, and we have different matrices whose determinant equals it [14, chapter 12]. Denoting with $A := \mathbb{K}[X_1, X_2]$ the coefficient ring and R the ring $A[t_1, t_2]$ graded as an A-module with $\deg(t_1) = \deg(t_2) = 1$, we choose a Sylvester/Bézout mixed matrix containing only one column of Bézout type, i.e. the matrix of the map (choosing usual monomial bases)

$$\begin{array}{ccccccc} R_{c-2} & \oplus & R_{c-2} & \oplus & R_0 & \rightarrow & R_{2c-2} \\ (u & \oplus & v & \oplus & a) & \mapsto & uF_1 + vF_2 + \mathrm{Bez}(a), \end{array}$$

where $F_1 := qX_1 - p_1$, $F_2 := qX_2 - p_2$, and $\mathrm{Bez}(a)$ is the Jacobian of F_1, F_2. We assume from now that $\deg(\mathcal{V}) > 1$ (the case $\deg(\mathcal{V}) = 1$ is easy since then $\mathcal{V}$ is a line). Let us denote with $\mathbb{M}$ the Sylvester part of this matrix, and by Δ_i, for $i = 1, \ldots, 2c-1$, the signed determinant of the maximal minor of $\mathbb{M}$ obtained by erasing the i^{th} row. It follows that

$$\mathrm{Res}(F_1, F_2) = \sum_{i=1}^{2c-1} c_i \Delta_i, \qquad (3)$$

where $c_i \in A$ is the coefficient of t^i in $\mathrm{Bez}(a)$, which by construction is either zero or has positive degree in the X_i's. It turns out that

$${}^t\mathbb{M} \begin{pmatrix} t_1^{2c-2} \\ t_1^{2c-3}t_2 \\ \vdots \\ t_2^{2c-2} \end{pmatrix} = \begin{pmatrix} t_1^{c-2}F_1 \\ \vdots \\ t_2^{c-2}F_1 \\ t_1^{c-2}F_2 \\ \vdots \\ t_2^{c-2}F_2 \end{pmatrix}. \qquad (4)$$

Now observe that $\mathrm{rank}(\mathbb{M}) = 2c-2$. Thus, by definition of the Δ_i's, the vector $(\Delta_1, \ldots, \Delta_{2c-1})$ is a generator of the kernel of ${}^t\mathbb{M}$. From this and (2), (3) we deduce easily that ϕ is proper if and only if the $\gcd(\Delta_1, \cdots, \Delta_{2c-1}) \in \mathbb{K}^*$: a properness criterion.

Assuming that ϕ is proper, then there exists $i \in \{1, \cdots, 2c-1\}$ such that $\Delta_i \neq 0$ in A and Δ_i does not vanish identically on $\mathcal{V}$. We then claim that both rational maps (when $i = 1$ or $i = 2c-1$ there is only one defined map)

$$\mathbb{P}^2 \to \mathbb{P}^1 : (X_1 : X_2 : X_3) \mapsto (\Delta_i : \Delta_{i+1})$$

$$\mathbb{P}^2 \to \mathbb{P}^1 : (X_1 : X_2 : X_3) \mapsto (\Delta_{i-1} : \Delta_i)$$

give an inversion of ϕ, i.e. induce a map ψ from an open subset $U \subset \mathcal{V} \subset \mathbb{P}^2$ to $\mathbb{P}^1$ such that for all $\mathbf{x} \in U$ we have $\phi \circ \psi(\mathbf{x}) = \mathbf{x}$. Indeed, we may choose U so that the co-restriction of ϕ to U is finite of degree 1 and so that $\Delta_i(\mathbf{x}) \neq 0$ for all $\mathbf{x} \in U$. It follows that the dimension of the kernel of $\mathbb{M}(\mathbf{x})$ equals 1 for all $\mathbf{x} \in U$. Comparing (4) to the following identity in $\mathbb{K}[X_1, X_2, X_3]$

$$(\Delta_1 \ \Delta_2 \ \cdots \ \Delta_{2c-1})\ \mathbb{M} = 0,$$

yields immediately the claim.

Remark 2.1. *Observe also that, assuming that ϕ is proper, the previous argument shows that all the Δ_i's, with i going from 1 to $2c-1$, are non-zero since an inversion of ϕ must have a 1-dimensional image.*

Example: *Consider the example of the usual parametrization of a circle*

$$X_1 = \frac{2t_1}{1+t_1^2}, \ X_2 = \frac{1-t_1^2}{1+t_1^2}.$$

It corresponds to the following rational map

$$\mathbb{P}^1 \to \mathbb{P}^2 : (t_1 : t_2) \mapsto (2t_1t_2 : t_2^2 - t_1^2 : t_1^2 + t_2^2).$$

The matrix $\mathbb{M}$ is easily computed from this map:

$$\mathbb{M} = \begin{pmatrix} X_1 & 1+X_2 \\ -2 & 0 \\ X_1 & X_2 - 1 \end{pmatrix}.$$

It follows that

$$\Delta_1 = \det \begin{pmatrix} -2 & 0 \\ X_1 & X_2 - 1 \end{pmatrix} = 2(1 - X_2),$$

$$\Delta_2 = -\det \begin{pmatrix} X_1 & 1+X_2 \\ X_1 & X_2 - 1 \end{pmatrix} = 2X_1,$$

$$\Delta_3 = \det \begin{pmatrix} X_1 & 1+X_2 \\ -2 & 0 \end{pmatrix} = 2(1 + X_2).$$

Hence we deduce that ϕ is proper and obtain an inverse of ϕ with both rational maps

$$\mathbb{P}^2 \to \mathbb{P}^1 : (X_1 : X_2 : X_3) \mapsto (1 - X_2 : X_1),$$

$$\mathbb{P}^2 \to \mathbb{P}^1 : (X_1 : X_2 : X_3) \mapsto (X_1 : 1 + X_2), \qquad (5)$$

that is to say $t_1 = \frac{1-X_2}{X_1}$ or $t_1 = \frac{X_1}{1+X_2}$, which are the same modulo the implicit equation of $\mathcal{V}$:

$$\frac{1-X_2}{X_1} - \frac{X_1}{1+X_2} = \frac{1 - X_1^2 - X_2^2}{X_1(1+X_2)}.$$

3. THE PROPERNESS PROBLEM

Now we get back to the general case (1), as stated in the introduction, with the aim of generalizing the results of section 2 to this context. Denoting by *supp*(.) the support of a list of polynomials, we will assume the following:

1. $supp(p_1, \ldots, p_{n+1}, q) \subset \mathcal{A} \subset \mathbb{Z}^n$, and $\dim(\mathcal{A}) = n$.
2. Let $X_{\mathcal{A}}$ be the toric variety associated with $\mathcal{A}$ ([14]). The variety $V_{X_{\mathcal{A}}}(p_1, \ldots, p_{n+1}, q) = \emptyset$.

Remark 3.1. *In the case of curves we presented in the previous section, the toric variety $X_{\mathcal{A}}$ corresponds to the projective line $\mathbb{P}^1$.*

Let $\mathbf{P}$ be the convex hull of $\mathcal{A}$, that is $\mathbf{P} := conv(\mathcal{A})$, and $F(X_1, \ldots, X_{n+1})$ be an implicit equation of $\mathcal{V}$.

Theorem 3.2. *If ϕ is dominant and assumptions 1 and 2 hold, then we have the following "degree formula":*

$$d \deg(F) = \mathbf{vol}(\mathbf{P}),$$

where $\mathbf{vol}(\cdot)$ stands for the "normalized volume", and d is the degree of ϕ, i.e. the cardinality of the generic fiber of ϕ.

PROOF. This is just a restatement of [9, appendix] to the toric case. $\square$

Denoting with $\mathrm{Res}_{\mathcal{A}}(\cdot)$ the sparse resultant operator as defined in [10], the following result gives us a way of computing the polynomial F (recall that F denotes an implicit equation of $\mathcal{V}$ and is hence defined up to a nonzero multiplicative constant):

PROPOSITION 3.3. *With the same assumptions as in Theorem 3.2 we have*

$$\mathrm{Res}_{\mathcal{A}}(qX_1 - p_1, \ldots, qX_{n+1} - p_{n+1}) = F(X_1, \ldots, X_{n+1})^d$$

up to a nonzero multiplicative constant.

PROOF. The fact that the resultant operator applied to the polynomials $qX_i - p_i$ gives a non-zero constant times a power of the implicit equation follows straightforwardly from the properties of the resultant (see [9]). In order to verify that the power appearing is actually the degree of ϕ, we use the fact that $\mathrm{Res}_{\mathcal{A}}$ is actually the "Chow form" of the variety $X_{\mathcal{A}}$ and hence it is a polynomial in the Plücker coordinates, of degree $\mathbf{vol}(P)$ (see [14]). As we can use either the Plücker coordinates or the dual Plücker coordinates, it is easy to see that the dual Plücker coordinates of the vector $qX_1 - p_1, \ldots, qX_{n+1} - q_{n+1}$ have degree one in the variables X. This completes the proof. $\square$

Now we consider "homogeneous" polynomials $P_i(y_1, \ldots, y_s)$ and $Q(y_1, \ldots, y_s)$, $i = 1, \ldots, n+1$ where s is the number of facets of P, and the P_i (resp. Q) are the homogenizations of p_i (resp. q) with respect to the polytope $\mathbf{P}$ (see [7]).

For $i = 1, \ldots, n+1$, let

$$F_i(y_1, \ldots, y_s) := Q(y_1, \ldots, y_s)X_i - P_i(y_1, \ldots, y_s)$$

and regard them as polynomials in $S := \mathcal{K}[y_1, \ldots, y_s]$, where $\mathcal{K} := \mathbb{K}(X_1, \ldots, X_{n+1})$. Let ρ be the *critical degree* of the sequence $(F_1, \ldots, F_{n+1})$ as defined in [8], and consider, as in [12], the *subresultant complex*. This is the following Koszul complex associated to the sequence $(F_1, \ldots, F_{n+1})$:

$$0 \to S_{-\beta_0} \to \cdots \to \bigoplus_{i=1}^{n+1} S_{\rho-\alpha_i} \xrightarrow{\psi} S_\rho \to 0 \qquad (6)$$

where β_0 is the anticanonical divisor associated with this data (see [7]). We denote by $\mathbb{M}$ the matrix of the map ψ in any given $\mathcal{K}$-vector space bases. Observe that the entries of $\mathbb{M}$ are polynomials in $\mathbb{K}[X_1, \ldots, X_{n+1}]$ of degree at most 1.

THEOREM 3.4. *The* gcd *of all (maximal) square minors of size* $\dim_{\mathbb{K}}(S_\rho) - 1$ *of* $\mathbb{M}$ *over* $\mathbb{K}[X_1, \ldots, X_{n+1}]$ *equals* F^α*, where* $\alpha \in \mathbb{N}$*, up to a nonzero multiplicative constant. Moreover* $\alpha = 0$ *if and only if* ϕ *is proper.*

PROOF. If $G(X_1, \ldots, X_n)$ is a common factor of all the maximal minors of ψ, then G is also a common factor of all the subresultants Δ_α, with $\deg(\alpha) = \rho$ (see [12]). But it turns out that, as in [12], we can write

$$\mathrm{Res}_{\mathcal{A}}(F_1, \ldots, F_{n+1}) = \sum_{\deg(\alpha)=\rho} c_\alpha \Delta_\alpha,\ c_\alpha \in \mathbb{K}[X_1, \ldots, X_{n+1}]. \qquad (7)$$

Hence, G must divide the right-hand side, and due to Proposition 3.3, G must be a factor of F. As F is irreducible, G must be a power of F. If G has positive degree in the variables X_i's, then it can be shown that the c_α also have positive degree in the X_i's and this implies that $d > 1$. $\square$

Let us put this theorem in a more geometric context. We denote by $V_{\mathbb{M}}$ the variety in the affine space $\mathbb{A}^{n+1}$ defined as the zero locus of all square minors of size $\dim_{\mathbb{K}}(S_\rho) - 1$ of $\mathbb{M}$. Then theorem 3.4 says that the pure codimension 1 part of $V_{\mathbb{M}}$ equals

$$\begin{cases} \emptyset & \text{if } \phi \text{ is proper} \\ \mathcal{V} & \text{if } \phi \text{ is not proper.} \end{cases}$$

Consequently, checking if ϕ is proper is equivalent to checking the rank of $\mathbb{M}$ on *any* non-empty open subset of $\mathcal{V}$. We deduce the following criterion for the properness of a parametrization:

PROPOSITION 3.5. *Let* $\mathbb{M}_{\mathbf{t}}$ *be the matrix, with entries in* $\mathbb{K}(t_1, \ldots, t_n)$*, deduced from* $\mathbb{M}$ *by substituting each* X_i *with* $\frac{p_i}{q}$*. Then,* ϕ *is proper if and only if the rank of* $\mathbb{M}_{\mathbf{t}}$*, over* $\mathbb{K}(t_1, \ldots, t_n)$*, equals* $\dim(S_\rho) - 1$ *(its maximal possible value).*

PROOF. This proposition follows directly from previous observations since the image of the map ϕ contains a non-empty open subset of $\mathcal{V} \subset \mathbb{A}^{n+1}$. $\square$

REMARK 3.6. *From a computational point of view, checking if the map* ϕ *is proper consists in checking if the rank of the matrix* $\mathbb{M}_{\mathbf{t}}$ *equals its maximal possible value, which can be basically done with a simple Gaussian elimination. Notice also that, as a consequence of proposition 3.5, the properness of* ϕ *can be decided with* probability one *by considering a matrix* $\mathbb{M}_{\mathbf{t}}$ *where the variables* $t_1, \ldots, t_n$ *are specialized randomly in* $(\mathbb{K}^*)^n$*; this matrix is then a* numeric *matrix, and rank computations become quite more simple and efficient.*

4. SUBRESULTANTS AND THE INVERSION PROBLEM

In this section we will introduce toric subresultants, review some of their properties (see [12] for proofs and details) and show how to apply them to the inversion problem.

Let h be a monomial in $S = \mathcal{K}[y_1, \ldots, y_s]$ of critical degree ρ. Consider the *subresultant complex* with respect to h :

$$0 \to S_{-\beta_0} \to \cdots \to \bigoplus_{i=1}^{n+1} S_{\rho-\alpha_i} \xrightarrow{\tilde{\psi}} S_\rho/\langle h \rangle \to 0, \qquad (8)$$

where $\tilde{\psi}$ is the co-restriction of ψ defined in (6) to $S_\rho/\langle h \rangle$. It turns out (see [12]) that if h does not belong to the ideal $(F_1, \ldots, F_{n+1})$, then the complex (8) is generically exact. So, we can compute the determinant of this complex with respect to the monomial bases (see [14, appendix A] for a definition of the determinant of a complex). We will denote it with Δ_h, and will call this element the h-subresultant of $F_1, \ldots, F_{n+1}$.

PROPOSITION 4.1 ([12]). *We have:*

1. Δ_h *is a polynomial in the coefficients of the system* $F_1, \ldots, F_{n+1}$*. It is not identically zero if and only if*

$$\mathcal{K}\langle h \rangle + (F_1, \ldots, F_{n+1})_\rho = \mathcal{K}[x_1, \ldots, x_s]_\rho.$$

2. For any pair of monomials h, h' of critical degree ρ,

$$\Delta_h\, h' \pm \Delta_{h'}\, h \in (F_1, \ldots, F_{n+1})_\rho.$$

Proposition 4.1 will allow us to give an inversion formula for (1) provided that the parametrization is invertible. First, we have to find at least two integer points in the interior of $(n+1)\mathbf{P}$.

LEMMA 4.2. *Let $\mathcal{L}_\mathcal{A}$ be the lattice generated affinely by $\mathcal{A}$. The cardinality of $((n+1)\mathbf{P})^\circ \cap \mathcal{L}_\mathcal{A}$ equals to one if and only if $\mathcal{A}$ is affinely isomorphic to a set of $n+1$ points of the form $\{\mathbf{0}, d_1\mathbf{e_1}, \ldots, d_n\mathbf{e_n}\}$, where the $\mathbf{e_i}$ are the canonical vectors of $\mathbb{R}^n$ and the d_i are positive numbers. If this is the case, then the parametrization is invertible if and only if $d_1 = \ldots = d_n = 1$ and the system is non-degenerate (i.e. the toric jacobian of the F_i is not identically zero).*

PROOF. It is clear that if $\mathcal{A}$ consists of $n+1$ vectors as in the statement of the Lemma, then the parametrization is invertible if and only if the system is non-degenerate and all the d_i are equal to one. Also, if $\mathcal{A}$ is affinely isomorphic to such a set, then $\mathcal{L}_\mathcal{A}$ is affinely isomorphic to $\oplus_{i=1}^n d_i\mathbb{Z}$, and hence the only point in $((n+1)\mathbf{P})^\circ \cap \mathcal{L}_\mathcal{A}$ is the image via this isomorphism of the vector $(d_1, \ldots, d_n)$.

In order to show the converse, in [4, Proposition 1.2] it is shown that the toric jacobian of a generic system supported in $\mathcal{A}$ has its support in $((n+1)\mathbf{P})^\circ \cap \mathcal{L}_\mathcal{A}$. If there is only one integer point there, then the toric jacobian of this system is just a constant times a monomial. This constant must be the sparse resultant of the system (see [4, Theorem 2.2]). As the jacobian has degree one in the coefficients of each of the input polynomials, this shows that the normalized volume of $\mathbf{P}$ (which is the degree of the resultant) with respect to the lattice $\mathcal{L}_\mathcal{A}$ equals one, and hence $\mathbf{P}$ is a fundamental simplex in $\mathcal{L}_\mathcal{A}$. So, $\mathcal{A}$ must be affinely isomorphic to a set of the form $\{\mathbf{0}, d_1\mathbf{e_1}, \ldots, d_n\mathbf{e_n}\}$. $\square$

Lemma 4.2 says essentially that if the interior of $(n+1)\mathbf{P}$ has only one point, then the parametrization is linear and hence the inverse problem is easy to solve in this case. ¿From now on we will assume w.l.o.g. that the interior of $(n+1)\mathbf{P}$ has at least two integer points. This means that the interior of $n\mathbf{P}$ has at least one point (otherwise the complex (8) cannot be generically exact). Moreover, we have the following:

LEMMA 4.3. *If $\mathbf{vol}(\mathbf{P}) > \mathbf{1}$, then the interior of $(n+1)\mathbf{P}$ has at least $n+2$ points.*

PROOF. Consider the jacobian complex given in [4] for computing the sparse resultant of $n+1$ generic polynomials with support in $\mathcal{A}$. As each maximal minor of the last map is a multiple of the sparse resultant, and a basis of the image of the last map is given by the integer points lying in $(n+1)\mathbf{P}$, then

$$\#\left((n+1)\mathbf{P}\right)^\circ \cap \mathbb{Z}^n \geq \deg\left(\mathrm{Res}_\mathcal{A}\right) - n = (n+1)\mathbf{vol}(\mathbf{P}) - n.$$

$\square$

PROPOSITION 4.4. *For all $i \in \{1, \ldots, n\}$ let h_i, h_i' be the homogenizations of $\mathbf{p_i}, \mathbf{p_i} + \mathbf{e_i}$ (two points of $\mathcal{A}$) with respect to $\mathbf{P}$ respectively, and $\tilde{h}$ be the homogenization of any point in the interior of $n\mathbf{P}$ with respect to $(n\mathbf{P})^\circ$. If (1) is invertible then*

$$(t_1, \ldots, t_n) \mapsto (\pm\frac{\Delta_{\tilde{h}h_1'}}{\Delta_{\tilde{h}h_1}}, \ldots, \pm\frac{\Delta_{\tilde{h}h_n'}}{\Delta_{\tilde{h}h_n}}) \tag{9}$$

is an inversion of the parametrization.

PROOF. First notice that for all i $\Delta_{\tilde{h}h_i}$ is non-zero, similarly to remark 2.1; and in fact all the Δ_h with h the homogenization of any point in the interior of $(n+1)P$ with respect to $(n+1)P$ is non-zero. Now due to Proposition 4.1, it turns out that $\Delta_{\tilde{h}h_i}\tilde{h}h_i' \pm \Delta_{\tilde{h}h_i'}\tilde{h}h_i$ is in the homogeneous ideal generated by the F_i's. Dehomogenizing and using the original coordinates, we have that $\Delta_{\tilde{h}h_i}t^\alpha t_i \pm \Delta_{\tilde{h}h_i'}t^\alpha$ must vanish on $\mathcal{V}$ for some monomial t^α. Hence, the inversion formula holds. $\square$

We did not clarify the signs involved in this proposition to not overload the notations. We believe that it should be clear to the reader how to choose the signs. Moreover we will describe this precisely in the next sections when dealing with an algorithmic version of this result and some examples.

REMARK 4.5. *Proposition 4.4 may be regarded as a "general inversion formula" in the sense that it only depends on the set $\mathcal{A}$ and works for generic parametrizations. We will see in the following section that in practice we do not need to compute determinants of complexes, just maximal minors of Sylvester matrices, as in [12].*

5. MATRIX FORMULATION FOR THE INVERSION PROBLEM

In this section we will focus on the case $n = 2$ in order to make the statements and examples easier to follow, its generalization to larger values of n being straightforward. We suppose that the polynomials p_1, p_2, p_3 and q satisfy conditions 1 and 2 given in section 3.

We do not need to compute the whole complex (6) or even pass to toric coordinates in order to use the previous results. All we need is the last map ψ whose Sylvester-type matrix $\mathbb{M}$ is:

$$\begin{array}{ccc} {\mathcal{S}_{int(2\mathbf{P})}}^3 & \to & \mathcal{S}_{int(3\mathbf{P})} \\ (A_1, A_2, A_3) & \mapsto & \sum_{i=1}^3 A_i(qX_i - p_i), \end{array} \tag{10}$$

where $\mathcal{S}_{int(2\mathbf{P})}$ (resp. $int(3\mathbf{P})$) denotes the $\mathbb{K}$-vector space generated by monomials whose exponents have integer coordinates and lie in the interior of the polygon $2\mathbf{P}$ (resp. $3\mathbf{P}$).

The size of $\mathbb{M}$ depends on the polygon $\mathbf{P}$ as follows. Let $\mathbf{a}$ be the area of $\mathbf{P}$ and $\mathbf{b}$ be the number integer points lying in the boundary or $\mathbf{P}$. Then, due to Ehrart reciprocity, it turns out that the rank of the co-domain of ψ is $9\mathbf{a} - \frac{3}{2}\mathbf{b} + 1$ and the dimension of the domain is $3(4\mathbf{a} - \mathbf{b} + 1)$.

In [11], a lifting algorithm is proposed in order to get a submatrix of ψ of maximal rank, but the algorithm works in the generic case, so we cannot use it straightforwardly here. We can also adapt the resultant-based method presented in [15, Chapter 15] and work with the resultant matrices presented in [3], but their size is larger than the subresultants we are considering here. In this case, the resultant matrices of Canny and Emiris are of order $9\mathbf{a} + \frac{3}{2}\mathbf{b} + 1$.

Once we know that the parametrization is invertible, it turns out that the rank of ψ equals $\mathbf{r} := \dim\left(\mathcal{S}_{int(3\mathbf{P})}\right) - 1$. Then, we may compute the inverse as in (5): by deleting some columns in $\mathcal{M}$, choose a submatrix M_ψ of the matrix of ψ in the monomial bases having maximal rank; it will have size $(\mathbf{r}+1)\times\mathbf{r}$. For any $(\alpha,\beta)\in int(3\mathbf{P})\cap\mathbb{Z}^2$, let $m^{\alpha,\beta}$ be the $\mathbf{r}\times\mathbf{r}$ signed determinant of the square matrix made by deleting the row indexed by (α,β) in M_ψ.

Proposition 5.1. *Let (α_1,β_1) and (α_2,β_2) be points in $int(3\mathbf{P})\cap\mathbb{Z}^2$ such that both points (α_1+1,β_1) and (α_2,β_2+1) are also in $int(3\mathbf{P})\cap\mathbb{Z}^2$. The inversion of the parametrization is induced by*

$$t_1 := \frac{m^{\alpha_1+1,\beta_1}}{m^{\alpha_1,\beta_1}} \quad t_2 := \frac{m^{\alpha_2,\beta_2+1}}{m^{\alpha_2,\beta_2}}.$$

Proof. This follows straigthforwardly from Proposition 4.4 due to the fact that the maximal minors of M_ψ are actually subresultants times a constant factor (the same for all the maximal minors of M_ψ). This factor gets cancelled in the quotient, and we get (9). We can also argue as follows: by using Cramer's rule on M_ψ, it turns out that $m^{\alpha_1+1,\beta_1}+m^{\alpha_1,\beta_1}t_1$ lies in the image of ψ, i.e. vanishes in $\mathcal{V}$. As m^{α_1,β_1} does not vanish, we can get t_1 by equating to zero this expression. An analogue reasoning leads to the other expression for t_2. □

Remark 5.2. *The fact that we can find integer points satisfying the hypothesis of Proposition 5.1 is a consequence of Lemma 4.3.*

6. EXAMPLES

In this section we provide examples, mostly taken from [17, appendix], to show how our method works in the case $n=2$. We implemented the algorithm in Maple and ran it on a Pentium III 700 Mhz with 256M of RAM. The timing of computations given hereafter aim only at underlying the potentiality of this subresultant-based method to solve both properness and inversion problems.

Example 6.1: We begin with the following simple example [17, example P_9]:

$$\left\{\begin{array}{rcl} p_1(t_1,t_2) &=& {t_1}^2+{t_1}^2t_2-t_1, \\ p_2(t_1,t_2) &=& t_2-t_1, \\ p_3(t_1,t_2) &=& t_1+t_2, \\ q(t_1,t_2) &=& t_1-{t_1}^2+t_2. \end{array}\right.$$

The interior points of the polytopes $2\mathbf{P}$ and $3\mathbf{P}$ are respectively

$$[{t_1}^2t_2, {t_1}^3t_2], \quad \text{and}$$

$$[{t_1}^3t_2, {t_1}^4t_2, {t_1}^5t_2, {t_1}^2{t_2}^2, {t_1}^3{t_2}^2, {t_1}^4{t_2}^2, {t_1}^5{t_2}^2].$$

The matrix $\mathbb{M}$ is hence a 6×7-matrix (meaning 6 lines and 7 columns); its computation and the computation of its rank, which is 6, takes 0.03s. Here it is:

$$\left(\begin{array}{cccccc} -1-X_1 & 0 & -1-X_2 & 0 & -X_3+1 & 0 \\ 1+X_1 & -1-X_1 & X_2 & -1-X_2 & X_3 & -X_3+1 \\ 0 & 1+X_1 & 0 & X_2 & 0 & X_3 \\ -X_1 & 0 & 1-X_2 & 0 & -X_3+1 & 0 \\ 0 & -X_1 & 0 & 1-X_2 & 0 & -X_3+1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{array}\right).$$

From the monomial basis indexing $3\mathbf{P}$ we deduce that

$$t_1 = \frac{\Delta_2}{\Delta_1}, \quad t_2 = \frac{\Delta_5}{\Delta_1},$$

where Δ_i denotes the signed determinant of the submatrix of $\mathbb{M}$ obtained by erasing the ith line.

Example 6.2: Our second example corresponds to the parameterized surface [17, example P_6]:

$$\left\{\begin{array}{rcl} p_1(t_1,t_2) &=& t_2+2\,t_1\,t_2-3\,{t_1}^2-{t_2}^2, \\ p_2(t_1,t_2) &=& 3+t_2+2\,t_1+2\,t_1\,t_2+3\,{t_1}^2, \\ p_3(t_1,t_2) &=& 1+2\,t_2+2\,t_1-2\,t_1\,t_2-2\,{t_1}^2, \\ q(t_1,t_2) &=& 1. \end{array}\right.$$

The interior points of the polytopes $2\mathbf{P}$ and $3\mathbf{P}$ are respectively

$$[t_1t_2, {t_1}^2t_2, t_1{t_2}^2] \text{ and}$$

$$[t_1t_2, {t_1}^2t_2, {t_1}^3t_2, {t_1}^4t_2, t_1{t_2}^2, {t_1}^2{t_2}^2, {t_1}^3{t_2}^2, t_1{t_2}^3, {t_1}^2{t_2}^3, t_1{t_2}^4].$$

The matrix $\mathbb{M}$ is hence a 9×10-matrix; its computation as well as the computation of its rank, returning 9, take together 0.03s. From there it follows that an inversion is obtained by

$$t_1 = \frac{\Delta_2}{\Delta_1}, \quad t_2 = \frac{\Delta_5}{\Delta_1},$$

with the same notations that in the previous example. If one is interested in the developed result, its computation is completed in 0.2s (but the result is too large to be printed in the text). However note that it is often useful to keep matrix formulation in many cases: this is, with the universal property, a radical advantage of resultant-based methods.

Example 6.3: Our third example is bigger than both previous ones. It corresponds to the following parameterized surface [17, example P_{15}]

$$\left\{\begin{array}{rcl} p_1(t_1,t_2) &=& 3t_2+3{t_1}^2t_2-{t_2}^3, \\ p_2(t_1,t_2) &=& 3t_1+3{t_2}^2t_1-{t_1}^3, \\ p_3(t_1,t_2) &=& 3{t_2}^2-3{t_1}^2, \\ q(t_1,t_2) &=& 1. \end{array}\right.$$

The matrix $\mathbb{M}$ we computed is a 28×30-matrix; its computation as well as the computation of its rank, returning 27, take together 0.05s. The monomial basis indexing $int(2\mathbf{P})$ and $int(3\mathbf{P})$ we obtained are respectively

$$[t_1t_2, {t_1}^2t_2, {t_1}^3t_2, {t_1}^4t_2, {t_2}^2t_1, {t_1}^2{t_2}^2, {t_1}^3{t_2}^2, t_1{t_2}^3, {t_1}^2{t_2}^3, t_1{t_2}^4]$$

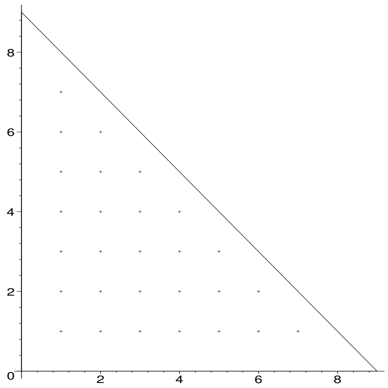
and

$$[t_1t_2, {t_1}^2t_2, {t_1}^3t_2, {t_1}^4t_2, {t_1}^5t_2, {t_1}^6t_2, {t_1}^7t_2, {t_2}^2t_1, {t_1}^2{t_2}^2, {t_1}^3{t_2}^2,$$

$${t_1}^4{t_2}^2, {t_1}^5{t_2}^2, {t_1}^6{t_2}^2, t_1{t_2}^3, {t_1}^2{t_2}^3, {t_1}^3{t_2}^3, {t_1}^4{t_2}^3, {t_1}^5{t_2}^3, t_1{t_2}^4,$$

$${t_1}^2{t_2}^4, {t_1}^3{t_2}^4, {t_1}^4{t_2}^4, t_1{t_2}^5, {t_1}^2{t_2}^5, {t_1}^3{t_2}^5, t_1{t_2}^6, {t_1}^2{t_2}^6, t_1{t_2}^7].$$

The one indexing $int(3\mathbf{P})$ can be represented in the following usual picture (where t_1 and t_2 are represented by the coordinate axes):



It follows that an inversion is obtained, for instance, with

$$t_1 = \frac{\Delta_2}{\Delta_1}, \quad t_2 = \frac{\Delta_7}{\Delta_3}.$$

Example 6.4: Finally, we would like to end this section by emphasizing the *universal* property of resultant-based methods that we had already mentioned in remark 4.5. In the case of the inversion problem this means that we can pre-compute the matrix $\mathbb{M}$ by advance for some classes of surfaces; these classes are defined by the non-vanishing of the corresponding resultant used in proposition 3.3. Let us take a concrete example. The second example we treated above fits into the class of surfaces parameterized by dense polynomials of degree 2 (in variables t_1, t_2). In this way we can apply our algorithm with the "generic" parametrization

$$\begin{cases} p_1(t_1,t_2) & = c_{1,0} + c_{1,1}t_1 + c_{1,2}t_2 + c_{1,3}t_1t_2 + c_{1,4}t_1^2 + c_{1,5}t_2^2, \\ p_2(t_1,t_2) & = c_{2,0} + c_{2,1}t_1 + c_{2,2}t_2 + c_{2,3}t_1t_2 + c_{2,4}t_1^2 + c_{2,5}t_2^2, \\ p_3(t_1,t_2) & = c_{3,0} + c_{3,1}t_1 + c_{3,2}t_2 + c_{3,3}t_1t_2 + c_{3,4}t_1^2 + c_{3,5}t_2^2, \\ q(t_1,t_2) & = c_{0,0} + c_{0,1}t_1 + c_{0,2}t_2 + c_{0,3}t_1t_2 + c_{0,4}t_1^2 + c_{0,5}t_2^2, \end{cases}$$

where the $c_{i,j}$'s are viewed as formal parameters (i.e.as variables with weight zero). We thus obtain a 9×10-matrix $\mathbb{M}$ whose entries are polynomials in the $c_{i,j}$'s, and also a *universal* solution to the inversion problem. It follows that for any specialization of this particular class of surfaces, as the second example treated above, we just have to specialize the $c_{i,j}$'s in the *universal* solution that we had pre-computed to obtain the result.

7. FUTURE WORK

It would be interesting to have a"mixed version" of these results. To be more precise, suppose that the parametrization is of the form $X_i = \frac{p_i(t)}{q_i(t)}$, with $supp(p_i, q_i) \subset \mathcal{A}_i$, and the family $\mathcal{A}_1, \ldots, \mathcal{A}_{n+1} \subset \mathbb{Z}^n$ "essential" as defined in [20]. There is a toric variety associated with this data (see [14]), and a sparse resultant operator $\mathrm{Res}_{\mathcal{A}_1,\ldots,\mathcal{A}_n}$ such that, if the polynomials $p_i(t), q_i(t)$, $i = 1, \ldots, n+1$ do not have a common zero in this toric variety, then

$$\mathrm{Res}_{\mathcal{A}_1,\ldots,\mathcal{A}_n}(q_1(t)X_1 - p_1(t), \ldots, q_{n+1}X_{n+1} - p_{n+1}) = F(X)^d$$

for some positive number d. It should be interesting to relate this number d with the degree of the map ϕ. Are they always the same? If so, one could apply the theory of sparse subresultants to this context, and get smaller and more compact matrices for solving the properness/inversion problem as the following example shows.

EXAMPLE 7.1. *This parametrization is extracted from [17, example P_1]:*

$$\begin{cases} X_1 & = & \frac{t_1}{t_1+t_2} \\ X_2 & = & \frac{t_1^2-t_1+1}{t_2+1} \\ X_3 & = & t_1^2 + t_2 \end{cases}$$

We can consider F_1 as a polynomial of total degree 1 and F_2, F_3 having both total degrees 2. Then we get the following more compact matrix in critical degree:

$$\mathbb{M}_2 := \begin{pmatrix} X_2-1 & 1 & X_2 & -1 & 0 & 0 \\ X_3 & 0 & -1 & -1 & 0 & 0 \\ 0 & X_1-1 & X_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & X_1-1 & X_1 & 0 \\ 0 & 0 & 0 & 0 & X_1-1 & X_1 \end{pmatrix}.$$

The maximal minors of this matrix are subresultants:

$$\begin{aligned} \Delta_1 &= -X_1^2(X_2X_1 - 1 - X_2) \\ \Delta_{t_1} &= X_1^3(X_2 - 1 - X_3) \\ \Delta_{t_2} &= X_1^2(X_2 - 1 - X_3)(X_1 - 1) \\ \Delta_{t_2^2} &= (X_1-1)^2 \times \\ & (X_2X_1 - X_2 - X_1 + 1 - X_1X_3 + X_1X_2X_3 - X_2X_3) \end{aligned}$$

and from here we can solve the inverse problem:

$$\begin{aligned} t_1 &= -\frac{\Delta_{t_1}}{\Delta_1} = \frac{X_1(X_2-1-X_3)}{X_2X_1-1-X_2} \\ t_2 &= \frac{\Delta_{t_2}}{\Delta_1} = \frac{X_2X_1-X_2-X_1+1-X_1X_3+X_3}{X_2X_1-1-X_2} \end{aligned}$$

In another direction, it would be interesting to understand to what extent these methods can be applied to the case where base points are present. One can show that if the zero locus of the variety defined by $p_1, \ldots, p_{n+1}, q$ in $X_{\mathcal{A}}$ is not empty, then the sparse resultant is identically zero, but if there is only one single solution, then the subresultants in critical degree cannot be all zero.Moreover, one can recover this common solution as in [22]. Can we adapt this method to the case where the base points are finite and local complete intersection, as it was shown in [13]? Also, it would be interesting to know if one can use residual resultants for solving inversion and properness problems in the presence of base points. In [1] it was shown that these resultants can be used to solve the implicitization problem, giving a result similar to proposition 3.3, but it remains to introduce an appropriate notion of *residual subresultants* in order to obtain all the needed tools for the inversion and properness problems.

8. REFERENCES

[1] Busé, Laurent. *Residual resultant over the projective plane and the implicitization problem.* In B. Mourrain, editor, *Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation*, pages 48–55, London, Ontario, 2001. New-York, ACM Press.

[2] Busé, Laurent; Elkadi, Mohamed; Mourrain Bernard. *Using projection operators in computer aided geometric design.* In *Topics in Algebraic Geometry*

and Geometric Modeling. AMS Press, Contemporary Mathematics 334, 2003.

[3] Canny, John F.; Emiris, Ioannis Z. *A subdivision-based algorithm for the sparse resultant.* J. ACM 47 (2000), no. 3, 417–451.

[4] Cattani, Eduardo; Dickenstein, Alicia; Sturmfels, Bernd. *Residues and resultants.* J. Math. Sci. Univ. Tokyo 5 (1998), no. 1, 119–148.

[5] Chardin, Marc. *Multivariate subresultants.* J. Pure Appl. Algebra 101, no. 2, 129-138 (1995).

[6] Chionh, Eng-Wee; Goldman, Ronald N. *Degree, multiplicity, and inversion formulas for rational surfaces using u-resultants.* Comput. Aided Geom. Design 9, no .2, 93-108 (1992).

[7] Cox, David A. *The homogeneous coordinate ring of a toric variety.* J. Algebraic Geom. 4 (1995), no. 1, 17–50.

[8] Cox, David A. *Toric residues.* Ark. Mat. 34 (1996), no. 1, 73–96.

[9] Cox, David A. *Equations of parametric curves and surfaces via syzygies.* Symbolic computation: solving equations in algebra, geometry, and engineering (South Hadley, MA, 2000), 1–20, Contemp. Math., 286, Amer. Math. Soc., Providence, RI, 2001.

[10] Cox, David; Little, John; O'Shea, Donal. *Using algebraic geometry.* Graduate Texts in Mathematics, 185. Springer-Verlag, New York, 1998.

[11] D'Andrea, Carlos; Emiris, Ioannis Z. *Hybrid sparse resultant matrices for bivariate polynomials.* Computer algebra (London, ON, 2001). J. Symbolic Comput. 33 (2002), no. 5, 587–608.

[12] D'Andrea, Carlos; Khetan, Amit. *Macaulay style formulas for computing residues.* Preprint, 2003 `math.AG/030715`.

[13] D'Andrea, Carlos; Khetan, Amit. *Implicitization of rational surfaces with toric varieties.* Preprint, 2003.

[14] Gel'fand, I. M.; Kapranov, M. M.; Zelevinsky, A. V. *Discriminants, resultants, and multidimensional determinants.* Mathematics: Theory & Applications. Birkhuser Boston, Inc., Boston, MA, 1994.

[15] *Handbook of computer aided geometric design.* Edited by Gerald Farin, Josef Hoschek and Myung-Soo Kim. North-Holland, Amsterdam, 2002.

[16] *Parametric algebraic curves and applications.* Including papers from the IMACS-ACA Session on Parametric Curves and Applications in Computer-aided Geometric Design held at the University of New Mexico, Albuquerque, NM, May 1995. Edited by C. M. Hoffmann, J. R. Sendra and F. Winkler. J. Symbolic Comput. 23 (1997), no. 2-3. Academic Press, Oxford, 1997. pp. 133–333.

[17] Pérez-Díaz, Sonia; Schicho, Josef; Sendra, J. Rafael. *Properness and inversion of rational parametrizations of surfaces.* Appl. Algebra Engrg. Comm. Comput. 13 (2002), no. 1, 29–51.

[18] Schicho, Josef. *Inversion of birational maps with Gröbner bases.* Gröbner bases and applications (Linz, 1998), 495–503, London Math. Soc. Lecture Note Ser., 251, Cambridge Univ. Press, Cambridge, 1998.

[19] Sendra, J. Rafael; Winkler, Franz. *Symbolic parametrization of curves.* J. Symbolic Comput. 12 (1991), no. 6, 607–631.

[20] Sturmfels, Bernd. *On the Newton polytope of the resultant.* J. Algebraic Combin. 3 (1994), no. 2, 207–236.

[21] Szanto, Agnes. *Multivariate subresultants using Jouanolou's resultant matrices.* Preprint.

[22] Szanto, Agnes. *Solving overdetermined systems by subresultant methods.* Preprint.

[23] van Hoeij, Mark. *Rational parametrizations of algebraic curves using a canonical divisor.* Parametric algebraic curves and applications (Albuquerque, NM, 1995). J. Symbolic Comput. 23 (1997), no. 2-3, 209–227.