An Algorithmic Criterion for Deciding the Properness of Rational Parametrizations*

Sonia Pérez-Díaz
Dpto de Matemáticas
Universidad de Alcalá
E-28871 Madrid, Spain
sonia.perez@uah.es

Josef Schicho
RISC-LINZ
Johannes Kepler Universität
A-4040 Linz, Austria
josef.schicho@risc.uni-linz.ac.at

J. Rafael Sendra
Dpto de Matemáticas
Universidad de Alcalá
E-28871 Madrid, Spain
rafael.sendra@uah.es

Abstract

In this paper we characterize the properness of rational parametrizations of hypersurfaces by means of the existence of intersection points of some additional algebraic hypersurfaces directly generated from the parametrization over a field of rational functions. More precisely, if V is a hypersurface over an algebraically closed field of characteristic zero and $\mathcal{P}(\bar{t}) = \left(\frac{p_1(\bar{t})}{q_1(\bar{t})}, \ldots, \frac{p_n(\bar{t})}{q_n(\bar{t})}\right)$ is a rational parametrization of V, then the characterization is given in terms of the intersection points of the hypersurfaces defined by $x_i q_i(\bar{t}) - p_i(\bar{t})$, $i = 1, \ldots, n$ over the algebraic closure of $\mathbb{K}(V)$. In addition, for the case of surfaces we show how these results can be stated algorithmically. As a consequence we present an algorithmic criteria to decide whether a given rational parametrization is proper that, in the affirmative case, also computes the inverse of the parametrization. Moreover, for surfaces the auxiliary hypersurfaces turn to be plane curves over $\mathbb{K}(V)$, and hence the algorithm is essentially based on resultants. We have implemented these ideas, and we have empirically compared our method with the method based on Gröbner basis.

*First and third authors partially supported by DGES PB98-0713-C02-01 and and DGES HU1999-0029. Second author partially supported by the Austrian Science Fund (FWF) in the frame of the SFB 013.

Introduction

Unirational algebraic varieties, specially rational curves and surfaces, play an important role in the frame of practical applications (see [8],[9],[10]). Many authors have addressed problems related to the construction of conversion algorithms for these type of varieties; i.e. algorithmic methods that change from the implicit representation to the parametric one, and viceversa (see [3], [6], [7], [9], [11], [12], [15], [16], [17], etc).

In addition, if one considers the rational parametrization as a rational mapping from an affine space onto the variety, two natural questions appears. First, deciding whether the mapping is birational (i.e. whether the parametrization is proper); secondly, in case of birationality, the question of computing the inverse of the parametrization is considered. More precisely, let $\mathcal{P}(t_1, \ldots, t_r)$ be a rational parametrization of a variety V over an algebraically closed field of characteristic zero. Then $\mathcal{P}$ defines the rational mapping

$$\begin{array}{rccc} \mathcal{P}: & \mathbb{K}^r & \longrightarrow & V \\ & (t_1, \ldots, t_r) & \longmapsto & \mathcal{P}(t_1, \ldots, t_r) \end{array}$$

Thus, we study the question of deciding whether $\mathcal{P}$ is proper (i.e. invertible). Moreover, in the affirmative case, we want to compute the rational inverse of $\mathcal{P}$, i.e. a rational mapping assigning to every point, in a non-empty Zariski subset of V, the corresponding parameter value.

An algorithm approach to the most general case, based on Gröbner Basis, can be found in [13]. We, in this paper, deal with the case of hypersurfaces. For plane curves, the problem is directly related to Lüroth's theorem, that is valid over any field, and different algorithmic procedures to solve the problem can be found in [1], [2], [14], [19]. For surfaces, although it is known from Castelnuovo's theorem that unirationality and rationality are equivalent over algebraically closed fields, algorithmic questions and approaches are still required. It is also interesting to remark that the knowledge of the inverse provides an alternative method to compute the implicit equation of the surface.

In this paper we present a criteria for deciding the properness of rational parametrizations of hypersurfaces, based on the existence of intersection points of some algebraic hypersurfaces over the field of rational functions of the given hypersurface. For the case of surfaces, these auxiliary hypersurfaces turn to be plane curves, and therefore the problem is solved by means of resultants. Furthermore, the general criteria can be stated algorithmically. As a consequence of these results we present an algorithm that decides whether a given rational parametrization is proper, and in the affirmative case computes the inverse. Moreover, we have implementated these ideas in Maple. We have designed two prototypes of the algorithm, one deterministic and the second heuristic, and actual computing times in comparison to the method based on Gröbner bases are analyzed.

The structure of the paper is as follows: In Section 1 we prove the characterization of the properness of rational parametrizations of hypersurfaces. In Section 2 we show how these results can be improved in order to derive an algorithmic approach. Section 3 is devoted to outline the algorithm and examples. Section 4 focusses on the actual computing times of our implementations.

1 Characterization of the Properness

In this section we show how to characterize the birationality of a rational parametrization of a hypersurface over an algebraically closed field of characteristic zero by means of some auxiliary hypersurfaces constructed directly from the parametrization. This result provides a constructive method for checking the properness of rational parametrizations of hypersurfaces, and for computing the inverse, if a method for determining intersection points is given. Applications of this statement can be seen in the next section.

We start with a lemma that characterizes the birationality of parametrizations in terms of the injectivity.

LEMMA 1. Let $\mathbb{F}$ be an algebraically closed field of characteristic zero,

$$\begin{array}{rccc} \mathcal{Q}: & \mathbb{F}^{n-1} & \longrightarrow & V \subset \mathbb{F}^n \\ & \overline{t} & \longmapsto & (\mathcal{Q}_1,(\overline{t}),\ldots,\mathcal{Q}_n(\overline{t})) \end{array}$$

be a rational parametrization of a hypersurface V. Let

$$\begin{array}{rccc} \mathcal{U}: & V & \longrightarrow & \mathbb{F}^{n-1} \\ & \overline{x} & \longmapsto & (\mathcal{U}_1,(\overline{x}),\ldots,\mathcal{U}_{n-1}(\overline{x})) \end{array}$$

be a rational map, where the denominators of $\mathcal{U}$ do not belong to the ideal of V. The following statements are equivalent:

(1.) $\mathcal{U}$ is the inverse of $\mathcal{P}$.

(2.) For almost all points $\overline{x} \in V$, it holds that $\overline{x} = \mathcal{Q}(\mathcal{U}(\overline{x}))$.

(3.) For almost all points $\overline{t} \in \mathbb{F}^{n-1}$, it holds that $\overline{t} = \mathcal{U}(\mathcal{Q}(\overline{t}))$.

PROOF.
By definition, (2) is an explicit way of saying that the composition $\mathcal{Q} \circ \mathcal{U} : V \to V$ is defined and is the identity as a rational map, and (3) is an explicit way of saying that $\mathcal{U} \circ \mathcal{Q} : \mathbb{F}^{n-1} \to \mathbb{F}^{n-1}$ is defined and is the identity. This shows that (1) implies both (2) and (3), and that the conjunction of (2) and (3) implies (1).
By definition of "parametrization", $\mathcal{Q}$ is a *dominant* rational map from $\mathbb{F}^{n-1}$ to V, i.e. its image is Zariski dense. We show indirectly that either (2) or (3) implies that also $\mathcal{U}$ is dominant. Indeed: if $\mathcal{U}$ would not be dominant, then we would have a rational

map (either $\mathcal{Q} \circ \mathcal{U}$ or $\mathcal{U} \circ \mathcal{Q}$) between two varieties of dimension $n-1$ factoring through a set of strictly lower dimension. But on the other hand, this map is supposed to be the identity, which is clearly dominant. Thus this is a contradiction, and then $\mathcal{U}$ is dominant.
It is well-known (see [5], p. 77) that dominant maps induce field embeddings. Hence we have field embeddings $\mathcal{Q}^* : \mathbb{F}(V) \to \mathbb{F}(\bar{t})$ and $\mathcal{U}^* : \mathbb{F}(\bar{t}) \to \mathbb{F}(V)$.
Next we show that (2) implies (3). Let us assume (2). Then the composite field embedding $\mathcal{U}^* \circ \mathcal{Q}^* : \mathbb{F}(V) \to \mathbb{F}(V)$ is the identity. It follows that

$$\mathcal{U}^* \circ \mathcal{Q}^* \circ \mathcal{U}^* = \mathcal{U}^* \circ id_{\mathbb{F}(\bar{t})}.$$

Because of $\mathcal{U}^*$ is injective and therefore left cancelable, it follows that $\mathcal{Q}^* \circ \mathcal{U}^* = id_{\mathbb{F}(\bar{t})}$, which is equivalent to (3).
The proof of the implication (3)$\to$(2) is analogous. $\square$.

We observe that from Lemma 1 one might derive two methods to compute the inverse. The first one uses statement (3), and deals with linear conditions, provided some assumptions on the degree. A second approach may be based on statement (2), and leads to algebraic equations over the field of rational funcitions over the hypersurface. Even though, the second method seems to be more complicated, we will see that it leads to better algorithms where no assumptions on the degree have to be taken. Furthermore, if one works with surfaces, the algebraic equations that appear in the method can be resolved by means of resultants.

Once we have this general statement we introduce the notation that will be use in the sequel. Let $\mathbb{K}$ be an algebraically closed field of characteristic zero, $F \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ an irreducible polynomial defining a unirational hypersurface V, and let

$$\mathcal{P}(t_1, \ldots, t_{n-1}) = \left(\frac{p_1(t_1, \ldots, t_{n-1})}{q_1(t_1, \ldots, t_{n-1})}, \ldots, \frac{p_n(t_1, \ldots, t_{n-1})}{q_n(t_1, \ldots, t_{n-1})} \right) \in \mathbb{K}(t_1, \ldots, t_{n-1})^n$$

be a rational parametrization of V, such that $\gcd(p_i, q_i) = 1 \;\; \forall i \in \{1, 2, \ldots, n\}$.
Also let K the algebraic closure of the field $\mathbb{K}(V)$.

In this situation, we consider the affine hypersurfaces $V_1, V_2, \ldots, V_n$ defined, respectively, over K by the polynomials

$$G_i(t_1, \ldots, t_{n-1}) = x_i q_i(t_1, \ldots, t_{n-1}) - p_i(t_1, \ldots, t_{n-1}) \in \mathbb{K}(V)[t_1, \ldots, t_{n-1}], \;\; \forall i \in \{1, \ldots, n\}.$$

Finally let us also consider the affine hypersurface V_{n+1} defined, over K by the polynomial

$$G_{n+1}(t_1, \ldots, t_{n-1}) = lcm(q_i(t_1, \ldots, t_{n-1}), \ldots, q_n(t_1, \ldots, t_{n-1})) \in \mathbb{K}(V)[t_1, \ldots, t_{n-1}].$$

The next theorem characterize the properness of the parametrization $\mathcal{P}(t_1, \ldots, t_{n-1})$ by means of intersection points of the hypersurfaces $V_1, \ldots, V_n$ defined above.

THEOREM 1. The following statements are equivalent:

(1.) The parametrization $\mathcal{P}(t_1, \ldots, t_{n-1})$ is proper.

(2.) There exists exactly one point $A = (A_1, A_2, \ldots, A_{n-1}) \in [(V_1 \cap V_2 \cap \cdots \cap V_n) \setminus (V_1 \cap V_2 \cap \cdots \cap V_n \cap V_{n+1})] \cap K^{n-1}$.

Furthermore, if (2) holds, then A is the inverse of $\mathcal{P}$.

PROOF.
$\boxed{(1)\Rightarrow(2)}$ Let $\overline{x} = (x_1, \ldots, x_n)$, and $M = (M_1(\overline{x}), M_2(\overline{x}), \ldots, M_{n-1}(\overline{x}))$ be the inverse of the rational proper parametrization $\mathcal{P}(t_1, \ldots, t_{n-1})$. Then,

$$\mathcal{P}(M) = \overline{x} \;\; mod \;\; I(V)$$

Therefore, crossing out denominators one gets that

$$M \in V_1 \cap V_2 \cap \cdots \cap V_n \cap K^{n-1}$$

Furthermore, since M is the inverse of the parametrization one has that $q_i(M)$ is not zero $\forall i \in \{1, \ldots, n\}$, and then $M \notin V_{n+1}$. Hence, $M \in [(V_1 \cap V_2 \cap \cdots \cap V_n) \setminus (V_1 \cap V_2 \cap \cdots \cap V_n \cap V_{n+1})] \cap K^{n-1}$.
Finally, let us see that M is unique. Let $M^* \in K^{n-1} \cap [(V_1 \cap V_2 \cap \cdots \cap V_n) \setminus (V_1 \cap V_2 \cap \cdots \cap V_n \cap V_{n+1})]$. Taking into account that $M^* \notin V_{n+1}$, one obtains that $q_i(M^*)$ is not zero $\forall i \in \{1, \ldots, n\}$. Therefore the equalities $G_i(M^*) = 0 \;\; \forall i \in \{1, \ldots, n\}$ imply that

$$\mathcal{P}(M^*) = \overline{x} \;\; mod \;\; I(V)$$

Thus, $\mathcal{P} \circ M^* = id_V$. Hence, left composing by $\mathcal{P}^{-1}$, one concludes that $M^* = \mathcal{P}^{-1} = M$.
$\boxed{(2)\Rightarrow(1)}$ Since there exists a unique point in $[(V_1 \cap V_2 \cap \cdots \cap V_n) \setminus (V_1 \cap V_2 \cap \cdots \cap V_n \cap V_{n+1})] \cap K^{n-1}$, A is fixed under the action of the Galois group. Therefore, $A \in \mathbb{K}(V)^{n-1}$. Reasoning as we did for the uniqueness in the previous implication, one gets that $\mathcal{P} \circ A = id_V$. Now applying Lemma 1 one gets (1). $\square$.

EXAMPLE 1. Let V be the hypersurface in $\mathbb{C}^4$ defined by the irreducible polynomial

$$\begin{gathered} F(x,y,z,w) = \; -8\,x\,y + 2\,y^2 + 4\,y^2 z - 3\,y^2 w + 16\,x\,y^2 - 24\,x^2\,y + \\ +16\,x^2\,y^2 + 16\,x^3 + 16\,x^2\,z - 14\,x^2\,w + 12\,x\,y\,w - 16\,x\,y\,z + 8\,x^2 + \\ +42\,x\,y^2\,w + 16\,x\,y^2\,z - 4\,y^3 - 3\,y^2 z\,w - 8\,x\,z^2\,y + 12\,x\,y\,z\,w + 8\,x^2\,z^2 + \\ +3\,w^2 x^2 - 14\,w\,x^2\,z - 16\,x^3\,y + 16\,x^3\,z + 36\,x^3\,w - 76\,x^2\,y\,w - \\ -24\,x^2\,y\,z + 8\,x^4 + 2\,y^2 z^2 + 2\,y^4 - 4\,y^3\,z - 8\,y^3\,x - 6\,y^3\,w \in \mathbb{C}[x,y,z,w] \end{gathered}$$

and the rational parametrization

$$\mathcal{P}(t_1,t_2,t_3) = \left(\frac{t_1-1}{t_3+t_1^2+1}, \frac{2\,t_1-t_2}{t_3+t_1^2+1}, \frac{2\,t_2-t_3}{t_3+t_1^2+1}, \frac{t_2^2}{t_3+t_1^2+1}\right)$$

Let us check whether $\mathcal{P}(t_1,t_2,t_3)$ is a proper parametrization.
Taking into account Theorem 1, we have to analyze the intersection points of the four curves V_1, V_2, V_3, V_4, defined respectively over $\overline{\mathbb{C}(V)}$ by the polynomials

$$\begin{cases} G_1(t_1,t_2,t_3) = \; x\,t_3 + x\,t_1^2 + x - t_1 + 1, \\ G_2(t_1,t_2,t_3) = \; y\,t_3 + y\,t_1^2 + y - 2\,t_1 + t_2, \\ G_3(t_1,t_2,t_3) = \; z\,t_3 + z\,t_1^2 + z - 2\,t_2 + t_3, \\ G_4(t_1,t_2,t_3) = \; w\,t_3 + w\,t_1^2 + w - t_2^2. \end{cases}$$

Let us consider the point $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3) \in \mathbb{C}(V)$ with

$$\mathcal{A}_1 = \frac{-2\,x + 3\,y^2 - 2\,x^2 - 4\,x\,y + 3\,x\,w - 2\,x\,z}{10\,x^2 + 3\,y^2 - 12\,x\,y},$$

$$\mathcal{A}_2 = \frac{-2\,y^2 + 2\,y + 4\,x\,y - 3\,y\,w + 2\,z\,y + 6\,x\,w - 4\,x - 4\,x^2 - 4\,x\,z}{10\,x^2 + 3\,y^2 - 12\,x\,y},$$

$$\mathcal{A}_3 = \frac{-4\,y^2 - 6\,y\,w - 4\,z\,y + 8\,x\,y + 4\,y - 8\,x}{10\,x^2 + 3\,y^2 - 12\,x\,y} + \\ + \frac{-8\,x^2 - 3\,z\,w + 12\,x\,w + 4\,x\,z + 2\,z + 2\,z^2}{10\,x^2 + 3\,y^2 - 12\,x\,y}.$$

It verifies, for instance using Gröbner Basis, that

$$\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3) \in V_1 \cap V_2 \cap V_3 \cap V_4,$$

and that

$$\mathcal{A}(\mathcal{P}(t_1,t_2,t_3)) = (t_1,t_2,t_3).$$

Thus, applying Theorem 1, we deduce that $\mathcal{P}$ is proper and the inverse mapping is $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$. $\square$

2 Application to Surfaces

In this section, we show how to apply Theorem 1 to the special case of surfaces. The particular case of planes curves can be treated similarly, but we do not deal with it in this paper. For surfaces, Theorem 1 can be improved such that algorithmic characterizations based on resultants can be stated. As a consequence of these results an algorithm for deciding the properness and for computing the inverse, if it exists, is derived.

In this situation, the notation introduced in Section 1 is adapted as follows: $F \in \mathbb{K}[x, y, z]$ is an irreducible polynomial defining a rational surface V, and

$$\mathcal{P}(t_1, t_2) = \left(\frac{p_1(t_1, t_2)}{q_1(t_1, t_2)}, \frac{p_2(t_1, t_2)}{q_2(t_1, t_2)}, \frac{p_3(t_1, t_2)}{q_3(t_1, t_2)} \right) \in \mathbb{K}(t_1, t_2)^3$$

is a rational parametrization of V, where $\gcd(p_i, q_i) = 1 \ \ \forall i \in \{1, 2, 3\}$. In this situation, V_1, V_2, V_3 are the plane curves defining, respectively, over K (we recall that K is an algebraically closed field of characteristic zero) by the polynomials

$$\begin{array}{l} G_1(t_1, t_2) = x q_1(t_1, t_2) - p_1(t_1, t_2), \\ G_2(t_1, t_2) = y q_2(t_1, t_2) - p_2(t_1, t_2), \\ G_3(t_1, t_2) = z q_3(t_1, t_2) - p_3(t_1, t_2). \end{array}$$

Furthermore, we introduce a new curve V_4 that is defined over K by the polynomial $G_4(t_1, t_2) = lcm(q_1(t_1, t_2), q_2(t_1, t_2), q_3(t_1, t_2))$. Note that V_4 is empty if $\mathcal{P}(t_1, t_2)$ is a polynomial parametrization, and otherwise is a plane curve. For simplicity, we assume w.l.o.g. that $\mathcal{P}(t_1, t_2)$ does not parametrize a plane. Note that the problem for plane parametrizations is trivial. Moreover, one can check whether $\mathcal{P}(t_1, t_2)$ corresponds to a plane by introducing undermined coefficients a, b, c, d and solving the linear system of equations generated by the equality $a\frac{p_1(t_1,t_2)}{q_1(t_1,t_2)} + b\frac{p_2(t_1,t_2)}{q_2(t_1,t_2)} + c\frac{p_3(t_1,t_2)}{q_3(t_1,t_2)} = d$.

In the next Lemma we analyze the intersection points of the auxiliary curves V_1, V_2, V_3, V_4 introduced at the beginning of this section.

Lemma 1. The intersection points of the curves V_1, V_2, V_3, V_4, are in $\mathbb{K}^2$.
Proof. Let $(\alpha, \beta) \in V_1 \cap V_2 \cap V_3 \cap V_4$. Then, $G_4(\alpha, \beta) = 0$. Thus, there exists a denominator q_i that vanishes on (α, β); let us say w.l.o.g that it is q_1. Therefore, since $(\alpha, \beta) \in V_1$ it holds that

$$p_1(\alpha, \beta) = q_1(\alpha, \beta) = 0 \ \ mod \ \ I(V).$$

Now, since $gcd(p_1, q_1) = 1$, it holds that the resultant of p_1, and q_1 w.r.t. t_2 is not identically zero. Furthermore, this resultant is in $\mathbb{K}[t_1]$, and its roots are the t_1-coordinates of the intersection points of the curves given by p_1 and q_1 over $\mathbb{K}$. Hence, since $\mathbb{K}$ is algebraically closed one has that α is in $\mathbb{K}$; similarly for the t_2-coordinate. □

Applying Lemma 1, Theorem 1 can be improved for the case of surfaces. More precisely:

Theorem 2. The following statements are equivalent:

(1.) The parametrization $\mathcal{P}(t_1, t_2)$ is proper.

(2.) There exists exactly one point $A = (A_1, A_2) \ \in (V_1 \cap V_2 \cap V_3) \cap (K^2 \setminus \mathbb{K}^2)$.

(3.) There exists exactly one point $A = (A_1, A_2) \ \in (V_1 \cap V_2 \cap V_3) \cap (K \setminus \mathbb{K})^2$.

(4.) There exists exactly one point $A = (A_1, A_2) \ \in (V_1 \cap V_2 \cap V_3) \setminus (V_1 \cap V_2 \cap V_3 \cap V_4)$.

Furthermore, if either (2) or (3) or (4) holds then A is the inverse of $\mathcal{P}$.

PROOF. (1) $\Leftrightarrow$ (4) follows from Theorem 1. In order to prove that (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3) we see that $S_1 = S_2 = S_3$ where

$$S_1 = (V_1 \cap V_2 \cap V_3) \cap (K^2 \setminus \mathbb{K}^2)$$

$$S_2 = (V_1 \cap V_2 \cap V_3) \setminus (V_1 \cap V_2 \cap V_3 \cap V_4)$$

$$S_3 = (V_1 \cap V_2 \cap V_3) \cap (K \setminus \mathbb{K})^2.$$

¿From Lemma 1 one has that $S_1 \subset S_2$. Now, take $A \in S_2$. Then, reasoning as the in proof of the uniqueness of in the implication (1) $\Rightarrow$ (2) of Theorem 1, one gets that A is a right inverse of $\mathcal{P}$. Thus, no component of A can be constant, and therefore $A \in S_3$. Finally, it is clear that $S_3 \subset S_1$. $\square$.

In the following we show how one decide computationally statement (2), (3) and (4) of Theorem 2. We start with a technical result where we remark the one to one relation between the intersection points of three planes curves, C_1, C_2, C_3, without common components and the roots of a univariate polynomial computed by a resultant.

For this purpose, in the next lemma we assume w.l.o.g. that the *gcd* of each two of the leading coefficients of the defining polynomials of C_1, C_2, C_3, w.r.t. one the variables, is trivial. Note that this condition can always be achieved by a linear change of coordinates.

PROPOSITION 1. Let $\mathbb{L}$ be a subfield of an algebraically closed field $\mathbb{F}$ of characteristic zero, and let C_1, C_2, C_3 be plane algebraic curves over $\mathbb{F}$, with no common components, defined by the polynomials F_1, F_2, $F_3 \in \mathbb{L}[t_1, t_2]$, respectively. Let F_1, F_2, F_3 be such that each two of their leading coefficients, w.r.t. one the variables, have trivial gcd. Let F_1 do not have a factor in $\mathbb{L}[t_1]$. The t_1-coordinates of the intersection points of C_1, C_2, C_3 are the roots of the content w.r.t Z of the resultant w.r.t. t_2 of the polynomials $F_1, F_2 + ZF_3$.

PROOF. Let $R(t_1, Z)$ be the resultant w.r.t. t_2 of F_1, and $F_2 + ZF_3$, and let $S(t_1)$ be the content of $R(t_1, Z)$ w.r.t Z. First of all note that, since C_1, C_2, C_3 do not have common components, then $R(t_1, Z)$ is not identically zero. Now we prove that the t_1-coordinates of the points in $C_1 \cap C_2 \cap C_3$ are the roots of $S(t_1)$. Indeed: let α be a root of $S(t_1)$ (note that α does not depend on Z). Then $R(\alpha, Z) = 0$. Thus, since we have assume that the *gcd* of each two of the leading coefficients of F_1, F_2, F_3, w.r.t. t_2 is trivial, one has that there exists $\beta \in \mathbb{F}$ such that $F_1(\alpha, \beta) = F_Z(\alpha, \beta) = 0$. Let us see that β does not depend on Z. If $\beta = \beta(Z)$ depends on Z, there exists infinitely many values of Z in $\mathbb{F}$ such that $F_1(\alpha, \beta(Z)) = 0$. This implies that $m(t_1)$ divides F_1, where $m(t_1)$ is the minimal polynomial of α over $\mathbb{L}$, which is impossible by hypotesis. Therefore, β does not depend on Z, and hence. $F_1(\alpha, \beta) = F_2(\alpha, \beta) = F_3(\alpha, \beta) = 0$.

Reciprocally, if one assume that (α, β) is a common point of C_1, C_2, C_3, one obtains that $F_1(\alpha, \beta) = F_Z(\alpha, \beta) = 0$. Thus $R(\alpha, Z) = 0$. Furthermore, since (α, β) does not depend on Z, one has that $S(\alpha) = 0$. $\square$.

In the next propositions, we see that our auxiliary curves V_1, V_2, V_3 are in the conditions of Proposition 1.

PROPOSITION 2. The curves V_1, V_2, V_3, do not have common components.
PROOF. Let us assume that G_1, G_2, G_3 have a common component. Then, there exist $M, N_i \in \mathbb{K}(V)[t_1, t_2]$ such that

$$G_i(t_1, t_2) = M(t_1, t_2)N_i(t_1, t_2), \text{ for } i = 1, 2, 3$$

The coefficients of M and N_i are rational functions over V. Thus, taking common denominators, the equality above can be written in $K[t_1, t_2]$ as

$$T_i(x, y, z)G_i = M^* N_i^* + A_i(x, y, z)F(x, y, z)$$

where $A_i, T_i \in \mathbb{K}[x, y, z]$, $M^*, N_i^* \in \mathbb{K}[x, y, z][t_1, t_2]$ and F is the implicit equation of V. Now we consider the set Ω consisting in all $P \in V$ such that $T_i(P) \neq 0$, and $M^*(P, t_1, t_2)$ is not constant, and $N_i^*(P, t_1, t_2)$ is not zero. Note that Ω is a non-empty open subset of V since T_i represents a denominator of an element in $\mathbb{K}(V)$, M^* corresponds to a numerator of a non constant polynomial over $\mathbb{K}(V)$, and N_i^* corresponds to a numerator of a non zero polynomial over $\mathbb{K}(V)$.
In this situation, for $i = 1, 2, 3$ and for all $P = (a_1, a_2, a_3) \in \Omega$ it holds that

$$T_i(P)(q_i(t_1, t_2)a_i - p_i(t_1, t_2)) = M^*(P, t_1, t_2)N_i^*(P, t_1, t_2)$$

Observe that $\gcd(q_i(t_1, t_2), M^*(P, t_1, t_2)) = 1$ for $i = 1, 2, 3$, since otherwise it would imply that $gcd(q_i, p_i) \neq 1$ for some i. For each $P \in \Omega$ we consider the set

$$\Sigma_P = \{Q \in \mathbb{K}^2 \;/\; M^*(P, Q) = 0,\ q_i(Q) \neq\ 0 \text{ for } i = 1, 2, 3\}.$$

Note that since $\gcd(q_i(t_1, t_2), M^*(P, t_1, t_2)) = 1$ one has that Σ_P is a non-empty open. Finally, using the Theorem of the dimension of fibres (see [18], pp.76) there exists an open set Ω' of V such that for every $P \in \Omega'$ the fibres $\mathcal{P}^{-1}(P)$ are zero dimensional. Now take $P \in \Omega \cap \Omega'$ (note that $\Omega \cap \Omega' \neq \emptyset$ because V is irreducible). Then one has that $\Sigma_P \subset \mathcal{P}^{-1}(P)$ which is impossible since Σ_P is open and $\mathcal{P}^{-1}(P)$ is zero dimensional. $\square$.

PROPOSITION 3. At least one of the polynomials G_1, G_2, G_3 does not have factors in $\mathbb{K}(V)[t_1]$ neither in $\mathbb{K}(V)[t_2]$
PROOF. We distinguish two cases depending on whether there exists or not one component of $\mathcal{P}$ depending simultaneously on both parameters. If none component of $\mathcal{P}$ depends simultaneously on t_1, t_2, we may assume w.l.o.g. that $\mathcal{P}$ is of the form $(\frac{p_1(t_1)}{q_1(t_1)}, \frac{p_2(t_2)}{q_2(t_2)}, \frac{p_3(t_2)}{q_3(t_2)})$. Therefore, the implicit equation of V depends only on y, z, and

hence it is a cylinder. Thus, the subfield of $\mathbb{K}(V)$ generated by the class of x is algebraically closed in $\mathbb{K}(V)$. Let us see that irreducibility over $\mathbb{K}(x)$ is equivalent to irreducibility over $\mathbb{K}(V)$. Indeed, if G_1 does not factor over $\mathbb{K}(x)$, but it factors over the algebraic closure, the coefficients of the factors are algebraic over $\mathbb{K}(x)$, and hence they do not belong to $\mathbb{K}(V)$. Thus, it suffices to prove that G_1 is irreducible over $\mathbb{K}(x)$, but this is obvious since G_1 is irreducible over $\mathbb{K}$.

Let us assume at least one component of $\mathcal{P}$ depends on t_1, t_2. Let us say that it is the first one. Observe that G_1 has a factor in $\mathbb{K}(V)[t_1]$ (similarly in $\mathbb{K}(V)[t_2]$) if and only if the content w.r.t. t_2 is not trivial; i.e. the content depends on t_1. Since the euclidian algorithm does not extend the ground field, one deduces that the above condition is equivalent to ask G_1 not to have a trivial content w.r.t. t_2 in $\mathbb{K}(x)[t_1]$, where x can be seen as a transcendental element over $\mathbb{K}$, since we have assumed that $\mathcal{V}$ is not a plane. Let us now assume that there exists a non–trivial content. It implies that there exists polynomials $A(x,t_1), B(x), D(x,t_1,t_2) \in \mathbb{K}[x,t_1,t_2]$ such that $deg_{t_1}(A) \geq 1$ and

$$B(x)G_1(x,t_1,t_2) = A(x,t_1)D(x,t_1,t_2).$$

Obviously, we may assume that A is primitive w.r.t. x. Thus, A divides G_1 as polynomials in $\mathbb{K}[x,t_1,t_2]$. Therefore, $deg_x(A) \leq 1$. If $deg_x(A) = 0$ one gets that $\gcd(q_1,p_1) \neq 1$ which is impossible by hypothesis. If $deg_x(A) = 1$, then the cofactor of A in G_1 does not depend on x. Therefore, it must be constant because $gcd(q_1,p_1) = 1$. Thus, G_1 does not depend on t_2, which is impossible. □

¿From Propositions 1,2,3 one can derive an algorithmic method to compute the t_1 and the t_2 coordinates of the points in $V_1 \cap V_2 \cap V_3$. We state the result for the t_1–coordinates, and we assume w.l.o.g. that G_1 is the polynomial without factors in $\mathbb{K}(V)[t_1]$ (see Proposition 2). A similar result holds for the t_2–coordinates.

Corollary 1. If each two of the leading coefficients of G_1, G_2, G_3, w.r.t. t_2 have trivial gcd, the t_1-coordinates of the intersection points of V_1, V_2, V_3 are the roots of the polynomial

$$S(t_1) = Content_Z(Resultant_{t_2}(G_1, G_2 + ZG_3)) \in \mathbb{K}(V)[t_1]$$

Remark. In the following, we will refer to the polynomial $S(t_1)$, introduced in the Corollary 1, as the polynomial defining the t_1-coordinates of the intersection points of the curves V_1, V_2, V_3. □

The next proposition states that the defining polynomial the t_1-coordinates of $V_1 \cap V_2 \cap V_3$ does not have non-constant multiple roots; similarly for the polynomial defining the t_2–coordinates.

Proposition 4. If $\mathcal{P}$ is proper, then the polynomial

$$S(t_1) = Content_Z(Resultant_{t_2}(G_1, G_2 + ZG_3))$$

does not have multiple non-constant roots.
PROOF. Let $M(x,y,z) = (A(x,y,z), B(x,y,z))$ be the inverse of $\mathcal{P}(t_1,t_2)$. Now, we observe that, from Theorem 2, one has that $M(x,y)$ is the unique non-constant point in $V_1 \cap V_2 \cap V_3$. We claim that for generic Z, M is a point of transversal intersection of the two plane curves with equation $G_1 = 0$ (i.e. V_1) and $G_2 + ZG_3 = 0$. To show this, we have to show that M is a simple point of both curves, and that the two tangents at M are distinct.

Note that V_1 is a generic curve of the pencil of plane curves spanned by $p_1(t_1,t_2) = 0$ and $q_1(t_1,t_2) = 0$. By Bertini's theorem (see [4], p 137), V_1 is smooth outside the common zero set of p_1 and q_1. Since M is not in this zero set, M is a smooth point of V_1. Similarily, M is a smooth point of V_2 and V_3. Therefore, the gradients of G_2 and G_3 are not zero at M, and therefore the gradient of $G_2 + ZG_3$ at M also is not zero for generic Z.

Now, assume indirectly that the gradients at M of G_1 and of G_2+ZG_3 are parallel for all Z. This is only possible if all three curves V_1, V_2, V_3 have common tangent. Because M is not in the zero set of q_i, the gradient of G_i is parallel to the gradient of the rational function $p_i(t_1,t_2)/q_i(t_1,t_2)$. Therefore the common tangent assumption implies that the Jacobi matrix of $\mathcal{P}$ is rank deficient at M. Now, let Ω be the non–empty open subset of $\mathbb{K}^2$ where the parametrization $\mathcal{P}$ is defined and moreover the inverse M is defined on the image of $\mathcal{P}$. Then, for every $(a,b) \in \Omega$ one has that the rank of the jacobian matrix of $\mathcal{P}$ at $M(\mathcal{P}(a,b)) = (a,b)$ is rank deficient. But then the image of the parametrization is only a curve, contradicting our assumption. Therefore, we have proved that M is a transversal intersection of G_1 and $G_2 + ZG_3$.

By well-known properties of resultants, it follows that $Resultant_{t_2}(G_1, G_2 + ZG_3)$ has only a simple root at $A(x,y,z)$. Since S is a divisor of $Resultant_{t_2}(G_1, G_2+ZG_3)$, A is a simple root of S.□

¿From Theorem 2 and Proposition 4 one deduces the following characterization.

THEOREM 3. Let $\overline{S}(t_1)$ and $\overline{S^*}(t_2)$ be the defining polynomials of the t_1-coordinates and the t_2-coordinates of the points in $(V_1 \cap V_2 \cap V_3) \cap (K \setminus \mathbb{K})^2$, respectively. The following statements are equivalent:

(1.) $\mathcal{P}$ is proper.

(2.) $\overline{S}(t_1)$ is linear, and the polynomial

$$M(t_2) = \frac{\gcd_{\mathbb{K}(V)[t_2]}(G_1(A_1,t_2), G_2(A_1,t_2), G_3(A_1,t_2))}{\gcd_{\mathbb{K}(V)[t_2]}(G_1(A_1,t_2), G_2(A_1,t_2), G_3(A_1,t_2), G_4(A_1,t_2))},$$

only has one distinct root, where $A_1 \in K$ is the root of $\overline{S}(t_1)$.

(3.) $\overline{S}(t_1)$ and $\overline{S}^*(t_2)$ are linear.

PROOF.

$\boxed{1\Rightarrow 2}$ If $\mathcal{P}$ is proper, taking into account Theorem 2, one has that $(V_1\cap V_2\cap V_3)\setminus(V_1\cap V_2\cap V_3\cap V_4)$ only has one point (α,β) in K^2. Since the roots of $\overline{S}(t_1)$ correspond to the t_1-coordinates of $(V_1\cap V_2\cap V_3)\setminus(V_1\cap V_2\cap V_3\cap V_4)$, one deduces that α is the unique root of the polynomial $\overline{S}(t_1)$. Furthermore, taking into account that $M(t_2)$ defines the t_2-coordinates of $(V_1\cap V_2\cap V_3)\setminus(V_1\cap V_2\cap V_3\cap V_4)$, one also has that β is the only different root of $M(t_2)$.

$\boxed{2\Rightarrow 3}$ If follows from the fact that $M(t_2)$ corresponds to the t_2-coordinate in $(V_1\cap V_2\cap V_3)\setminus(V_1\cap V_2\cap V_3\cap V_4)$ over K.

$\boxed{3\Rightarrow 1}$ Using that $\overline{S}(t_1)$ and $\overline{S}^*(t_2)$ define the t_1-coordinates and t_2-coordinates of the points in $(V_1\cap V_2\cap V_3)\setminus(V_1\cap V_2\cap V_3\cap V_4)$ respectively, one deduces that $(V_1\cap V_2\cap V_3)\setminus(V_1\cap V_2\cap V_3\cap V_4)$ only has one different point $(A_1,A_2)\in K$. Therefore, from Theorem 2 one concludes that $\mathcal{P}$ is proper. $\square$

3 Algorithm and Examples

The results in Section 2 can be applied to derive an algorithm that decides the properness of a given rational parametrization of a surface, and that (in the affirmative case) determines the inverse. In this section, we outline the algorithm and we illustrate it by examples.

<u>Algorithm</u> Inversion$(\mathcal{P},F)$

- **Input:** $F\in\mathbb{K}[x,y,z]$ irreducible and defining a surface (not being a plane) V over $\mathbb{K}$, and $\mathcal{P}(t_1,t_2)=(\frac{p_1}{q_1},\frac{p_2}{q_2},\frac{p_3}{q_3})$ a rational parametrization of V, where $\gcd(p_i,q_i)=1\ \forall i\in\{1,2,3\}$.
- **Output:** the message "$\mathcal{P}$ `is not proper`" or the inverse of $\mathcal{P}$.

(1) Compute the polynomials

$$G_1(t_1,t_2)=xq_1(t_1,t_2)-p_1(t_1,t_2),\quad G_2(t_1,t_2)=yq_2(t_1,t_2)-p_2(t_1,t_2),$$
$$G_3(t_1,t_2)=zq_3(t_1,t_2)-p_3(t_1,t_2),$$

that define the curves V_1,V_2,V_3, respectively.

(2) Check whether each two of the leading coefficients of G_1,G_2,G_3, w.r.t. t_2 is trivial, (resp. w.r.t. t_1). If not, do a change of coordinates to solve it.

(3) Compute the polynomial $S(t_1)$ defining the t_1-coordinates of the intersection points of V_1,V_2,V_3 (see Corollary 1).

(4) Compute the polynomial $\overline{S}(t_1)$ obtained by crossing out the constant roots of the polynomial $S(t_1)$.

(5) If $\bar{S}(t_1)$ is not linear then return "$\mathcal{P}$ `is not proper`".
Else let α the root of $\bar{S}(t_1)$

(6) Compute the polynomial $S^*(t_2)$ defining the t_2-coordinates of the intersection points of V_1, V_2, V_3 (see Corollary 1).

(7) Compute the polynomial $\overline{S}^*(t_2)$ obtained by crossing out the constant roots of the polynomial $S^*(t_2)$.

(8) If $\bar{S}^*(t_2)$ is not linear then return "$\mathcal{P}$ `is not proper`".
Else let β the root of $\bar{S}^*(t_2)$, and return "(α, β) `is the inverse of` $\mathcal{P}$".

CORRECTNESS. The algorithm follows essentially from Theorem 3. In addition note that, taking into account Proposition 1, when computing S and S^* in steps (2) and (6) respectively, the correspondent resultant can not be identically zero. □

REMARK. In order to compute the polynomial $\overline{S}(t_1)$ (and similarly $\overline{S}^*(t_2)$), one may do the following: substitute the parametrization $(\frac{p_1(s_1,s_2)}{q_1(s_1,s_2)}, \frac{p_2(s_1,s_2)}{q_2(s_1,s_2)}, \frac{p_3(s_1,s_2)}{q_3(s_1,s_2)})$ for (x, y, z) into S; the new variables s_1, s_2 are necessary to avoid coincidence with t_1. Then clear denominators by multiplying with a polynomial in $\mathbb{K}[s_1, s_2]$ and compute the content with respect to (s_1, s_2). This polynomial $C(t_1)$ corresponds to the constant roots. $\overline{S}(t_1)$ is obtained as the quotient of S by C. □

Finally we illustrate the algorithm by three examples. In examples 2 and 4 the parametrizations turn to be proper and their inverse is determine. However in example 3 the algorithm shows that the given parametrization is not proper. We use the following notation:

$$Resultant_{\mathbb{A}[h]}(F_1, F_2, h)$$

will denote the resultant w.r.t. h of the polynomials F_1, $F_2 \in \mathbb{A}[h]$ where $\mathbb{A}$ is a U.F.D. Also

$$content_h(R)$$

will denote the content of R w,r,t, h.

EXAMPLE 2. Let V be the surface defined by the irreducible polynomial $F = 1 - 2x + y + 2x^2 + x^2z^2 - 2xy + yx^2 - 2xz - yzx + 2zx^2 + zyx^2 \in \mathbb{C}[x, y, z]$, and the rational parametrization

$$\mathcal{P}(t_1, t_2) = \left(\frac{t_1}{t_2 + t_1}, \frac{t_1^2 + 1}{t_2}, \frac{1 + t_2}{t_1} \right).$$

Let us check whether $\mathcal{P}(t_1, t_2)$ is a proper parametrization. For this purpose, we apply the algorithm. First we consider the polynomials

$$G_1(t_1, t_2) = x(t_1 + t_2) - t_1, \quad G_2(t_1, t_2) = yt_2 - (t_1^2 + 1),$$

$$G_3(t_1, t_2) = zt_1 - (1 + t_2), \quad G_4(t_1, t_2) = t_1t_2(t_1 + t_2).$$

Doing the computation one has

$$R = Resultant_{\mathbb{C}(V)[t_1,Z][t_2]}(G_1, G_2 + ZG_3, t_2) = (-t_1yx - x + yt_1 - {t_1}^2x) + (-x + xzt_1 - t_1 + xt_1)Z$$

In addition, $S = content_Z(R) = t_1zx - t_1 - x + t_1x$. Note that S does not have constant roots, hence $\overline{S}(t_1) = S(t_1)$. Moreover, since $\bar{S}(t_1)$ is linear we obtain the first coordinate of the inverse

$$\alpha(x, y, z) = \frac{-x}{-xz + 1 - x}.$$

Reasoning similarly with the variable t_2, we obtain

$$R^* = Resultant_{\mathbb{C}(V)[t_2,Z][t_1]}(G_1, G_2 + ZG_3, t_1) = (-x^2t_2^2 - 1 + 2x - x^2 + yt_2 - 2yt_2x + yt_2x^2) +$$

$$+ (xt_2z - x^2t_2z - t_2 + 2xt_2 - t_2x^2 - 1 + 2x - x^2)Z$$

In addition, $S^* = content_Z(R^*) = xt_2z - x^2t_2z - t_2 + 2xt_2 - t_2x^2 - 1 + 2x - x^2$. Note that S^* does not have constant roots, hence $\overline{S}^*(t_2) = S^*(t_2)$. Moreover, since $\bar{S}^*(t_2)$ is linear we obtain the second coordinate of the inverse

$$\beta(x, y, z) = \frac{-x + 1}{xz - 1 + x}.$$

Thus, applying the algorithm, we deduce that $\mathcal{P}$ is proper and its inverse mapping is:

$$\mathcal{P}^{-1}(t_1, t_2) = (\alpha, \beta) = (\frac{-x}{-xz + 1 - x}, \frac{-x + 1}{xz - 1 + x})$$

Now, let us compute the inverse applying statement (2) of Corollary 1. Reasoning as above, we compute the first coordinate of the inverse, α. Then we substitue α in $\{G_1, G_2, G_3\}$, and compute the gcd

$$\gcd_{\mathbb{C}(V)[t_2]}(G_1(\alpha, t_2), G_2(\alpha, t_2), G_3(\alpha, t_2)) = \frac{x(-1 + x - t_2 + xt_2 + t_2zx)}{-1 + x + zx}.$$

Hence we get

$$\beta(x, y, z) = \frac{1 - x}{xz - 1 + x}.$$

Thus, applying Corollary 1, we deduce that $\mathcal{P}$ is proper and its inverse mapping is:

$$\mathcal{P}^{-1}(t_1, t_2) = \left(\frac{-x}{-xz + 1 - x}, \frac{1 - x}{xz - 1 + x}\right).$$

□

Example 3. Let V be the surface defined by the irreducible polynomial $F = -x + zx + z^2 - z + xy \in \mathbb{C}[x, y, z]$, and the rational parametrization

$$\mathcal{P}(t_1, t_2) = \left(\frac{t_2}{1 + t_2t_1^2}, \frac{t_1^2(t_2 + 1)}{1 + t_2t_1^2}, \frac{1}{1 + t_2t_1^2}\right).$$

Let us analyze whether $\mathcal{P}(t_1, t_2)$ is a proper parametrization. For this purpose, we apply the algorithm. First we consider the polynomials

$$G_1(t_1, t_2) = x(1 + t_2 t_1^2) - t_2, \quad G_2(t_1, t_2) = y(1 + t_2 t_1^2) - t_1^2(t_2 + 1),$$

$$G_3(t_1, t_2) = z(1 + t_2 t_1^2) - 1, \quad G_4(t_1, t_2) = 1 + t_2 t_1^2.$$

Doing the computation one has

$$R = Resultant_{\mathbb{C}(V)[t_1,Z][t_2]}(G_1, G_2 + ZG_3, t_2) = (-t_1^4 x - y + t_1^2) + (-t_1^2 x - t_1^2 x - z)Z$$

In addition $S = content_Z(R) = -t_1^2 x - z + 1$. Note that S does not have constant roots, hence $\overline{S}(t_1) = S(t_1)$. Moreover, since $\bar{S}(t_1)$ is not linear, one deduces that $\mathcal{P}$ is not proper. □

Example 4. Let V be the surface defined by the irreducible polynomial $F = -3\,y\,z^2 + 4\,z\,y - 5\,z^3 + 10\,z^2 - y^3 + 2\,x\,y^2 + y^2\,z + 2\,y^2 - 4\,y - 4\,z - 4\,x\,z\,y + 2\,z^2\,x \in \mathbb{C}[x, y, z]$, and the rational parametrization

$$\mathcal{P}(t_1,\, t_2) = \left(\frac{t_1\,(t_1 + t_2\,t_1 - 1)}{t_1 - t_1^2 + t_2}, \frac{t_2 - t_1}{t_1 - t_1^2 + t_2}, \frac{t_1 + t_2}{t_1 - t_1^2 + t_2} \right).$$

Let us check whether $\mathcal{P}(t_1, t_2)$ is a proper parametrization. For this purpose, we apply the algorithm. First we consider the polynomials

$$G_1(t_1, t_2) = \, x\,(t_1 - t_1^2 + t_2) - t_1\,(t_1 + t_2\,t_1 - 1), \quad G_2(t_1, t_2) = \, y\,(t_1 - t_1^2 + t_2) - t_2 + t_1,$$
$$G_3(t_1, t_2) = \, z\,(t_1 - t_1^2 + t_2) - t_1 - t_2, \quad G_4(t_1, t_2) = \, t_1 - t_1^2 + t_2.$$

Doing the computation one has

$$R(t_1, Z) = resultant_{\mathbb{C}(V)[t_1,Z][t_2]}(G_3, G_1 + Z\,G_2, t_2) =$$

$$= \, Z\,(-2\,t_1 + y\,t_1^2 + 2\,t_1\,z - z\,t_1^2) + (-t_1 + t_1^2 + t_1\,z + x\,t_1^2 + t_1^3\,z - t_1^4\,z - z\,t_1^2 - t_1^3).$$

In addition,

$$S(t_1) = content_Z(R(t_1, Z)) = \, -2\,t_1 + y\,t_1^2 + 2\,t_1\,z - z\,t_1^2.$$

Note that $S(t_1)$ has the root $t_1 = 0$ in $\mathbb{C}$. We cross out this root of the polynomial S, an we obtain the polynomial $\overline{S}$:

$$\overline{S}(t_1) = \, -2 + y\,t_1 + 2\,z - z\,t_1.$$

Moreover, since $\bar{S}(t_1)$ is linear we obtain the first coordinate of the inverse

$$\alpha = \, -2\,\frac{-1 + z}{y - z}$$

Reasoning similarly with the variable t_2, we obtain

$$R^*(t_2, Z) = resultant_{\mathbb{C}(V)[t_2,Z][t_1]}(G_3, G_1 + Z\,G_2, t_1) =$$

$$= Z^2\,(z^2\,t_2^2 - 2\,z\,t_2^2\,y + y^2\,t_2^2 - 2\,z\,y\,t_2 + 2\,y\,t_2 - 2\,z^2\,t_2 + 2\,z\,t_2)+$$
$$+Z\,(4\,z^2\,t_2^2 + 2\,z^2\,t_2^3 - z\,y\,t_2 - 2\,z\,t_2^2\,x - 2\,z\,t_2^2\,y - 2\,z\,t_2^3\,y + 2\,x\,y\,t_2^2+$$
$$+y\,t_2 + 2\,t_2 - z\,t_2 - 6\,z\,t_2^2 - 2\,t_2^3\,z + 2\,y\,t_2^2 + 2\,t_2^3\,y - z^2\,t_2 + 2\,x\,t_2 + 2\,t_2^2 - 2\,z\,x\,t_2)+$$
$$+(-2\,z\,t_2^2\,x - 2\,t_2^3\,z\,x - z\,x\,2 + t_2 + x\,t_2 - z\,t_2 - 4\,z\,t_2^2 + 2\,t_2^2 + 2\,z^2\,t_2^2-$$
$$-4\,t_2^3\,z + 2\,z^2\,t_2^3 + 2\,x\,t_2^2 + 2\,t_2^3 + z^2\,t_2^4 - 2\,z\,t_2^4 + x^2\,t_2^2 + 2\,x\,t_2^3 + t_2^4).$$

$$S^*(t_2) = content_Z(R^*(t_2, Z)) =$$
$$= z^2\,t_2^2 - 2\,z\,t_2^2\,y + y^2\,t_2^2 - 2\,z\,y\,t_2 + 2\,y\,t_2 - 2\,z^2\,t_2 + 2\,z\,t_2.$$

$S^*(t_2)$ has the constant root $t_2 = 0$ in $\mathbb{C}$. We cross out this root of the polynomial S^*, and we obtain the polynomial $\overline{S}^*$:

$$\overline{S}^*(t_2) = z^2\,t_2 - 2\,z\,t_2\,y + y^2\,t_2 - 2\,z\,y + 2\,y - 2\,z^2 + 2\,z.$$

Moreover, since $\bar{S}^*$ is linear we obtain the second coordinate of the inverse

$$\beta = 2\,\frac{z\,y - y + z^2 - z}{z^2 + y^2 - 2\,z\,y}.$$

Thus, applying the algorithm, we deduce that $\mathcal{P}$ is proper and its inverse mapping is:

$$\mathcal{P}^{-1}(t_1, t_2) = (\alpha, \beta) = (-2\,\frac{-1 + z}{y - z}, 2\,\frac{z\,y - y + z^2 - z}{z^2 + y^2 - 2\,z\,y})$$

□

4 Practical Implementation

This section is devoted to the experimental computing times of the previous algorithm. It focuses on the implementation of two prototypes of the algorithm and actual computing times in Maple V.5.1, running on a PC INTEL PENTIUM 350 MHz and 64 MB of RAM, and times are given in seconds of CPU.

The first implementation assumes that the implicit equation of the surface is known. We use the implicit equation of the surface to carry out the arithmetic over $\mathbb{K}(V)$. Note that, since $I(V) = (F)$, basic arithmetic on $\mathbb{K}[V]$ can be carried out by computing polynomial remainders. Therefore the quotient field $\mathbb{K}(V)$ is computable. In addition, we remark that we compute resultants of polynomials in $\mathbb{K}(V)[t_1, t_2]$ that is a UFD, and we also calculate gcds of univariate polynomials over $\mathbb{K}(V)$, and hence in an euclidean domain.

The second implementation avoids the requirement on the implicit equation. For this purpose, elements are represented (not uniquely) as function of polynomials in the variables x, y, z. In order to check zero equality one may use the parametrization. However, this can be too time consuming. Instead, we test zero-equality by substituting a random point on the surface. The result of this zero test is correct with probability almost one. In addition, if the output is a rational inverse, we also test its correctness by checking it on a randomly choosen point on the surface.

In the following table we illustrate the performance of our two implementations showing times for some parametrizations. In the table we also show the degree of each parametrization. In the appendix, we give the parametrizations considered in this analysis.

Parametrization	Degree	Time of our Deterministic implentation	Time of our Probabilistic implentation	Time using Gröbner basis
P_1	2	0.95	0.92	> 3000
P_2	2	0.22	0.11	> 3000
P_3	2	1.62	1.62	> 2000
P_4	4	0.16	0.23	4.24
P_5	2	6.89	6.89	0.14
P_6	2	10.60	10.69	0.58
P_7	2	0.58	0.56	0.51
P_8	3	0.46	0.51	2.26
P_9	3	0.13	0.09	0.72
P_{10}	3	0.13	0.20	> 3000
P_{11}	3	0.085	0.04	0.59
P_{12}	2	1.45	1.50	> 4000
P_{13}	3	3.64	3.50	> 3000
P_{14}	3	11.49	11.23	> 3000
P_{15}	3	1.22	1.21	6.22
P_{16}	2	1.94	1.91	> 3000
P_{17}	2	22.39	21.49	> 4000
P_{18}	7	67.70	0.41	4.53
P_{19}	8	547.10	0.52	7.44
P_{20}	8	426.99	0.43	6.65
P_{21}	7	706.06	0.4	> 4000

5 Appendix: Parametrizations in Section 4

$$P_1 = \left(\frac{t_1}{t_1+t_2}, \frac{{t_1}^2 - t_1 + 1}{t_2+1}, {t_1}^2 + t_2\right)$$

$$P_2 = \left(\frac{t_1^2+t_2}{t_1+t_2}, \frac{t_1^2 - t_1 + 1}{t_2^2+1}, \frac{t_1^2+t_2}{t_1}\right)$$

$$P_3 = \left(\frac{2t_2^2 - 3t_1^2}{-2t_1^2 - t_1t_2}, \frac{-2t_1t_2}{2t_1 - t_2^2}, \frac{t_2^2 + 2t_1t_2}{3t_2 + 3t_1}\right)$$

$$P_4 = \left(\frac{-(3+3t_1^3t_2)}{t_2}, \frac{1/2(3t_1t_2 - 2t_1^2)}{t_2}, \frac{-1/3(2-3t_1)}{t_2}\right)$$

$$P_5 = \left(3 - t_2 - t_1 - 3t_1t_2 + 2t_2^2 + 3t_1^2, -1 - 2t_2 + t_1 - 3t_1t_2 + 2t_2^2 + 3t_1^2, -2 - 2t_2 - 3t_1^2\right)$$

$$P_6 = \left(t_2 + 2t_1t_2 - 3t_1^2 - t_2^2, 3 + t_2 + 2t_1 + 2t_1t_2 + 3t_1^2, 1 + 2t_2 + 2t_1 - 2t_1t_2 - 2t_1^2\right)$$

$$P_7 = \left(t_1 + t_2t_1^2 - 1, \frac{t_2^2}{t_2 + t_1t_2 + 1}, t_1 + t_2t_1^2 - t_2\right)$$

$$P_8 = \left(\frac{t_1t_2 + 1 + t_1}{t_2^2 + t_1^2}, \frac{1}{t_2^2 + t_1^2}, \frac{t_2^2 + t_1^2 + 1}{(t_2^2 + t_1^2)t_2}\right)$$

$$P_9 = \left(\frac{t_1(t_1 + t_1t_2 - 1)}{t_1 - t_1^2 + t_2}, \frac{-t_1 + t_2}{t_1 - t_1^2 + t_2}, \frac{t_1 + t_2}{t_1 - t_1^2 + t_2}\right)$$

$$P_{10} = \left(\frac{t_1t_2 + 1}{t_1 + 1}, \frac{t_2}{t_1 - 1}, \frac{t_1 + t_2}{(t_1^2 - 1)t_2}\right)$$

$$P_{11} = \left(\frac{t_1}{t_1^2 + t_1t_2 - 3}, \frac{t_1 + t_2^3}{t_1 + t_2}, \frac{1}{t_1 + t_2}\right)$$

$$P_{12} = \left(\frac{t_1 + t_2^2}{t_1 + t_2 - 1}, \frac{t_1^2 + t_2}{t_1} + 3, \frac{t_1}{t_2 + t_1t_2 + 1}\right)$$

$$P_{13} = \left(\frac{t_1^2 + t_2^2 + t_1^3}{t_1^2}, t_2 + t_1^3, \frac{t_1}{t_2^2 + 1}\right)$$

$$P_{14} = \left(\frac{t_1^2 + t_2^2 + t_1^3}{t_1^2}, \frac{t_2 + t_1^3}{t_1 + t_2 - 4}, \frac{t_1}{t_2^2 + 1}\right)$$

$$P_{15} = \left(3t_2 + 3t_2t_1^2 - t_2^3, 3t_1 + 3t_2^2t_1 - t_1^3, 3t_2^2 - 3t_1^2\right)$$

$$P_{16} = \left(-3/2 - 1/2t_1t_2 + 1/2t_2 - t_1, \frac{-(-1 + 2t_2 + 3t_2^2 - t_1^2)}{-1 + 2t_1}, -1 - t_1t_2 - 2/3t_1 + t_2^2 - 1/3t_1^2\right)$$

$$P_{17} = \left(\frac{2t_1t_2 + 2t_2^2 - 3t_1^2}{t_1(t_2+1)}, -\frac{t_1(2t_2+1)}{t_2+3t_1}, \frac{2+t_1t_2+3t_2^2}{t_2(-2t_1+t_2)} \right)$$

$$P_{18} =$$

$$(\frac{-t_1(2+t_1(43t_2^5 - 66t_2^4 - 53t_2^3 - 61t_2^2 - 23t_2 - 37) + t_1(-19t_2^5 - 47t_2^4 + 68t_2^3 - 72t_2^2 - 87t_2 + 79))}{t_1(-19t_2^5 - 47t_2^4 + 68t_2^3 - 72t_2^2 - 87t_2 + 79) + 1 + t_1^2(80t_2^5 + 72t_2^4 + 66t_2^3 - 29t_2^2 - 91t_2 - 53)},$$

$$\frac{-1 - t_1(43t_2^5 - 66t_2^4 - 53t_2^3 - 61t_2^2 - 23t_2 - 37) + t_1^2(80t_2^5 + 72t_2^4 + 66t_2^3 - 29t_2^2 - 91t_2 - 53)}{t_1(-19t_2^5 - 47t_2^4 + 68t_2^3 - 72t_2^2 - 87t_2 + 79) + 1 + t_1^2(80t_2^5 + 72t_2^4 + 66t_2^3 - 29t_2^2 - 91t_2 - 53)}, t_2)$$

$$P_{19} =$$

$$(\frac{-t_1(2+t_1(77t_2^6 + 66t_2^4 + 54t_2^3 - 5t_2^2 + 99t_2 - 61) + t_1(-59t_2^6 + 45t_2^5 - 8t_2^4 - 93t_2^2 + 92t_2 + 43))}{t_1(-59t_2^6 + 45t_2^5 - 8t_2^4 - 93t_2^2 + 92t_2 + 43) + 1 + t_1^2(97t_2^6 + 50t_2^5 + 79t_2^4 + 56t_2^3 + 49t_2^2 + 63t_2)},$$

$$,\frac{t_1^2(97t_2^6 + 50t_2^5 + 79t_2^4 + 56t_2^3 + 49t_2^2 + 63t_2) - t_1(77t_2^6 + 66t_2^4 + 54t_2^3 - 5t_2^2 + 99t_2 - 61) - 1)}{t_1(-59t_2^6 + 45t_2^5 - 8t_2^4 - 93t_2^2 + 92t_2 + 43) + 1 + t_1^2(97t_2^6 + 50t_2^5 + 79t_2^4 + 56t_2^3 + 49t_2^2 + 63t_2)}, t_2)$$

$$P_{20} =$$

$$(\frac{-t_1(2+t_1(-27t_2^6 + 32t_2^5 - 24t_2^3 - 46t_2^2 + 12t_2 + 81) + t_1(-4t_2^6 + 38t_2^5 - 61t_2^3 - 58t_2^2 - 91t_2 + 45))}{t_1(-4t_2^6 + 38t_2^5 - 61t_2^3 - 58t_2^2 - 91t_2 + 45) + 1 + t_1^2(58t_2^6 - 92t_2^5 - 8t_2^3 + 36t_2^2 - 90t_2 + 96)},$$

$$,\frac{t_1^2(58t_2^6 - 92t_2^5 - 8t_2^3 + 36t_2^2 - 90t_2 + 96) - t_1(-27t_2^6 + 32t_2^5 - 24t_2^3 - 46t_2^2 + 12t_2 + 81) - 1}{t_1(-4t_2^6 + 38t_2^5 - 61t_2^3 - 58t_2^2 - 91t_2 + 45) + 1 + t_1^2(58t_2^6 - 92t_2^5 - 8t_2^3 + 36t_2^2 - 90t_2 + 96)}, t_2)$$

$$P_{21} =$$

$$(\frac{-t_1(2t_1+t_1(92t_2^5+43t_2^4-62t_2^3+77t_2^2+66t_2+54)+2+t_1(63t_2^5+57t_2^4-59t_2^3+45t_2^2-8t_2-93))}{t_1(63t_2^5+57t_2^4-59t_2^3+45t_2^2-8t_2-93)+1+t_1^2(-35t_2^5+97t_2^4+50t_2^3+79t_2^2+56t_2+49)+t_1^2(63t_2^5+57t_2^4-59t_2^3+45t_2^2-8t_2-93)+t_1^2+2t_1},$$

$$,\frac{-t_1^2+t_1^2(-35t_2^5+97t_2^4+50t_2^3+79t_2^2+56t_2+49)-1-t_1(92t_2^5+43t_2^4-62t_2^3+77t_2^2+66t_2+54)-t_1^2(92t_2^5+43t_2^4-62t_2^3+77t_2^2+66t_2+54)-2t_1}{t_1(63t_2^5+57t_2^4-59t_2^3+45t_2^2-8t_2-93)+1+t_1^2(-35t_2^5+97t_2^4+50t_2^3+79t_2^2+56t_2+49)+t_1^2(63t_2^5+57t_2^4-59t_2^3+45t_2^2-8t_2-93)+t_1^2+2t_1}, t_2)$$

References

[1] Gutierrez J., Recio T. (1992). *Rational Function Decomposition and Gröbner Basis in the Parameterization of a Plane Curve.* LATIN 92, LNCS 583 pp. 231-246. Springer Verlag (1992).

[2] Goldman R.N., Sederberg T.W., Anderson D.C. (1984). *Vector elimination: A technique for the implicitization, inversion, and a intersection of planar parametric rational polynomial curves.* Computer Aided Design vol 1, pp. 337-356.

[3] González-Vega L. (1997), *Implicitization of Parametric Curves and Surfaces by using Multidimensional Newton Formulae.* J. Symbolic Computation vol. 23, pp. 137-152.

[4] Griffiths P., Harris J. (1978), *Principles of Algebraic Geometry.* John Wiley and Sons.

[5] Harris J. (1995), *Algebraic Geometry. A first Course*. Springer-Verlag.

[6] van Hoeij M. (1994), *Computing Parametrizations of Rational Algebraic Curves.* Proc. ISSAC'94, ACM Press, 187-190.

[7] van Hoeij M. (1997), *Rational Parametrizations of Curves Using Canonical Divisors.* J. of Symbolic Computation **23**, 209-227.

[8] Hoffmann C. M. (1993), *Geometric and Solid Modeling.* Morgan Kaufmann Publ., Inc.

[9] Hoffmann C.M., Sendra J.R., Winkler F. (1997), *Parametric Algebraic Curves and Applications.* J.of Symbolic Computation 23.

[10] Hoschek J., Lasser D. (1993), *Fundamentals of Computer Aided Geometric Design.* A.K. Peters Wellesley MA., Ltd.

[11] Schicho J. (1992), *On the Choice of Pencils in the Parametrization of Curves.* J. of Symbolic Computation **14**, 557-576.

[12] Schicho J. (1998), *Rational Parametrization of Surfaces.* J. of Symb. Comp. **26**, 1-9.

[13] Schicho J. (1998), *Inversion of Birational Maps with Gröbner Basis.* Lectures Notes Series 251 *Gröbner Basis and Applications.* B. Buchberger, F. Winkler (eds), pp 495-503. Cambridge Univ. Press.

[14] Sederberg T.W. (1986), *Improperly Parametrized Rational Curves.* Computer Aided Geometric Design **3**, 67-75.

[15] Sederberg T.W., Goldman R., Du H., (1997). *Impliciting Rational Curves by the method of moving algebraic curves.* J. Symbolic Computation vol. 23, pp. 153-176.

[16] Sendra J.R., Winkler F. (1991), *Symbolic Parametrization of Curves.* J. Symbolic Computation **12/ 6,** 607-631.

[17] Sendra J.R., Winkler F. (1997). *Parametrization of Algebraic Curves over Optimal Field Extensions.* J. Symbolic Computation vol. 23, pp. 191-207.

[18] Shafarevich, I.R. (1994). *Basic algebraic geometry Schemes; 1 Varieties in projective space.* Berlin New York : Springer-Verlag. vol. 1.

[19] Zippel R., *Rational Function Decomposition.* Proc. of ISSAC91 pp. 1-6 ACM Press.