Available online at www.sciencedirect.com
ScienceDirect
Journal of Symbolic Computation 43 (2008) 118–139
Journal of Symbolic Computation
www.elsevier.com/locate/jsc

A univariate resultant-based implicitization algorithm for surfaces[☆]

Sonia Pérez-Díaz[1], J. Rafael Sendra

Dpto de Matemáticas, Universidad de Alcalá, E-28871 Madrid, Spain

Received 14 March 2007; accepted 9 October 2007
Available online 22 October 2007

Abstract

In this paper, we present a new algorithm for computing the implicit equation of a rational surface $\mathcal{V}$ from a rational parametrization $\mathcal{P}(\bar{t})$. The algorithm is valid independent of the existence of base points, and is based on the computation of polynomial gcds and univariate resultants. Moreover, we prove that the resultant-based formula provides a power of the implicit equation. In addition, performing a suitable linear change of parameters, we prove that this power is indeed the degree of the rational map induced by the parametrization. We also present formulas for computing the partial degrees of the implicit equation.

Keywords: Implicitization; Rational surface parametrization; Partial degrees; Properness

1. Introduction

In this paper we deal with the problem of computing the implicit equation of a surface given rationally over a field of characteristic zero. That is, if $\mathcal{P}(\bar{t})$ is a rational surface parametrization, with coefficients in a field $\mathbb{L}$ of characteristic zero, we want to compute the equation defining the Zariski closure of $\{\mathcal{P}(\bar{t}) \mid \bar{t} \in U\}$, where U is a dense set of $\mathbb{K}^2$ (in the Zariski topology), and $\mathbb{K}$ the algebraic closure of $\mathbb{L}$.

Clearly, this problem can be approached by means of elimination theory techniques such as, for instance, Gröbner bases (see Adams and Loustaunau (1994) and Cox et al. (1997, 1998a)).

☆ Both the authors are supported by the Spanish "Ministerio de Educación y Ciencia" under the Project MTM2005-08690-C02-01.

E-mail addresses: sonia.perez@uah.es (S. Pérez-Díaz), rafael.sendra@uah.es (J. Rafael Sendra).

[1] Tel.: +34 91 886753; fax: +34 91 8854951.

0747-7171/$ - see front matter
doi:10.1016/j.jsc.2007.10.001

Nevertheless, many authors have developed special methods for the implicitization problem (see Kotsireas (2004) for a survey). Among them, one may mention for instance those based on multiresultant and u-resultants (see Chionh and Goldman (1992a,b)), on residual resultants (see Busé (2001)), on moving curves and surfaces (see Cox et al. (2000), D'Andrea (2001) and Sederberg and Chen (1995)), on syzygies (see Busé et al. (2003) and Cox (2001)), on homotopy techniques (see Kotsireas (2004)), on symmetric functions (see González-Vega (1997)), on interpolation techniques (see Marco and Martínez (2002) and Orecchia (2001)), etc. Some of these methods have difficulties in the presence of base points, some deal only with special cases, some, although always valid, do not have a totally satisfactory computing time performance.

In this paper we present a new algorithm, based on polynomial gcds and univariate resultants, which always works and whose computing time performance is quite satisfactory (see Section 7). More precisely, we prove that the resultant-based formula provides the implicit equation of the surface to a power. In addition, performing a suitable linear change of parameters, we prove that this power is indeed the degree of the rational map induced by the parametrization, and therefore this new approach generalizes the corresponding results for the case of plane algebraic curves stated in Sendra and Winkler (2001b). Moreover, we present formulas for computing the partial degrees of the implicit equation.

The structure of the paper is as follows: In Section 2, we introduce the notations that will be used throughout the paper. Section 3 is devoted to recalling how to compute the degree of the rational map induced by the surface's parametrization, and by a pair of bivariate rational functions. All results in this section are either included in Pérez-Díaz et al. (2002), Pérez-Díaz and Sendra (2004) or Pérez-Díaz and Sendra (2005), or can be easily deduced from there. In Section 4, we present the results concerning the partial degrees of the implicit equation of the surface. These results generalize those appearing in Pérez-Díaz and Sendra (2005) and Sendra and Winkler (2001b). In Section 5, we deal with the problem of implicitization for rational plane curves and cylinders. In particular, we recall the results obtained in Sendra and Winkler (2001b) for rational plane curves, and we present a generalization of these results for cylinders defined parametrically. In Section 6 we introduce and motivate the main implicitization formulae; the proofs of these results appear in Section 8. In Section 7 we derive the corresponding algorithm, we illustrate it by examples, and show some empirical analyses of its performance. In the Appendix we list the parametrizations appearing in the performance analysis.

2. Notations and basic notions

In this section we introduce the notations and terminology that will be used throughout this paper, as well as the general assumptions we impose. In addition, we see that these assumptions do not imply loss of generality.

Let $\mathbb{K}$ be an algebraically closed field of characteristic zero, and set $\mathbb{K}^\star = \mathbb{K}\setminus\{0\}$. We consider a rational surface $\mathcal{V}$ over $\mathbb{K}$. Let $F(\overline{x})$ be the implicit equation of $\mathcal{V}$ (note that the implicit equation of $\mathcal{V}$ is unique up to multiplication by elements in $\mathbb{K}^\star$), and let

$$\mathcal{P}(\overline{t}) = (\mathfrak{P}_1(\overline{t}), \mathfrak{P}_2(\overline{t}), \mathfrak{P}_3(\overline{t})) = \left(\frac{p_1(\overline{t})}{q_1(\overline{t})}, \frac{p_2(\overline{t})}{q_2(\overline{t})}, \frac{p_3(\overline{t})}{q_3(\overline{t})}\right) \in \mathbb{K}(\overline{t})^3,$$

be a rational parametrization of $\mathcal{V}$, with $\overline{t} = (t_1, t_2)$ and $\overline{x} = (x_1, x_2, x_3)$. We assume that $\mathfrak{P}_i(\overline{t})$ is always expressed in reduced form, i.e. $\gcd(p_i, q_i) = 1$. Associated with $\mathcal{P}(\overline{t})$, we consider the induced rational map:

$$\mathcal{P} : \mathbb{K}^2 \longrightarrow \mathcal{V} \subset \mathbb{K}^3;\ \overline{t} \longmapsto \mathcal{P}(\overline{t}).$$

Similarly, for $i, j \in \{1, 2, 3\}$, with $i < j$, we consider the pair of rational functions

$$\pi_{i,j}(\mathcal{P})(\bar{t}) = (\mathfrak{P}_i(\bar{t}), \mathfrak{P}_j(\bar{t})),$$

and we also denote by $\pi_{i,j}(\mathcal{P})$ the rational map induced by $\pi_{i,j}(\mathcal{P})$; i.e.

$$\pi_{i,j}(\mathcal{P}) : \mathbb{K}^2 \to \mathbb{K}^2;\ \bar{t} \mapsto (\mathfrak{P}_i(\bar{t}), \mathfrak{P}_j(\bar{t})).$$

Associated with $\mathcal{P}(\bar{t})$ we introduce the polynomial

$$G_i(\bar{t}, x_i) = p_i(\bar{t}) - x_i\, q_i(\bar{t}) \in \mathbb{K}[x_i][\bar{t}],\ \ i = 1, 2, 3,$$
$$G_4(\bar{t}) = \mathrm{lcm}(q_1, q_2, q_3) \in \mathbb{K}[\bar{t}].$$

Let $\mathbb{F}$ be the algebraic closure of the field $\mathbb{K}(\bar{x})$. We denote by $V_i^{\bar{x}}$ the algebraic set defined over $\mathbb{F}$ by the polynomial $G_i(\bar{t}, x_i)$, $i \in \{1, 2, 3\}$, and by V_4 the algebraic set defined over $\mathbb{K}$ by $G_4(\bar{t})$.

Now, we introduce the notion of settled parametrization. Let $i, j \in \{1, 2, 3\}$, with $i < j$. We say that $\mathcal{P}(\bar{t})$ is (i, j)-settled if:

(1) The gradients $\{\nabla\mathfrak{P}_i(\bar{t}),\ \nabla\mathfrak{P}_j(\bar{t})\}$ are linearly independent as vectors in $\mathbb{K}(\bar{t})^2$. Note that, since $\mathcal{P}(\bar{t})$ parametrizes a surface, the gradients of at least two of its components are linearly independent.
(2) $\mathfrak{P}_k(\bar{t})$ is not a constant, where $k \in \{1, 2, 3\} \setminus \{i, j\}$. Note that, if $\mathfrak{P}_k(\bar{t}) = \lambda \in \mathbb{K}$, the implicit equation is $x_k - \lambda = 0$, and hence the implicitization problem is trivial.

Related to the problem we are dealing with, we will use different concepts of degree. For a polynomial $G \in \mathbb{K}[\bar{x}]$ we denote by $\mathrm{tdeg}(G)$ the total degree of G and by $\deg_{x_i}(G)$ the degree of G w.r.t. x_i. We denote by $\deg(\mathcal{V})$ the degree of $\mathcal{V}$, that is $\deg(\mathcal{V}) = \mathrm{tdeg}(F)$. We define the partial degree of $\mathcal{V}$ w.r.t. x_i as the partial degree of its implicit equation, and we denote it by $\deg_{x_i}(\mathcal{V})$. Note that even though the degree of a surface is invariant under linear changes of coordinates, the partial degree does depend on the choice of coordinates (see Pérez-Díaz and Sendra (2005)). We denote by $\deg(\mathcal{P})$ the degree of the rational map $\mathcal{P}$ (for further details see e.g. Shafarevich (1994) p. 143, or Harris (1995) p. 80); similarly, for $\deg(\pi_{i,j}(\mathcal{P}))$. As an important result, we recall that the properness of $\mathcal{P}(\bar{t})$ is characterized by $\deg(\mathcal{P}) = 1$ (see Harris (1995) and Shafarevich (1994)). Also, we recall that the degree of a rational map can be seen as the cardinality of the fibre of a generic element (see Theorem 7, p. 76 in Shafarevich (1994)). We will use this characterization in our reasoning. For this purpose, if $\phi : V_1 \longrightarrow V_2$ is a rational map between varieties, and $Q \in V_2$, we denote by $\phi^{-1}(Q)$ the fibre of Q; i.e. $\phi^{-1}(Q) = \{P \in V_1 \mid \phi(P) = Q\}$.

General assumptions. We assume w.l.o.g that $\mathcal{P}(\bar{t})$ satisfies the following conditions:

(1) None of the projective curves defined by each non-constant $p_i(\bar{t})$ and $q_i(\bar{t})$ passes through the point at infinity $(0 : 1 : 0)$, where the homogeneous variables are (t_1, t_2, w). Note that this requirement can always be achieved by applying a linear transformation to $\mathcal{P}(\bar{t})$, and therefore there is no loss of generality for our purposes since one can always undo the linear transformation once the implicit equation has been computed.
(2) $\mathcal{P}(\bar{t})$ is $(1, 2)$-settled.

Remark 1. Observe that if $\mathcal{P}(\bar{t})$ satisfies the above general assumptions then:

(1) No rational component $\mathfrak{P}_i(\bar{t})$ is constant (see condition (1) of $(1, 2)$-settled for $\mathfrak{P}_1(\bar{t}), \mathfrak{P}_2(\bar{t})$, and condition (2) of $(1, 2)$-settled for $\mathfrak{P}_3(\bar{t})$).

(2) Assumption (1) implies that each polynomial $p_1, p_2, p_3, q_1, q_2, q_3$ is either a non-zero constant or has positive degree w.r.t. t_2 in which case its leading coefficient w.r.t. t_2 does not depend on t_1.
(3) The previous remark implies that, for $i = 1, 2, 3$, $\deg_{t_2}(G_i(\bar{t}, x_i)) > 0$, and that the leading coefficient of $G_i(\bar{t}, x_i)$ w.r.t. t_2 does not depend on t_1.
(4) Finally, condition (1) of (1, 2)-settled implies that either $\deg_{t_1}(G_1(\bar{t}, x_1)) > 0$ or $\deg_{t_1}(G_2(\bar{t}, x_2)) > 0$.

3. Computation of the degree of a rational map

In this section we show how to compute the degree of the rational maps $\mathcal{P}$ and $\pi_{i,j}(\mathcal{P})$. All results in this section are either included in Pérez-Díaz et al. (2002), Pérez-Díaz and Sendra (2004) or Pérez-Díaz and Sendra (2005), or can be easily deduced from there. Therefore, we omit proofs.

Consider the polynomials G_1, G_2, G_3, G_4, as well as the algebraic sets $V_1^{\bar{x}}, V_2^{\bar{x}}, V_3^{\bar{x}}, V_4$ (see Section 2). In the following theorems we use the notions of content and primitive part of a polynomial. Given a non-zero polynomial $a(\bar{x}) \in I[\bar{x}]$, where I is a unique factorization domain, we denote by $\mathrm{pp}_{\bar{x}}(a)$ the primitive part of a w.r.t. $\bar{x}$, and by $\mathrm{Content}_{\bar{x}}(a)$ the content part of a w.r.t. $\bar{x}$; that is, $a(\bar{x}) = \mathrm{Content}_{\bar{x}}(a(\bar{x}))\,\mathrm{pp}_{\bar{x}}(a(\bar{x}))$, where $\mathrm{Content}_{\bar{x}}(a) \in I$, and $\mathrm{pp}_{\bar{x}}(a)$ is a primitive polynomial, which means that the gcd of all coefficients of $\mathrm{pp}_{\bar{x}}(a)$ is 1. Note that $\mathrm{Content}_{\bar{x}}(a)$ is indeed the gcd of all the coefficients of $a(\bar{x})$. We finally recall that $\mathbb{F}$ is the algebraic closure of the field $\mathbb{K}(\bar{x})$. Under these conditions, the following results hold.

Theorem 1 (*Computation of* $\deg(\mathcal{P})$).

1. $\mathcal{P}^{-1}(\bar{x}) = \{\bar{t} \in \mathbb{F}^2 | G_i(\bar{t}, x_i) = 0, i \in \{1, 2, 3\}, G_4(\bar{t}) \neq 0\} = (\bigcap_{i=1}^3 V_i^{\bar{x}}) \setminus (\bigcap_{i=1}^3 V_i^{\bar{x}} \cap V_4)$.
2. $\mathcal{P}^{-1}(\bar{x}) = \{(A, B) \in \mathbb{F}^2 | S(A, \bar{x}) = 0, M(B, \bar{x}) = 0\}$, *where*
$$S(t_1, \bar{x}) = \mathrm{pp}_{\bar{x}}(\mathrm{Content}_Z(\mathrm{Res}_{t_2}(G_1, G_2 + ZG_3))),$$
$$M(t_2, \bar{x}) = \mathrm{pp}_{\bar{x}}(\gcd_{\mathbb{F}[t_2]}(G_1(A, t_2, x_1), G_2(A, t_2, x_2), G_3(A, t_2, x_3))),$$
where the content is taken in $\mathbb{K}(\mathcal{V})[\bar{t}]$.
3. $\mathcal{P}^{-1}(\bar{x}) \subseteq \{(A, B) \in \mathbb{F}^2 | S(A, \bar{x}) = 0, T(B, \bar{x}) = 0\}$, *where*
$$S(t_1, \bar{x}) = \mathrm{pp}_{\bar{x}}(\mathrm{Content}_Z(\mathrm{Res}_{t_2}(G_1, G_2 + ZG_3))),$$
$$T(t_2, \bar{x}) = \mathrm{pp}_{\bar{x}}(\mathrm{Content}_Z(\mathrm{Res}_{t_1}(G_1, G_2 + ZG_3))),$$
where the content is taken in $\mathbb{K}(\mathcal{V})[\bar{t}]$.
4. $\deg(\mathcal{P}) = \mathrm{Card}(\mathcal{P}^{-1}(\bar{x})) = \deg_{t_1}(S(t_1, \bar{x})) = \deg_{t_2}(T(t_2, \bar{x}))$.

Remark 2. In order to compute the content involved in the definition of the polynomials $S(t_1, \bar{x})$, $T(t_2, \bar{x})$, note that basic Arithmetic on the Euclidean domain $\mathbb{K}(\mathcal{V})[\bar{t}]$ can be carried out, without using the implicit equation of $\mathcal{V}$, by checking zero equality substituting $\mathcal{P}(\bar{t})$ in the polynomial expression. For more details see Pérez-Díaz et al. (2002).

For the next theorem, we consider the polynomial $H_{i,j}(\bar{t}) = \mathrm{lcm}(q_i, q_j)$, and the algebraic set $W_{i,j}$ defined over $\mathbb{K}$ by $H_{i,j}(\bar{t})$.

Theorem 2 (*Computation of* $\deg(\pi_{i,j}(\mathcal{P}))$). *Let* $i, j, k \in \{1, 2, 3\}$, $i < j$ *and* $i \neq k \neq j$.

1. $\pi_{i,j}(\mathcal{P})^{-1}(\overline{x}) = \left\{\overline{t} \in \mathbb{F}^2 \,\middle|\, G_\ell(\overline{t}, x_\ell) = 0, \ell \in \{i, j\}, H_{i,j}(\overline{t}) \neq 0\right\} = (V_i^{\overline{x}} \cap V_j^{\overline{x}}) \setminus (V_i^{\overline{x}} \cap V_j^{\overline{x}} \cap W_{i,j})$.
2. $\pi_{i,j}(\mathcal{P})^{-1}(\overline{x}) = \{(A, B) \in \mathbb{F}^2 | \; S_{i,j}(A, \overline{x}) = 0, \; M(B, \overline{x}) = 0\}$, *where*

$$S_{i,j}(t_1, \overline{x}) = \mathrm{pp}_{\overline{x}}(\mathrm{Res}_{t_2}(G_i(\overline{t}, x_i), G_j(\overline{t}, x_j))),$$
$$M(t_2, \overline{x}) = \mathrm{pp}_{\overline{x}}(\mathrm{gcd}_{\mathbb{F}[t_2]}(G_i(A, t_2, x_i), G_j(A, t_2, x_j))).$$

3. $\pi_{i,j}(\mathcal{P})^{-1}(\overline{x}) \subseteq \{(A, B) \in \mathbb{F}^2 | \; S_{i,j}(A, \overline{x}) = 0, \; T_{i,j}(B, \overline{x}) = 0\}$, *where*

$$S_{i,j}(t_1, \overline{x}) = \mathrm{pp}_{\overline{x}}(\mathrm{Res}_{t_2}(G_i(\overline{t}, x_i), G_j(\overline{t}, x_j))),$$
$$T_{i,j}(t_2, \overline{x}) = \mathrm{pp}_{\overline{x}}(\mathrm{Res}_{t_1}(G_i(\overline{t}, x_i), G_j(\overline{t}, x_j))).$$

4. $\deg(\pi_{i,j}(\mathcal{P})) = \mathrm{Card}(\pi_{i,j}(\mathcal{P})^{-1}(\overline{x})) = \deg_{t_1}(S_{i,j}(t_1, \overline{x})) = \deg_{t_2}(T_{i,j}(t_2, \overline{x}))$.

Remark 3. Observe that since $\gcd(p_i, q_i) = 1$ and $\deg_{t_2}(G_i(\overline{t}, x_i)) > 0$, the resultant $\mathrm{Res}_{t_k}(G_i(\overline{t}, x_i), G_j(\overline{t}, x_j))$, $i = 1, 2, k = 1, 2$, is not identically zero.

4. On the partial degrees of a surface

In this section, we generalize the results on partial degrees given in Sendra and Winkler (2001b), for the case of plane curves, and in Pérez-Díaz and Sendra (2005) for surfaces. We start by recalling the result for curves given in Theorem 5 in Sendra and Winkler (2001b). For this purpose, if $\mathcal{M}(t) = (\mathfrak{M}_1(t), \mathfrak{M}_2(t))$ is a rational plane curve parametrization, we denote $\pi_i(\mathcal{M})(t) = \mathfrak{M}_i(t)$, and by $\mathcal{M}$ and $\pi_i(\mathcal{M})$ the corresponding induced rational maps (see Section 2).

Theorem 3 (*Plane Curve Case Under Properness Assumption*). *Let $\mathcal{M}(t)$ be a rational parametrization in reduced form of a rational affine plane curve $\mathcal{C}$, and let $f(x_1, x_2) \in \mathbb{K}[x_1, x_2]$ be its defining polynomial. Then,*

1. (Partial degrees) *If $\mathcal{M}(t)$ is proper,*

$$\deg_{x_i}(\mathcal{C}) = \deg_{x_i}(f) = \deg(\pi_j(\mathcal{M})) = \deg_t(\pi_j(\mathcal{M})(t)),$$

where $i, j \in \{1, 2\}$ and $i \neq j$.
2. (Properness criterion) *$\mathcal{M}(t)$ is proper iff $\deg_t(\mathcal{M}(t)) = \max\{\deg_{x_1}(f), \deg_{x_2}(f)\}$.*

Theorem 3 seems to indicate that, under the assumption of properness, $\deg_{x_1}(\mathcal{V})$ (resp. for x_2, and for x_3) is given by the degree of the rational map induced by $\pi_{2,3}(\mathcal{P})$ (resp. $\pi_{1,3}(\mathcal{P})$, and $\pi_{1,2}(\mathcal{P})$). In Pérez-Díaz and Sendra (2005) (Theorem 5), Theorem 3 is generalized to the surface case, as follows.

Theorem 4 (*Non-Cylindrical Surface Case Under Properness Assumption*). *Let $\mathcal{V}$ not be a cylinder over any of the coordinate planes (i.e. $\deg_{x_k}(F) \neq 0, k = 1, 2, 3$), and let $S_{i,j}(t_1, \overline{x})$, $T_{i,j}(t_2, \overline{x})$ be the polynomials introduced in Theorem 2(3). Then,*

1. (Partial degrees) *If $\mathcal{P}(\overline{t})$ is proper*

$$\deg_{x_k}(\mathcal{V}) = \deg_{x_k}(F) = \deg(\pi_{i,j}(\mathcal{P})) = \deg_{t_1}(S_{i,j}) = \deg_{t_2}(T_{i,j}),$$

where $i, j, k \in \{1, 2, 3\}$, $i < j$ and $i \neq k \neq j$.
2. (Properness criterion) *$\mathcal{P}(\overline{t})$ is proper iff there exist $i, j, k \in \{1, 2, 3\}$, with $i < j$ and $i \neq k \neq j$, and such*

$$\deg_{x_k}(\mathcal{V}) = \deg_{x_k}(F) = \deg(\pi_{i,j}(\mathcal{P})) = \deg_{t_1}(S_{i,j}) = \deg_{t_2}(T_{i,j}).$$

In addition, in Pérez-Díaz and Sendra (2005) (Theorem 4), the following criterion to detect cylinders over the coordinates planes is given.

Theorem 5 (*Cylinder Criterion*). *Let $A_i(\overline{t}, \overline{h}) = q_i(\overline{h})G_i(\overline{t}, \mathfrak{P}_i(\overline{h}))$ where $\overline{h} = (h_1, h_2)$ and $i \in \{1, 2, 3\}$. Then $\mathcal{V}$ is a cylinder over the $x_i x_j$-plane iff* $\gcd(A_i, A_j) \neq 1$.

The following theorem generalizes the partial degree formula in Theorem 4 to the general surface case.

Theorem 6 (*General Surface Case*). *Let $\mathcal{P}(\bar{t})$ be non-necessarily proper. Then,*

$$\deg_{x_k}(\mathcal{V}) = \deg_{x_k}(F) = \frac{\deg(\pi_{i,j}(\mathcal{P}))}{\deg(\mathcal{P})} = \frac{\deg_{t_1}(S_{i,j})}{\deg_{t_1}(S)} = \frac{\deg_{t_2}(T_{i,j})}{\deg_{t_1}(S)},$$

where $i, j, k \in \{1, 2, 3\}$, $i < j$ and $i \neq k \neq j$, $S(t_1, \overline{x})$ as in Theorem 1(3), and $S_{i,j}(t_1, \overline{x})$, $T_{i,j}(t_2, \overline{x})$ as in Theorem 2(3).

Proof. We distinguish two cases depending on whether $\mathcal{V}$ is a cylinder or not.

1. Let $\mathcal{V}$ not be a cylinder over any coordinate plane, and let $i, j, k \in \{1, 2, 3\}$, $i < j$ and $i \neq k \neq j$. By Castelnuovo's Theorem (see Castelnuovo (1939)), there exists a proper parametrization $\mathcal{Q}(\bar{t})$ of $\mathcal{V}$, and by Lemma 3.1 in Arrondo et al. (1997) there exists $R(\bar{t}) \in \mathbb{K}(\bar{t})^2$ such that $\mathcal{P}(\bar{t}) = \mathcal{Q}(R(\bar{t}))$. Also note that $\dim(\pi_{i,j}(\mathcal{P})(\mathbb{K}^2)) = \dim(\pi_{i,j}(\mathcal{Q})(\mathbb{K}^2)) = \dim(\pi_{i,j}(\mathcal{V}))$; where $\pi_{i,j}(\mathcal{V})$ is the (i, j)-projection of $\mathcal{V}$. Moreover, since $\mathcal{V}$ is not a cylinder over the $x_i x_j$-plane, this dimension is 2. Thus, by Lemma 2 in Sendra and Winkler (2001a),
$$\deg(\pi_{i,j}(\mathcal{P})) = \deg(\pi_{i,j}(\mathcal{Q})) \cdot \deg(R), \quad \text{and} \quad \deg(\mathcal{P}) = \deg(\mathcal{Q}) \cdot \deg(R).$$
Since $\mathcal{Q}(\bar{t})$ is proper, $\deg(\mathcal{Q}) = 1$. Hence, $\deg(R) = \deg(\mathcal{P})$ which implies that $\deg(\pi_{i,j}(\mathcal{Q})) = \deg(\pi_{i,j}(\mathcal{P}))/\deg(\mathcal{P})$. Therefore, by Theorems 1, 2 and 4,
$$\deg_{x_k}(\mathcal{V}) = \deg_{x_k}(F) = \deg(\pi_{i,j}(\mathcal{Q})) = \frac{\deg(\pi_{i,j}(\mathcal{P}))}{\deg(\mathcal{P})} = \frac{\deg_{t_1}(S_{i,j})}{\deg_{t_1}(S)}.$$
2. Let $\mathcal{V}$ be a cylinder over the x_1x_2-plane (similarly over the other coordinate planes). Then, $\deg_{x_3}(F) = 0$. We distinguish two cases.
   i. Let $\deg_{x_2}(F) = 0$ (similarly if $\deg_{x_1}(F) = 0$). Since F is irreducible, up to multiplication by non-zero constants, $F(x_1, x_2, x_3) = x_1$. Under these conditions, we consider the surface $\mathcal{W}$ defined by
   $$G(x_1, x_2, x_3) = F(x_1 + x_2 + x_3, x_2, x_3) = x_1 + x_2 + x_3.$$
   Observe that $\mathcal{W}$ is not a cylinder and that $\mathcal{Q}(\bar{t}) = (p_1 - p_2 - p_3, p_2, p_3)$ parametrizes $\mathcal{W}$. In addition, $\deg(\pi_{2,3}(\mathcal{Q})) = \deg(\pi_{2,3}(\mathcal{P}))$ and $\deg(\mathcal{Q}) = \deg(\mathcal{P})$. Applying case 1, we get that
   $$\deg_{x_1}(F) = \deg_{x_1}(G) = \frac{\deg(\pi_{2,3}(\mathcal{Q}))}{\deg(\mathcal{Q})} = \frac{\deg(\pi_{2,3}(\mathcal{P}))}{\deg(\mathcal{P})} = \frac{\deg_{t_1}(S_{2,3})}{\deg_{t_1}(S)}.$$
   ii. Let $\deg_{x_2}(F) \neq 0$ and $\deg_{x_1}(F) \neq 0$. We consider the surface $\mathcal{W}$ defined by $G(x_1, x_2, x_3) = F(x_1 + x_3, x_2, x_3)$. Observe that $\mathcal{W}$ is not a cylinder and that $\mathcal{Q}(\bar{t}) = (p_1 - p_3, p_2, p_3)$ parametrizes $\mathcal{W}$. In addition, $\deg(\pi_{2,3}(\mathcal{Q})) = \deg(\pi_{2,3}(\mathcal{P})), \deg(\pi_{1,3}(\mathcal{Q})) = \deg(\pi_{1,3}(\mathcal{P}))$, and $\deg(\mathcal{Q}) = \deg(\mathcal{P})$. Under these conditions, applying case 1, we get that for $k = 1, 2,\ i, j \in \{1, 2, 3\}, i < j$ and $i \neq k \neq j$,
   $$\deg_{x_k}(F) = \deg_{x_k}(G) = \frac{\deg(\pi_{i,j}(\mathcal{Q}))}{\deg(\mathcal{Q})} = \frac{\deg(\pi_{i,j}(\mathcal{P}))}{\deg(\mathcal{P})} = \frac{\deg_{t_1}(S_{i,j})}{\deg_{t_1}(S)}. \quad \square$$

Example 1. Let $\mathcal{V}$ be the surface parametrized by

$$\mathcal{P}(\bar{t}) = \left(\frac{t_1^2 + t_2t_1 - 1 - t_1^2t_2 - 5t_1^4}{t_1}, \frac{4 - t_1^2 - 2t_2t_1 - t_2^2 + t_1^3 + 3t_1^2t_2 + 3t_1t_2^2 + t_2^3}{1 + t_1 + t_2 + 4t_1^2 + 8t_2t_1 + 4t_2^2}, \frac{1 + t_1^2t_2 + 5t_1^4}{t_1}\right).$$

By Theorem 1, $\deg(\mathcal{P}) = 4$ and by Theorem 2, $\deg(\pi_{1,2}(\mathcal{P})) = 12$, $\deg(\pi_{1,3}(\mathcal{P})) = 4$, and $\deg(\pi_{2,3}(\mathcal{P})) = 12$. Thus, by Theorem 6, $\deg_{x_3}(F) = 3$, $\deg_{x_2}(F) = 1$ and $\deg_{x_1}(F) = 3$. In fact,

$$F = x_1^2 + 2x_1x_3 + x_3^2 + x_2 + x_1x_2 + x_2x_3 - x_1^3 - 3x_1^2x_3 - 3x_1x_3^2 - x_3^3 - 4 + 4x_1^2x_2 + 8x_2x_1x_3 + 4x_2x_3^2.$$

5. Implicitization of plane curves and cylinders

In this section, we recall the result given in Sendra and Winkler (2001b) for the implicitization of plane algebraic curves, and we extend it to the case of cylinders. We start by recalling Theorem 8 in Sendra and Winkler (2001b).

Theorem 7 (*Implicitization of Plane Curves*). *Let $\mathcal{C}$ be a rational affine plane curve, let $f(x_1, x_2) \in \mathbb{K}[x_1, x_2]$ be its defining polynomial, and let $\mathcal{M}(t) = (m_1(t)/n_1(t), m_2(t)/n_2(t))$ be a rational parametrization in reduced form of $\mathcal{C}$. Then, up to multiplication by non-zero constants,*

$$f(x_1, x_2)^{\deg(\mathcal{M})} = \mathrm{Res}_t(H_1(t, x_1), H_2(t, x_2)),$$

where $H_i(t, x_i) = m_i(t) - x_in_i(t)$, $i = 1, 2$.

Note that the polynomials H_1, H_2 in Theorem 7 play the role, in the plane case, of the polynomials G_i introduced in Section 2. Also, observe that the implicit equation is expressed in Theorem 7 as a resultant. Thus, one may expect that in the cylindrical case the implicit equation is given in terms of the polynomials $S_{i,j}$. This is done in the next theorem.

Theorem 8 (*Implicitization of Cylinders*). *Let $\mathcal{V}$ be a cylinder over the x_ix_j-plane, where $i, j \in \{1, 2, 3\}$ and $i < j$.*

(1) *Let $a \in \mathbb{K}$ be such that $\mathfrak{P}_i(a, t_2), \mathfrak{P}_j(a, t_2)$ are in reduced form, and not both constant. Then, up to multiplication by non-zero constants,*

$$F(x_i, x_j)^{\deg(\pi_{i,j}(\mathcal{P}(a,t_2)))} = S_{i,j}(t_1, \bar{x}) = \mathrm{Res}_{t_2}(G_i(a, t_2, x_i), G_j(a, t_2, x_j)).$$

(2) *Let $b \in \mathbb{K}$ be such that $\mathfrak{P}_i(t_1, b), \mathfrak{P}_j(t_1, b)$ are in reduced form, and not both constant. Then, up to multiplication by non-zero constants,*

$$F(x_i, x_j)^{\deg(\pi_{i,j}(\mathcal{P}(t_1,b)))} = T_{i,j}(t_2, \bar{x}) = \mathrm{Res}_{t_1}(G_i(t_1, b, x_i), G_j(t_1, b, x_j)).$$

Proof. Let us see (1); statement (2) follows similarly. Let us assume w.l.o.g. that $(i, j) = (1, 2)$, and let $a \in \mathbb{K}$ be such that $\mathfrak{P}_1(a, t_2)$ is not constant (similarly if $\mathfrak{P}_2(a, t_2)$ is not constant). Then $F(x_1, x_2)$ defines an irreducible plane curve $\mathcal{C}$ in $\mathbb{K}^2$. $\pi_{1,2}(\mathcal{P}(a, t_2))$ is not constant because $\mathfrak{P}_1(a, t_2)$ is not constant. Moreover, since $F(\mathcal{P}(a, t_2)) = F(\pi_{1,2}(\mathcal{P}(a, t_2))) = 0$, one deduces that $\mathcal{C}$ is rational and that $\pi_{1,2}(\mathcal{P}(a, t_2))$ is a parametrization of $\mathcal{C}$ in reduced form. Thus, by

Theorem 7:

$$\mathrm{Res}_{t_2}(G_1(a, t_2, x_1), G_2(a, t_2, x_2)) = F(x_1, x_2)^{\deg(\pi_{1,2}(\mathcal{P}(a,t_2)))}.$$

Now, we prove the other equality in the statement. Let

$$R(t_1, \overline{x}) := \mathrm{Res}_{t_2}(G_1(\overline{t}, x_i),\ G_2(\overline{t}, x_j)),\quad R^*(\overline{x}) = \mathrm{Res}_{t_2}(G_1(a, t_2, x_1), G_2(a, t_2, x_2)).$$

Then, $S_{1,2}(t_1, \overline{x}) = \mathrm{pp}_{\overline{x}}(R(t_1, \overline{x}))$ and $R^*(\overline{x}) = F^{\lambda}$ where $\lambda = \deg(\pi_{1,2}(\mathcal{P}(a, t_2))) \in \mathbb{N}$. Furthermore, taking into account the behavior of the resultants under homomorphisms (see Winkler (1996)), and that the leading coefficient of the polynomials G_i w.r.t t_2 does not depend on t_1 (see assumption (1) in Section 2) we deduce that, up to constants in $\mathbb{K}^\star$, and for all $a \in \mathbb{K}$, $R(a, \overline{x}) = R^*(\overline{x}) = F(\overline{x})^{\lambda}$. Therefore, the primitive part of $R(t_1, \overline{x})$ w.r.t. $\overline{x}$ cannot depend on t_1. Thus $S_{1,2}(t_1, \overline{x}) = R^*(\overline{x})$ up to multiplication by non-zero constants. □

Remark 4. Note that, since $\mathcal{P}(\overline{t})$ parametrizes a surface, at least two coordinates of $\mathcal{P}(\overline{t})$ are not constant, and hence the hypotheses of the theorem are always satisfied.

In addition to Theorem 5, one deduces from Theorem 8 the following criterion for cylinders.

Corollary 1 (*Cylinder Criterion*). *The following statements are equivalent*

(1) *$\mathcal{V}$ is a cylinder over the $x_i x_j$-plane.*
(2) $\deg_{t_1}(S_{i,j}) = 0$.
(3) $\deg_{t_2}(T_{i,j}) = 0$.

Moreover, if $\mathcal{V}$ is a cylinder, both the polynomials $S_{i,j}$ and $T_{i,j}$ are a power of the implicit equation of $\mathcal{V}$.

Proof. From Theorem 8, if $\mathcal{V}$ is a cylinder over the $x_i x_j$-plane then $\deg_{t_1}(S_{i,j}) = \deg_{t_2}(T_{i,j}) = 0$ and both the polynomials are a power of the implicit equation of $\mathcal{V}$. Thus (1) implies (2) and (3). Let us see that (2) implies (1); similarly (3) implies (1). We assume that $\deg_{t_1}(S_{i,j}) = 0$. Let $R(t_1, \overline{x}) := \mathrm{Res}_{t_2}(G_i(\overline{t}, x_i),\ G_j(\overline{t}, x_j))$. Note that $R(t_1, \overline{x})$ is not identically zero (see Remark 3). We express R as $R(t_1, \overline{x}) = M(t_1)S_{i,j}(t_1, \overline{x})$, where M is the content of R w.r.t. $\overline{x}$. Now, observe that $G_k(\overline{t}, \mathfrak{P}_k(\overline{t})) = 0$ for $k = 1, 2, 3$. Thus, by the properties of the resultants (see Winkler (1996)), $R(t_1, \mathcal{P}(\overline{t})) = 0$. Therefore, $S_{i,j}(t_1, \mathcal{P}(\overline{t})) = 0$. This implies that F divides $S_{i,j}(t_1, \overline{x})$. Finally, since $S_{i,j}(t_1, \overline{x}) \in \mathbb{K}[x_i, x_j]$, one concludes that $F \in \mathbb{K}[x_i, x_j]$, and $\mathcal{V}$ is a cylinder over the $x_i x_j$-plane. □

The following lemma will be used in the next section.

Lemma 9. (i, j)*-settled rational surface parametrizations do not define cylinders over the $x_i x_j$-plane.*

Proof. Let $\mathcal{Q}(\overline{t}) = (\mathfrak{Q}_1(\overline{t}), \mathfrak{Q}_2(\overline{t}), \mathfrak{Q}_3(\overline{t}))$ be a rational (i, j)-settled surface parametrization, and $G(\overline{x})$ the defining polynomial of the surface $\mathcal{W}$ that it defines. Let $\mathcal{W}$ be a cylinder over the $x_i x_j$-plane, then $G(\overline{x}) \in \mathbb{K}[x_i, x_j]$. Taking derivatives in the equality $G(\mathcal{Q}(\overline{t})) = 0$ one gets that (G_i denotes the partial derivative of G w.r.t. x_i)

$$G_i(\mathcal{Q}(\overline{t}))\nabla(\mathfrak{Q}_i(\overline{t})) + G_j(\mathcal{Q}(\overline{t}))\nabla(\mathfrak{Q}_j(\overline{t})) = 0.$$

Now, observe that $G_i(\mathcal{Q}(\overline{t}))$ and $G_j(\mathcal{Q}(\overline{t}))$ cannot vanish simultaneously because this would imply that G_i and G_j divide the irreducible polynomial G, and hence G is constant. Therefore, $\{\nabla(\mathfrak{Q}_i(\overline{t})), \nabla(\mathfrak{Q}_j(\overline{t}))\}$ are linearly dependent, which is a contradiction. □

6. Main implicitization formulae

In the previous section, we have seen that the implicitization problem for cylinders reduces to the plane curve case. In this section we present the general formulae for computing the implicit equation of a rational surface that is not a cylinder over any of the coordinate planes. Observe that in Theorem 5 and Corollary 1 we have given algorithmic criteria to check whether $\mathcal{P}(\bar{t})$ defines one such cylinder. These general formulae generalize the formulas in Theorem 7 for plane curves, and in Theorem 8 for cylinders. Furthermore, the formulae provide a new method based on univariate resultants. For the clarity of explanation, in this section we motivate, present and illustrate the formula, and in the next section we prove it.

We recall that we have assumed w.l.o.g. that $\mathcal{P}(t)$ is a $(1, 2)$-settled parametrization (see Section 2). Thus, by Lemma 9, $\mathcal{V}$ is not a cylinder over the x_1x_2-plane. Therefore, taking into account Corollary 1, we have that $\deg_{t_1}(S_{1,2}(t_1, \bar{x})) > 0$ and $\deg_{t_2}(T_{1,2}(t_2, \bar{x})) > 0$.

Let us briefly and intuitively motivate the formulae. In Theorem 7, we have seen that the implicit equation $f(x_1, x_2)$ of a rational plane curve, parametrized in reduced form as $\mathcal{M}(t) = (\frac{m_1(t)}{n_1(t)}, \frac{m_2(t)}{n_2(t)})$, is related to a resultant as follows:

$$f(x_1, x_2)^{\deg(\mathcal{M})} = \mathrm{Res}_t(H_1(t, x_1), H_2(t, x_2)),$$

where $H_i(t, x_i) = m_i(t) - x_i n_i(t)$, $i = 1, 2$, and $\mathcal{M}$ is the rational map induced by $\mathcal{M}(t)$. By the well-known properties of resultants, if we regard $H_i(t, x_i)$ as univariate polynomials in $\mathbb{K}(x_1, x_2)[t]$, and $\mathbb{L}$ denotes the algebraic closure of $\mathbb{K}(x_1, x_2)$, then

$$f(x_1, x_2)^{\deg(\mathcal{M})} = \mathrm{Res}_t(H_1(t, x_1), H_2(t, x_2)) = A(x_1)^r \prod_{\substack{U(x_1)\in\mathbb{L}\\ H_1(U,x_1)=0}} H_2(U(x_1), x_2),$$

where $A(x_1)$ is the leading coefficient of H_1 w.r.t. t and $r := \deg_t(H_2)$. Therefore,

$$f(x_1, x_2)^{\deg(\mathcal{M})} = A(x_1)^r \prod_{U(x_1)\in\pi_1(\mathcal{M})^{-1}(x_1)} H_2(U(x_1), x_2).$$

Thus for the case of the surface $\mathcal{V}$, one might expect that $F(\bar{x})^{\deg(\mathcal{P})}$ is given, up to factors in $\mathbb{K}[x_1, x_2]^{\star}$, by

$$\prod_{U\in\pi_{1,2}(\mathcal{P})^{-1}(x_1,x_2)} G_3(U(x_1, x_2), x_3).$$

Indeed, in Section 8 (see Lemma 16 and Remark 7), we prove that

$$F(\bar{x})^{\deg(\mathcal{P})} = \mathrm{pp}_{x_3}\left(\prod_{U\in\pi_{1,2}(\mathcal{P})^{-1}(x_1,x_2)} G_3(U(x_1, x_2), x_3)\right).$$

For instance, let $\mathcal{V}$ be the surface parametrized by

$$\mathcal{P}(\bar{t}) = \left(\frac{t_2 + t_1^3}{t_2 t_1^2}, \frac{t_2 + t_1^3}{t_1}, t_1^3 t_2 + 5\right).$$

The implicit equation of $\mathcal{V}$ is

$$F(\bar{x}) = x_2^3 - x_1^2 x_3 x_2^2 + 5x_1^2 x_2^2 + 25x_1^3 - 10x_1^3 x_3 + x_1^3 x_3^2.$$

Applying Theorem 2, we get that $\pi_{1,2}(\mathcal{P})^{-1}(x_1, x_2) = \{U_{1,+}, U_{1,-}, U_{2,+}, U_{2,-}\}$, where

$$U_{1,\pm} = \left(\frac{\pm\sqrt{2(x_1x_2 + \sqrt{\Xi})x_2}\,(x_1x_2 - \sqrt{\Xi})}{4x_1x_2}, \frac{\pm\sqrt{2(x_1x_2 + \sqrt{\Xi})x_2}}{2x_1} \right),$$

$$U_{2,\pm} = \left(\frac{\pm\sqrt{2(x_1x_2 - \sqrt{\Xi})x_2}\,(x_1x_2 + \sqrt{\Xi})}{4x_1x_2}, \frac{\pm\sqrt{2(x_1x_2 - \sqrt{\Xi})x_2}}{2x_1} \right),$$

with $\Xi = x_1^2x_2^2 - 4x_1x_2$. Now, up to multiplication by a non-zero constant,

$$\mathrm{pp}_{x_3}\left(\prod_{U \in \pi_{1,2}(\mathcal{P})^{-1}(x_1,x_2)} G_3(U, x_3) \right) = (x_2^3 - x_1^2x_3x_2^2 + 5x_1^2x_2^2 + 25x_1^3$$
$$-10x_1^3x_3 + x_1^3x_3^2)^2 = F(\overline{x})^2.$$

Moreover, applying Theorem 1, $\deg(\mathcal{P}) = 2$.

Obviously, in general, trying to compute the elements in the fibre $\pi_{1,2}(\mathcal{P})^{-1}(x_1, x_2)$ is not a good idea. Instead of that, we provide a resultant-based version of the above formula. In the following theorem, that will be proved in Section 8, we formally state this result.

Theorem 10 (*First Main Implicitization Formula*). *Let $\mathcal{V}$ be a rational affine surface defined by the irreducible polynomial $F(\overline{x}) \in \mathbb{K}[\overline{x}]$, and let $\mathcal{P}(\overline{t})$ be a rational $(1, 2)$-settled parametrization of $\mathcal{V}$ in reduced form. Then, there exists $r \in \mathbb{N}$, such that, up to constants in $\mathbb{K}^\star$,*

$$F(\overline{x})^r = \mathrm{pp}_{x_3}(h(\overline{x})),$$

where

(1) $h(\overline{x}) = \mathrm{Content}_{\{Z,W\}}(\mathrm{Res}_{t_2}(T_{1,2}(t_2, \overline{x}), K(t_2, Z, W, \overline{x}))) \in \mathbb{K}[\overline{x}]$,
(2) $K(t_2, Z, W, \overline{x}) = \mathrm{Res}_{t_1}(S_{1,2}(t_1, \overline{x}), G(\overline{t}, Z, W, \overline{x})) \in \mathbb{K}[t_2, Z, W, \overline{x}]$,
(3) $G(\overline{t}, Z, W, \overline{x}) = G_3(\overline{t}, x_3) + ZG_1(\overline{t}, x_1) + WG_2(\overline{t}, x_2) \in \mathbb{K}[\overline{t}, Z, W, \overline{x}]$, *and*
(4) $S_{1,2}(t_1, \overline{x}), T_{1,2}(t_2, \overline{x})$ *are as in Theorem 2.*

The above result relates the implicit equation to a natural power with the primitive part of $h(\overline{x})$. In the next theorem, we present a second formula where this exponent turns out to be the degree of the rational map induced by the parametrization.

Theorem 11 (*Second Main Implicitization Formula*). *Let $\mathcal{V}, \mathcal{P}(\overline{t}), F, h, K, G, S_{1,2}, T_{1,2}$ be as in Theorem 10. If $S_{1,2}, T_{1,2}$ are square-free then, up to constants in $\mathbb{K}^\star$,*

$$F(\overline{x})^{\deg(\mathcal{P})} = \mathrm{pp}_{x_3}(h(\overline{x})).$$

Remark 5. We observe that, since the elements of $\pi_{1,2}(\mathcal{P})^{-1}(x_1, x_2)$ are simple points of transversal intersection of the polynomials $G_1(\overline{t}, x_1), G_2(\overline{t}, x_2)$ (see Lemma 5 in Pérez-Díaz and Sendra (2005)), and $(0 : 1 : 0)$ is not on the projective curves defined by G_1, G_2 (see assumptions in Section 2), then $T_{1,2}, S_{1,2}$ are square-free if $(0 : 1 : 0)$, $(1 : 0 : 0)$ are not on any line connecting two points on the fibre, and $(1 : 0 : 0)$ is not on the projective curves defined by G_1, G_2. Thus, in order to apply Theorem 11 one simply has to consider a linear change of variables $L(\overline{t})$ on $\mathcal{P}(\overline{t})$ (see Cox et al. (1998b)) such that the previous conditions are satisfied, and the general assumptions introduced in Section 2 are preserved. Under these conditions, Theorem 11 can be applied to the new parametrization $\mathcal{P}^\star(\overline{t}) = \mathcal{P}(L(\overline{t}))$.

Coming back to the above example, we get

$$G_1(\bar{t}, x_1) = t_2 + t_1^3 - x_1 t_2 t_1^2, \;\; G_2(\bar{t}, x_2) = t_2 + t_1^3 - x_2 t_1, \;\; G_3(\bar{t}, x_3) = t_1^3 t_2 + 5 - x_3.$$

Moreover

$$S_{1,2}(t_1, x_1, x_2) = -x_1 t_1^4 + x_2 x_1 t_1^2 - x_2, \quad T_{1,2}(t_2, x_1, x_2) = x_1^3 t_2^4 - x_1^2 t_2^2 x_2^2 + x_2^3.$$

Then,

$$\begin{aligned}\mathrm{pp}_{x_3}(\mathrm{Content}_{\{Z,W\}}(\mathrm{Res}_{t_2}(T_{1,2}, K))) &= (x_2^3 - x_1^2 x_3 x_2^2 + 5x_1^2 x_2^2 + 25x_1^3 \\ &\quad -10x_1^3 x_3 + x_1^3 x_3^2)^2 = F(\bar{x})^2.\end{aligned}$$

Observe that both the polynomials $S_{1,2}$ and $T_{1,2}$ are square-free and $\deg(\mathcal{P}) = 2$.

7. Algorithm, examples and practical implementation

In this section we present the algorithm derived from the formula provided by Theorem 10. A similar algorithm can be derived from Theorem 11. Also, we illustrate the algorithm by some examples. Finally, we present some computing times of our implementation.

Implicitization Algorithm for Surfaces: Given the rational parametrization, in reduced form,

$$\mathcal{P}(\bar{t}) = (\mathfrak{P}_1(\bar{t}), \mathfrak{P}_2(\bar{t}), \mathfrak{P}_3(\bar{t})) = \left(\frac{p_1(\bar{t})}{q_1(\bar{t})}, \frac{p_2(\bar{t})}{q_2(\bar{t})}, \frac{p_3(\bar{t})}{q_3(\bar{t})}\right), \text{ where } \bar{t} = (t_1, t_2)$$

of a surface $\mathcal{V}$, the algorithm computes the implicit equation $F(\bar{x})$ of $\mathcal{V}$.

1. [Cylinder detection] Apply Theorem 5 to check whether $\mathcal{V}$ is a cylinder over the $x_i x_j$-plane. In the affirmative case: find $a \in \mathbb{K}$ such that $\mathfrak{P}_i(a, t_2)$ is not a constant and $\mathfrak{P}_i(a, t_2)$, $\mathfrak{P}_j(a, t_2)$ are in reduced form (see Theorem 8), determine (see Theorem 2)
$$F^*(\bar{x}) = \mathrm{Res}_{t_2}(G_i(a, t_2, x_i), G_j(a, t_2, x_j)),$$
and return $\ll F^*(\bar{x})/\gcd(F^*(\bar{x}), \frac{\partial F^*(\bar{x})}{\partial x_i}) \gg$.
2. [$(1, 2)$-settled preparation] Find $i, j \in \{1, 2, 3\}$ such that $\{\nabla\mathfrak{P}_i(\bar{t}), \nabla\mathfrak{P}_j(\bar{t})\}$ are linearly independent. If $(i, j) \neq (1, 2)$ apply to $\mathcal{P}(t)$ the linear change of coordinates $\mathcal{L} := \{x_1 = x_i, x_2 = x_j, x_3 = x_k\}$ where $k \in \{1, 2, 3\} \setminus \{i, j\}$.
3. [General assumptions preparation] Check whether any of the projective curves defined by each non-constant $p_i(\bar{t})$ and $q_i(\bar{t})$ passes through the point at infinity $(0 : 1 : 0)$, where the homogeneous variables are (t_1, t_2, w). If so, apply a linear change of parameters to $\mathcal{P}(\bar{t})$.
4. Compute the polynomials
   (a) $G_i(\bar{t}, x_i) := p_i(\bar{t}) - x_i\, q_i(\bar{t}), \; i = 1, 2, 3.$
   (b) $S_{1,2}(t_1, \bar{x})$ and $T_{1,2}(t_2, \bar{x})$ as in Theorem 2.
   (c) $G(\bar{t}, Z, W, \bar{x}) = G_3(\bar{t}, x_3) + ZG_1(\bar{t}, x_1) + WG_2(\bar{t}, x_2)$.
   (d) $K(t_2, Z, W, \bar{x}) = \mathrm{Res}_{t_1}(S_{1,2}, G)$.
   (e) $h(\bar{x}) = \mathrm{Content}_{\{Z,W\}}(\mathrm{Res}_{t_2}(T_{1,2}, K))$.
   (f) $F^*(\bar{x}) = \mathrm{pp}_{x_3}(h(\bar{x}))$ and $\tilde{F}(\bar{x}) = F^*(\bar{x})/\gcd(F^*(\bar{x}), \frac{\partial F^*(\bar{x})}{\partial x_1})$.
5. Return $\ll \tilde{F}(\mathcal{L}^{-1}(\bar{x})) \gg$

Remark 6. In order to determine $h(\overline{x})$, one needs to compute univariate resultants of polynomials in $\mathbb{K}[\overline{t}, Z, W, \overline{x}]$. Nevertheless, taking into account Lemma 9 in Pérez-Díaz and Sendra (2004), one may deduce that there exists a non-open Zariski subset Ω of $\mathbb{K}^2$ such that for $(Z_i, W_i) \in \Omega, i = 1, 2$, the polynomial $h(\overline{x})$ is equal to

$$\gcd(\mathrm{Res}_{t_2}(T_{1,2}(t_2, \overline{x}), K(t_2, Z_1, W_1, \overline{x})), \mathrm{Res}_{t_2}(T_{1,2}(t_2, \overline{x}), K(t_2, Z_2, W_2, \overline{x}))),$$

where

$$K(t_2, Z_i, W_i, \overline{x}) = \mathrm{Res}_{t_1}(S_{1,2}(t_1, \overline{x}),\ G(\bar{t}, Z_i, W_i, \overline{x})).$$

Therefore, one may also derive an heuristic algorithm from Theorem 10.

In the following, we illustrate the algorithm by some examples.

Example 2. Let $\mathcal{V}$ be the surface parametrized by

$$\mathcal{P}(\bar{t}) = \left(\frac{78 - 24\,t_2 + 8\,t_1 + 8\,t_2^2}{28 - 18\,t_2 + 62\,t_1 + 62\,t_2^2}, -36\,(t_1 + t_2^2)^3 - 95\,(t_1 + t_2^2)^2 + 8\,t_1 + 8\,t_2^2 + 92, \frac{8\,(t_1 + t_2^2)^2 - 95\,t_1 - 95\,t_2^2 - 17}{44\,(t_1 + t_2^2)^2 + 66\,t_1 + 66\,t_2^2 - 62}\right).$$

In Step 1, we apply Theorem 5, and we deduce that $\mathcal{V}$ is a cylinder over the x_2x_3-plane since $\gcd(A_2, A_3) = (t_1 - h_1 - h_2^2 + t_2^2) \neq 1$, where $A_i(\bar{t}, \overline{h}) = q_i(\overline{h})G_i(\bar{t}, \mathfrak{P}_i(\overline{h}))$, $\overline{h} = (h_1, h_2)$, and $i \in \{2, 3\}$. We check that $\mathfrak{P}_2(0, t_2)$ is not a constant and that $\mathfrak{P}_2(0, t_2)$, $\mathfrak{P}_3(0, t_2)$ are in reduced form. So, we compute $\mathrm{Res}_{t_2}(G_2(0, t_2, x_2), G_3(0, t_2, x_3))$, and taking its square-free factorization one gets that the implicit equation of $\mathcal{V}$ is

$$\begin{aligned} F(\overline{x}) = {} & 141\,275\,192\,x_3^2 - 858\,132\,x_2\,x_3^3 - 4901\,336\,x_2\,x_3^2 + 21\,296\,x_2^2x_3^3 - 9795\,933\,x_2 \\ & + 773\,561\,469\,x_3 - 5842\,477\,x_2\,x_3 - 6152\,156\,x_3^3 + 2112\,x_2^2x_3 - 128\,x_2^2 \\ & - 11\,616\,x_2^2x_3^2 + 861\,393\,645. \end{aligned}$$

Example 3. Let $\mathcal{V}$ be the surface parametrized by

$$\mathcal{P}(\bar{t}) = \left(\frac{2\,t_2^2 + 6 + t_1^2\,t_2^2 + t_2^6 + 3\,t_2^4}{t_1^2 + t_2^4 + 3\,t_2^2}, \frac{t_2^6 + 3\,t_2^4 + t_1^2}{t_2^2 + 3}, \frac{t_1^2}{(t_2^2 + 3)\,t_2^4}\right).$$

In Step 1, we check that $\mathcal{V}$ is not a cylinder over any of the coordinate planes. In Step 2, we see that $\mathcal{P}(\bar{t})$ is $(1, 2)$-settled, and in Step 3 we certify that the general assumptions are satisfied. In Step 4, we get:

(1) $G_1(\bar{t}, x_1) = 2\,t_2^2 + 6 + t_1^2\,t_2^2 + t_2^6 + 3\,t_2^4 - x_1\,t_1^2 - x_1\,t_2^4 - 3\,x_1\,t_2^2$, $G_2(\bar{t}, x_2) = t_2^6 + 3\,t_2^4 + t_1^2 - x_2\,t_2^2 - 3\,x_2$, $G_3(\bar{t}, x_3) = t_1^2 - x_3\,t_2^6 - 3\,x_3\,t_2^4$,

(2) $S_{1,2}(t_1, \overline{x}) = 152 + x_1^3\,x_2^2 + 8\,x_2^2\,x_1 - 12\,x_1^3\,x_2 - x_2^3\,x_1 + 10\,t_1^4 - 36\,t_1^2 + 48\,x_1 + 140\,x_2 + t_1^6 - 72\,x_1\,t_1^2 + 44\,x_2\,x_1 - 6\,x_1^2\,t_1^2 - 38\,x_2\,x_1^2 - 8\,x_1\,t_1^2\,x_2 - 28\,t_1^2\,x_2 + 26\,x_2^2 - 3\,x_2^3 - t_1^4\,x_2 - 5\,t_1^2\,x_2^2 + 3\,x_2^2\,x_1^2 + 4\,x_1^3\,t_1^2 + 3\,x_1^2\,t_1^4 + 6\,x_1^2\,t_1^2\,x_2 - t_1^4\,x_1\,x_2 - 2\,x_1\,t_1^2\,x_2^2 + x_1^3\,t_1^4 + 2\,x_1^3\,t_1^2\,x_2$, $T_{1,2}(t_2, \overline{x}) = t_2^6 - t_2^4 - x_1\,t_2^4 + x_1\,t_2^2 - x_2\,t_2^2 - 2 + x_2\,x_1$,

(3) $\mathrm{pp}_{x_3}(h(\overline{x})) = (4 + 4\,x_3^3 + 4\,x_2 + 12\,x_3 - 4\,x_2\,x_1\,x_3^3 - x_1^2\,x_2\,x_3^2 + x_2^2\,x_1^2\,x_3^2 + x_2^2\,x_1^2\,x_3^3 + 4\,x_2\,x_3^2 - 8\,x_2\,x_1\,x_3^2 + x_2^2\,x_3 - 2\,x_2\,x_1^2\,x_3 - 4\,x_2\,x_1\,x_3 - x_2^3\,x_3^2 - x_2\,x_1^2 + x_2^2 + 12\,x_3^2 + 8\,x_2\,x_3)^4$.

Therefore, the implicit equation defining the surface $\mathcal{V}$ is

$$F(\overline{x}) = 4 + 4x_3^3 + 4x_2 + 12x_3 - 4x_2x_1x_3^3 - x_1^2x_2x_3^2 + x_2^2x_1^2x_3^2 + x_2^2x_1^2x_3^3 + 4x_2x_3^2 - 8x_2x_1x_3^2 + x_2^2x_3 - 2x_2x_1^2x_3 - 4x_2x_1x_3 - x_2^3x_3^2 - x_2x_1^2 + x_2^2 + 12x_3^2 + 8x_2x_3.$$

Example 4. Let $\mathcal{V}$ be the surface parametrized by

$$\mathcal{P}(\bar{t}) = \left(\frac{t_1\ (t_1+t_2)}{t_2^4}, \frac{t_1}{t_2^4}, \frac{t_2}{t_1^4}\right).$$

In Step 1, we check that $\mathcal{V}$ is not a cylinder over any of the coordinate planes. In Step 2, we see that $\mathcal{P}(\bar{t})$ is (1, 2)-settled, and in Step 3 we consider $\mathcal{P}(t_1+t_2, t_2)$ in order to fulfill the general assumptions. In Step 4, we get:

(1) $G_1(\bar{t}, x_1) = x_1t_2^4 - t_1^2 - 3t_1t_2 - 2t_2^2$, $G_2(\bar{t}, x_2) = x_2t_2^5 - t_1 - t_2$, $G_3(\bar{t}, x_3) = x_3t_1^5 + 5x_3t_1^4t_2 + 10x_3t_1^3t_2^2 + 10x_3t_1^2t_2^3 + 5x_3t_1t_2^4 + x_3t_2^5 - t_2$,
(2) $S_{1,2}(t_1, \overline{x}) = x_1^4 - 4x_1^3t_1x_2 - 8x_1x_2^2 - 4x_2^3t_1^3x_1 + x_2^4t_1^4 - 8x_2^3t_1 + 6x_2^2t_1^2x_1^2$, $T_{1,2}(t_2, \overline{x}) = -x_2^2t_2^4 - x_2t_2 + x_1$,
(3) $\mathrm{pp}_{x_3}(h(\overline{x})) = -x_2^{14} - 3x_2^{13}x_3 - 3x_2^{12}x_3^2 - x_2^{11}x_3^3 - 15x_2^{11}x_3x_1^3 + 95x_2^{10}x_3^2x_1^3 - 15x_2^9x_3^3x_1^3 - 60x_2^8x_3^2x_1^6 - 60x_2^7x_3^3x_1^6 - 50x_2^5x_3^3x_1^9 + x_3^4x_1^{15}$.

Therefore, the implicit equation defining the surface $\mathcal{V}$ is

$$F(\overline{x}) = -x_2^{14} - 3x_2^{13}x_3 - 3x_2^{12}x_3^2 - x_2^{11}x_3^3 - 15x_2^{11}x_3x_1^3 + 95x_2^{10}x_3^2x_1^3 - 15x_2^9x_3^3x_1^3 - 60x_2^8x_3^2x_1^6 - 60x_2^7x_3^3x_1^6 - 50x_2^5x_3^3x_1^9 + x_3^4x_1^{15}.$$

We finish this section by illustrating in the following table the performance of our implementation. Computing times, running on a Dual Intel Xeon 3.4 GHz and 8 GB of RAM, are given in seconds of CPU. In the table, we also show the degree of each parametrization, the degree of the output implicit equation, and the number of terms of the implicit equation. The parametrizations used in the analysis appear in the Appendix.

$\mathcal{P}(\bar{t})$	Time	$\deg(\mathcal{P}(t))$	$\mathrm{tdeg}(F(\overline{x}))$	Number of terms of $F(\overline{x})$
$\mathcal{P}_1(\bar{t})$	0.500	6	32	111
$\mathcal{P}_2(\bar{t})$	0.046	7	16	10
$\mathcal{P}_3(\bar{t})$	0.031	12	48	148
$\mathcal{P}_4(\bar{t})$	0.469	6	24	1027
$\mathcal{P}_5(\bar{t})$	1.39	3	11	164
$\mathcal{P}_6(\bar{t})$	5.360	3	9	106
$\mathcal{P}_7(\bar{t})$	4.921	5	17	206
$\mathcal{P}_8(\bar{t})$	6.610	7	30	602
$\mathcal{P}_9(\bar{t})$	0.953	12	60	1645
$\mathcal{P}_{10}(\bar{t})$	0.062	12	36	156
$\mathcal{P}_{11}(\bar{t})$	0.171	6	23	418
$\mathcal{P}_{12}(\bar{t})$	3.5	10	26	367

Parametrizations $\mathcal{P}_4(\bar{t}), \mathcal{P}_6(\bar{t}), \mathcal{P}_7(\bar{t}), \mathcal{P}_8(\bar{t})$ have similar degrees, number of terms, etc. However, $\mathcal{P}_6(\bar{t}), \mathcal{P}_7(\bar{t}), \mathcal{P}_8(\bar{t})$ take over 10 times as long to compute than $\mathcal{P}_4(\bar{t})$. The explanation for this phenomenon is the following. If the polynomials $S_{1,2}$ or $T_{1,2}$, computed in Step 4(b) of the algorithm, are a power of another polynomial, say $S_{1,2} = \bar{S}_{1,2}(t_1, \bar{x})^{n_1}$ or $T_{1,2} = \bar{T}_{1,2}(t_2, \bar{x})^{n_2}$, the polynomials $\mathrm{Res}_{t_1}(S_{1,2}, G)$ and $\mathrm{Res}_{t_2}(T_{1,2}, G)$ (see Step 4(d) and (e)) are simpler to compute:

$$K = \mathrm{Res}_{t_1}(S_{1,2}, G) = \mathrm{Res}_{t_1}(\bar{S}_{1,2}, G)^{n_1},$$

$$\mathrm{Res}_{t_2}(T_{1,2}, K) = \mathrm{Res}_{t_2}(\bar{T}_{1,2}, K)^{n_2} = \mathrm{Res}_{t_2}(\bar{T}_{1,2}, \mathrm{Res}_{t_1}(\bar{S}_{1,2}, G))^{n_1 n_2}.$$

Now, for $\mathcal{P}_4(\bar{t})$,

$$S_{1,2} = \left(-4\,t_1^8 + 8\,t_1^6 x + 8\,x t_1^4 + 12\,x t_1^2 + xy\right)^2,$$

while for $\mathcal{P}_6(\bar{t}), \mathcal{P}_7(\bar{t}), \mathcal{P}_8(\bar{t})$, $S_{1,2}$ is square-free and very dense. Indeed, if we consider the new parametrization $\mathcal{P}_4^*(\bar{t}) = \mathcal{P}_4(t_2 - t_1, t_2)$, that obviously defines the same surface, the corresponding $S_{1,2}$ is now square-free of degree 16 with 148 terms, and the computing time for $\mathcal{P}_4^*(\bar{t})$ is 12.342.

8. Proof of the main implicitization formulae

We assume that we are under the hypotheses of Theorem 10; that is, $\mathcal{V}$ is a rational affine surface defined by the irreducible polynomial $F(\bar{x}) \in \mathbb{K}[\bar{x}]$, and $\mathcal{P}(\bar{t})$ is a rational $(1,2)$-settled parametrization of $\mathcal{V}$ in reduced form.

Lemma 12. *Let*

$$\mathcal{M}(x_1, x_2) = \mathrm{Res}_{t_2}(T_{1,2}(t_2, \bar{x}),\ R(t_2, \bar{x})),$$

where

$$R(t_2, x_1, x_2) = \mathrm{Content}_Z(\mathrm{Res}_{t_1}(G_1(\bar{t}, x_1) + ZG_2(\bar{t}, x_2), q_3(\bar{t}))).$$

Then, $\mathcal{M}(x_1, x_2)$ is not identically zero.

Proof. Let $D(\bar{t}, x_1, x_2, Z) := G_1(\bar{t}, x_1) + ZG_2(\bar{t}, x_2)$. First we see that $\deg_{t_2}(R) > 0$. Indeed, by Remark 1, G_1 does depend on t_2, and hence D does also depend on this variable. Now, since $q_3(t)$ is not zero because it is a denominator, R is either a constant or it has positive degree in t_2. If R is a non-zero constant, since $\mathcal{P}(\bar{t})$ is $(1,2)$-settled by Lemma 9 and Corollary 1 $\deg_{t_2}(T_{1,2}(t_2, \bar{x})) > 0$, one has that $\mathcal{M}$ is a non-zero constant, and thus the lemma holds. If $R = 0$, then D has a non-constant factor in $\mathbb{K}[\bar{t}]$, which is impossible because $\gcd(p_1, p_2) = 1$. Thus, in the following let q_3 be non-constant, and let us assume that $\mathcal{M} = 0$. We already know that $\deg_{t_2}(R) > 0$ and $\deg_{t_2}(T_{1,2}) > 0$. Therefore, $T_{1,2}$ and R have a common factor depending on t_2. Moreover, since this factor is primitive w.r.t. $\bar{x}$ (see Theorem 2), this factor (regarded as univariate polynomial in t_2) cannot have constant roots. Let B be a root of this factor (note that $B \notin \mathbb{K}$), then $T_{1,2}(B, \bar{x}) = R(B, \bar{x}) = 0$. Therefore, $\mathrm{Res}_{t_1}(D, q_3)(B) = 0$. Now, since q_3 is not a constant, and the leading coefficient of $q_3(\bar{t})$ w.r.t. t_1 does not vanish at B, because $B \notin \mathbb{K}$, and $\deg_{t_1}(D) > 0$ (see Remark 1(4)) applying well-known resultant properties (see Winkler (1996)), one deduces that there exists A such that $D(A, B, x_1, x_2, Z) = q_3(A, B) = 0$. Thus,

$G_1(A, B, x_1) = G_2(A, B, x_2) = q_3(A, B) = 0$. Now, we prove that $\pi_{1,2}(\mathcal{P})(A, B) = (x_1, x_2)$. Indeed, let us see that $\mathfrak{P}_1(A, B) = x_1$; similarly for $\mathfrak{P}_2(A, B) = x_2$. First observe that because of Remark 1(1), $\mathfrak{P}_1(\bar{t})$ is not a constant; in particular it is not zero. Moreover, $\gcd(p_1, q_1) = 1$. Therefore, the common solutions of $p_1(\bar{t}) = q_1(\bar{t}) = 0$ are in $\mathbb{K}^2$. So, $q_1(A, B) \neq 0$, since otherwise $p_1(A, B) = 0$ and $(A, B) \notin \mathbb{K}^2$; note that $B \notin \mathbb{K}$. Thus, $\mathfrak{P}_1(A, B)$ is well-defined, and since $G_1(A, B, x_1) = 0$, one has that $\mathfrak{P}_1(A, B) = x_1$. Thus, taking $U = (A, B)$, one has that $U \in \pi_{1,2}(\mathcal{P})^{-1}(x_1, x_2)$, $U \notin \mathbb{K}^2$ and $q_3(U) = 0$. Furthermore, $p_3(U) \neq 0$ because the intersection points of p_3, q_3 are in $\mathbb{K}^2$; note that $p_3(\bar{t})$ is not zero (recall that $\mathcal{P}(t)$ is $(1, 2)$-settled) and that $\gcd(p_3, q_3) = 1$, and hence the t_j-coordinates of the intersection points of the polynomials p_3, q_3 are given by $\mathrm{Res}_{t_i}(p_1, q_1) \in \mathbb{K}[t_j]$, $j, i \in \{1, 2\}$, $j \neq i$. Now, let F be expressed as

$$F(\bar{x}) = F_d(x_1, x_2)x_3^d + \cdots + F_0(x_1, x_2), \text{ where } F_d \neq 0.$$

Note that $d > 0$ because F does not define a cylinder over the x_1x_2-plane (see Lemma 9), that $F_0 \neq 0$, because if $d > 1$ and $F_0 = 0$ then F is reducible, which is impossible, and if $d = 1$ and $F_0 = 0$ then $\mathfrak{P}_3(\bar{t}) = 0$ which is impossible because $\mathcal{P}(\bar{t})$ is $(1, 2)$-settled. We introduce the polynomial

$$F^*(\bar{x}) = F_d(x_1, x_2) + \cdots + F_0(x_1, x_2)x_3^d.$$

Since $d > 0$ and $F_0, F_d \neq 0$, one has that x_3 does not divide F^*; i.e. $F^*(x_1, x_2, 0) \neq 0$. Clearly,

$$x_3^d F^*(\bar{x}) = F\left(x_1, x_2, \frac{1}{x_3}\right).$$

Let (note that $p_3 \neq 0$ because $(1, 2)$-settled hypothesis)

$$\mathcal{Q}(\bar{t}) = \left(\frac{p_1(\bar{t})}{q_1(\bar{t})}, \frac{p_2(\bar{t})}{q_2(\bar{t})}, \frac{q_3(\bar{t})}{p_3(\bar{t})}\right).$$

Then,

$$\left(\frac{q_3(\bar{t})}{p_3(\bar{t})}\right)^d F^*(\mathcal{Q}(\bar{t})) = F(\mathcal{P}(\bar{t})) = 0.$$

Since $q_3(\bar{t}) \neq 0$, $F^*(\mathcal{Q}(\bar{t})) = 0$. Hence $0 = F^*(\mathcal{Q}(U)) = F^*(x_1, x_2, 0)$, which is a contradiction. □

Lemma 13. *Let $h(\bar{x})$ be as in Theorem 10. Then,*

(1) *$h(\bar{x})$ is not identically zero.*
(2) $\mathrm{pp}_{x_3}(h(\bar{x}))$ *is not constant.*

Proof. Let us see statement (1). Since $\mathcal{P}(\bar{t})$ is $(1, 2)$-settled, reasoning as in the proof of Lemma 12, $\deg_{t_1}(S_{1,2}) > 0$. Moreover, by definition it is primitive w.r.t. $\bar{x}$ (see Theorem 2), and hence $S_{1,2} \in \mathbb{K}[t_1, x_1, x_2] \setminus \mathbb{K}[t_1]$. Similarly, $T_{1,2} \in \mathbb{K}[t_2, x_1, x_2] \setminus \mathbb{K}[t_2]$ and $\deg_{t_2}(T_{1,2}) > 0$. Furthermore, since $\mathcal{P}(\bar{t})$ is in reduced form, $G \in \mathbb{K}[\bar{t}, Z, W, \bar{x}] \setminus \mathbb{K}[\bar{t}, \bar{x}]$. Therefore, $\gcd(S_{1,2}, G) = 1$. Thus, K is not identically zero. Now, it only remains to prove that $\mathrm{Res}_{t_2}(T_{1,2}, K) \neq 0$ or equivalently that the polynomials are coprime. Let us assume that there exists $M \in \mathbb{K}[t_2, Z, W, \bar{x}]$ a non-constant common factor of K and $T_{1,2}$. Since $T_{1,2} \in \mathbb{K}[t_2, x_1, x_2] \setminus \mathbb{K}[t_2]$, $M \in \mathbb{K}[t_2, x_1, x_2] \setminus \mathbb{K}[t_2]$. Let B be a root of M as a univariate polynomial in t_2, then $B \notin \mathbb{K}$. Now, since $S_{1,2} \in \mathbb{K}[t_1, \overline{x}]$, its leading coefficient w.r.t. t_1 cannot vanish when substituting t_2 for B. Therefore, by well-know properties of the resultants (see e.g. Winkler (1996)), since $\deg_{t_1}(G) > 0$ (see Remark 1(4)), there exists A such that $S_{1,2}(A, x_1, x_2) = G(A, B, Z, W, \overline{x}) = 0$. Moreover, note that $(A, B) \notin \mathbb{K}^2$. In particular, this implies that $G_3(A, B, x_3) = q_3(A, B) - x_3 p_3(A, B) = 0$, which implies that $p_3(A, B) = q_3(A, B) = 0$; note that A, B are in the algebraic closure of $\mathbb{K}(x_1, x_2)$ and hence they do not depend on x_3. Now, taking into account that $p_3(\overline{t})$ is not zero (recall that $\mathcal{P}(t)$ is $(1, 2)$-settled) and that $\gcd(p_3, q_3) = 1$, one has that the t_j-coordinates of the intersection points of the polynomials p_3, q_3 are given by $\mathrm{Res}_{t_i}(p_3, q_3) \in \mathbb{K}[t_j]$, $j, i \in \{1, 2\}$, $j \neq i$. So $(A, B) \in \mathbb{K}^2$, which is a contradiction.

In order to prove statement (2), let $M(\overline{x}) = \mathrm{pp}_{x_3}(h(\overline{x}))$, $N(\overline{x}) = \mathrm{Content}_{x_3}(h(\overline{x}))$ and $L(Z, W, \overline{x}) = \mathrm{pp}_{\{Z,W\}}(\mathrm{Res}_{t_2}(T_{1,2}, K))$. Then,

$$\mathrm{Res}_{t_2}(T_{1,2}, K) = M(\overline{x})\, N(\overline{x})\, L(Z, W, \overline{x}).$$

By statement (1), M, N, L are not identically zero. Moreover, F cannot divide L because L is primitive w.r.t. $\{Z, W\}$. Also, F cannot divide N because it does not depend on x_3 and F does depend on this variable since it is not a cylinder over the x_1x_2-plane (see Lemma 9). Therefore, $L(Z, W, \mathcal{P}(\overline{t}))$ and $N(\mathcal{P}(\overline{t}))$ are not identically zero. In this situation, let $\overline{t}^{\,0} = (t_1^0, t_2^0) \in \mathbb{K}^2$ be such that (recall that $G_4 = \mathrm{lcm}(q_1, q_2, q_3)$)

$$G_4(\overline{t}^{\,0}) \neq 0,\ L(Z, W, \mathcal{P}(\overline{t}^{\,0})) \neq 0, \text{ and } N(\mathcal{P}(\overline{t}^{\,0})) \neq 0.$$

Since $G_j(\overline{t}^{\,0}, \mathcal{P}(\overline{t}^{\,0})) = 0$ for $j = 1, 2, 3$, and $S_{1,2}(t_1^0, \mathcal{P}(\overline{t}^{\,0})) = 0$, we deduce that $K(t_2^0, Z, W, \mathcal{P}(\overline{t}^{\,0})) = 0$. Moreover, taking into account that $T_{1,2}(t_2^0, \mathcal{P}(\overline{t}^{\,0})) = 0$ we get that

$$\mathrm{Res}_{t_2}(T_{1,2}(t_2, \mathcal{P}(\overline{t}^{\,0})), K(t_2, Z, W, \mathcal{P}(\overline{t}^{\,0}))) = 0.$$

Thus, by Lemma 4.3.1, p. 96 in Winkler (1996)

$$M(\mathcal{P}(\overline{t}^{\,0}))\, N(\mathcal{P}(\overline{t}^{\,0}))\, L(Z, W, \mathcal{P}(\overline{t}^{\,0})) = 0,$$

which implies that $M(\mathcal{P}(\overline{t}^{\,0})) = 0$. Thus, if $\mathrm{pp}_{x_3}(h(\overline{x}))$ is a constant (i.e. $M(\overline{x})$), it is zero which contradicts statement (1). □

Lemma 14. *Let*

(1) $n_i(t_1) = \mathrm{Res}_{t_2}(p_i(\overline{t}), q_i(\overline{t}))$, $i = 1, 2$,
(2) $\mathcal{N}_i(\overline{x}) = \mathrm{Res}_{t_1}(n_i(t_1), S_{1,2}(t_1, \overline{x}))$, $i = 1, 2$,
(3) *$L_i(x_i)$ be the leading coefficient w.r.t. t_2 of $G_i(\overline{t}, x_i)$, $i = 1, 2$ (note that, by Remark 1, L_i does not depend on t_1), let $A(\overline{x})$ the leading coefficient w.r.t. t_1 of $S_{1,2}(t_1, \overline{x})$,*
(4) *and let $P \in \mathbb{K}^3$ be such that $L_1(P) \cdot L_2(P) \cdot A(P) \neq 0$.*

Then, for each $i \in \{1, 2\}$, $\mathcal{N}_i(P) = 0$ if and only if there exists $(a, b) \in \mathbb{K}^2$ such that $q_i(a, b) = S_{1,2}(a, P) = 0$.

Proof. By Remark 1(1), $p_i \neq 0$, and clearly $q_i \neq 0$. Moreover, $\gcd(p_i, q_i) = 1$. Thus, $n_i(t_1) \neq 0$. Since $\deg_{t_1}(S_{1,2}(t_1, \overline{x})) > 0$ (see Lemma 9 and Corollary 1), and $\gcd(S_{1,2}, n_i) = 1$ (see Theorem 2), $\mathcal{N}_i(\overline{x}) \neq 0$. Now, we prove the lemma for $i = 1$; similarly for $i = 2$. First, we assume that there exists $(a, b) \in \mathbb{K}^2$ such that $q_1(a, b) = 0$ and $S_{1,2}(a, P) = 0$. Let

$$\mathcal{R}(t_1, \overline{x}) = \mathrm{Res}_{t_2}(G_1(\overline{t}, x_1), G_2(\overline{t}, x_2)), \text{ and } n(t_1) = \mathrm{Content}_{\overline{x}}(\mathcal{R}(t_1, \overline{x})).$$

By the definition of $S_{1,2}(t_1, \overline{x})$ (see Theorem 2), we have that

$$\mathcal{R}(t_1, \overline{x}) = S_{1,2}(t_1, \overline{x}) \cdot n(t_1).$$

From $S_{1,2}(a, P) = 0$, we deduce that $\mathcal{R}(a, P) = 0$. Since $L_i(P) \neq 0$, by well-known properties of resultants (see Winkler (1996)), there exists $b \in \mathbb{K}$ such that $G_i(a, b, P) = 0$, for $i = 1, 2$, which implies that $p_1(a, b) = 0$ (note that $q_1(a, b) = 0$). Therefore, $n_1(a) = 0$ and since $S_{1,2}(a, P) = 0$, we conclude that $\mathcal{N}_1(P) = 0$.

Conversely, let $\mathcal{N}_1(P) = 0$. In particular this implies that n_1 is not a constant. Since $A(P) \neq 0$, there exists $a \in \mathbb{K}$ such that $n_1(a) = 0$, and $S_{1,2}(a, P) = 0$. Since n_1 is not a constant, and that $\deg_{t_2}(p_1) > 0$ and $\deg_{t_2}(q_1) > 0$ (see Remark 1(2)), there exists $b \in \mathbb{K}$ such that $q_1(a, b) = p_1(a, b) = 0$. $\square$

Lemma 15. *Let K be as in Theorem 10, $A(\overline{x})$ the leading coefficient w.r.t. t_1 of $S_{1,2}(t_1, \overline{x})$, and $L(\overline{x})$ the leading coefficient of $G_1(\overline{t}, x_1)$ w.r.t. t_2. If $P \in \mathbb{K}^3$ is such that $A(P)L(P) \neq 0$, then $\deg_{t_2}(K(t_2, Z, W, P)) > 0$.*

Proof. First of all, we note that K is not identically zero (see proof of Lemma 13(1)). Furthermore, $\deg_{t_2}(K) > 0$, since $\deg_{t_1}(S_{1,2}) > 0$, and $\deg_{t_1}(G) > 0$ (see Remark 1(4)), and $\gcd(S_{1,2}, G) = 1$ (see proof of Lemma 13). Let us now assume that $A(P) \cdot L(P) \neq 0$ and that $K(t_2, Z, W, P)$ does not depend on t_2. Then, since

$$K(t_2, Z, W, \overline{x}) = \mathrm{Res}_{t_1}(S_{1,2}(t_1, \overline{x}),\ G(\overline{t}, Z, W, \overline{x})),$$

and $A(P) \neq 0$, by Lemma 4.3.1, p. 96 in Winkler (1996), one deduces that

$$\mathcal{N}(Z, W) := \mathrm{Res}_{t_1}(S_{1,2}(t_1, P),\ G(\overline{t}, Z, W, P)) \in \mathbb{K}[Z, W].$$

Now, since $L(P) \neq 0$ and by Remark 1(3) L does not depend on t_1, we have that $\gcd(S_{1,2}(t_1, P), G_1(\overline{t}, P)) = 1$, and hence $\gcd(S_{1,2}(t_1, P), G(\overline{t}, Z, W, P)) = 1$. Thus, $\mathcal{N}(Z, W)$ is not zero. Under these conditions, we consider $r \in \mathbb{K}$ such that $S_{1,2}(r, P) = 0$ (note that $\deg_{t_1}(S_{1,2}(t_1, P)) > 0$). Then, $G(r, t_2, Z, W, P) \in \mathbb{K}[Z, W]$ (otherwise, there would exist s in the algebraic closure of $\mathbb{K}(Z, W)$ such that $G(r, s, Z, W, P) = 0$, and s would be a root of the polynomial $\mathcal{N}(Z, W)$ which is impossible). Therefore, $G(r, t_2, Z, W, P) \in \mathbb{K}[Z, W]$, and hence $G_1(r, t_2, P) \in \mathbb{K}$ which is impossible because $L(P) \neq 0$. $\square$

Now, we are ready to prove the first main implicitization formula.

Proof of the first main formula (Theorem 10). Let $M(\overline{x})$, $N(\overline{x})$ and $L(Z, W, \overline{x})$ be as in the proof of statement (2) in Lemma 13; recall that $M(\overline{x}) = \mathrm{pp}_{x_3}(h(\overline{x}))$. Also, let $M'(\overline{x})$ be the square-free part of M and $\mathcal{V}'$ the algebraic set defined by M' over $\mathbb{K}$. By Lemma 13, M' is not a constant, and hence $\mathcal{V}'$ is a surface. Let us see that $\mathcal{V}' = \mathcal{V}$:

(1) We consider the subset Ω of $\mathbb{K}^2$

$$\Omega = \{\overline{t}^{\,0} \in \mathbb{K}^2 \mid G_4(\overline{t}^{\,0}) \cdot L(Z, W, \mathcal{P}(\overline{t}^{\,0})) \cdot N(\mathcal{P}(\overline{t}^{\,0})) \neq 0\}.$$

Reasoning as in the proof of Lemma 13(2), one sees that $\Omega \neq \emptyset$ and that, for every $\overline{t}^{\,0} \in \Omega$, $M'(\mathcal{P}(\overline{t}^{\,0})) = 0$. Thus $\mathcal{P}(\Omega) \subset \mathcal{V}'$. Taking the closure in the Zariski topology one gets that $\mathcal{V} \subset \mathcal{V}'$.

(2) Let $A(\overline{x})$,$B(\overline{x})$ be the leading coefficient of $S_{1,2}$, $T_{1,2}$ w.r.t. t_1 and t_2 respectively. Also, let $C(\overline{x})$ be the leading coefficient of G_1 w.r.t. t_2; note that by Remark 1(3), C depends only on x_1. Also, observe that, applying that $\mathcal{P}(\overline{t})$ is $(1,2)$-settled, and using Lemma 9 and Corollary 1, one has that $\deg_{t_1}(S_{1,2}) > 0$ and $\deg_{t_2}(T_{1,2}) > 0$. In addition, let $\mathcal{M}$ be as in Lemma 12, and $\mathcal{N}_1, \mathcal{N}_2$ as in Lemma 14. Finally, let $R(t_2, \overline{x})$ and $Q(t_2, Z, \overline{x}) := \sum_{i=0}^{n} a_i(t_2, \overline{x})Z^i$ be the content and the primitive part of $\mathrm{Res}_{t_1}(G_1(\overline{t}, x_1) + ZG_2(\overline{t}, x_2), q_3(\overline{t}))$ w.r.t. Z, respectively (see Lemma 12). We consider the polynomial

$$D^*(\overline{W}, x_1, x_2) = \mathrm{Res}_{t_2}\left(a_0, a_1 + \sum_{i=2}^{n} W_{i-1}a_i\right),$$

where $\overline{W} = (W_1, \ldots, W_{n-1})$ are new variables. D^* is not identically zero, since $\gcd(a_0, \ldots, a_n) = 1$. Let $D(x_1, x_2)$ be the product of all non-zero coefficients of D^* w.r.t. $\overline{W}$. We consider the subset

$$\Omega^* = \left\{P \in \mathcal{V}' \mid A(P) \cdot B(P) \cdot C(P) \cdot \mathcal{N}_1(P) \cdot \mathcal{N}_2(P) \cdot \mathcal{M}(P) \cdot D(P) \neq 0\right\}.$$

Clearly A, B, C, D are not identically zero. By Lemma 12, $\mathcal{M}$ is not zero, and $\mathcal{N}_1, \mathcal{N}_2$ are not zero (see proof of Lemma 14). So $\Omega^* \neq \emptyset$. In addition, let us see that Ω^* is dense in $\mathcal{V}'$. Indeed: let us assume that Ω^* is not dense, then $\mathcal{V}'$ has at least one component which is defined by a factor of $A(\overline{x}) \cdot B(\overline{x}) \cdot C(\overline{x}) \cdot \mathcal{N}_1(\overline{x}) \cdot \mathcal{N}_2(\overline{x}) \cdot \mathcal{M}(\overline{x})$. However, all these polynomials are in $\mathbb{K}[x_1, x_2]$, and therefore it would imply that $M(\overline{x})$ is not primitive w.r.t. x_3 which is a contradiction.
Now, let $P \in \Omega^*$. Since $M(P) = 0$, one has that

$$\mathrm{Res}_{t_2}(T_{1,2}(t_2, x_1, x_2),\ K(t_2, Z, W, \overline{x}))(P) = 0.$$

Moreover, $B(P) \neq 0$. Thus, by Lemma 4.3.1, p. 96 in Winkler (1996),

$$\mathrm{Res}_{t_2}(T_{1,2}(t_2, P),\ K(t_2, Z, W, P)) = 0.$$

Furthermore, since $P \in \Omega^*$, $\deg_{t_2}(T_{1,2}(t_2, P)) > 0$ and, by Lemma 15, we have that $\deg_{t_2}(K(t_2, Z, W, P)) > 0$. Thus, $K(t_2, Z, W, P)$, $T_{1,2}(t_2, P)$, regarded as univariate polynomials in t_2, have a common root, say b. Observe that since the polynomial $T_{1,2}(t_2, P) \in \mathbb{K}[t_2]$, $b \in \mathbb{K}$. Recall that

$$K(b, Z, W, P) = \mathrm{Res}_{t_1}(S_{1,2},\ G)(b, Z, W, P) = 0.$$

Now, since $A(P) \neq 0$ (note that $P \in \Omega^*$), by Lemma 4.3.1, p. 96 in Winkler (1996),

$$\mathrm{Res}_{t_1}(S_{1,2}(t_1, P), G(t_1, b, Z, W, P)) = 0.$$

Now, if $G(t_1, b, Z, W, P)$ is identically zero, since $\deg_{t_1}(S_{1,2}(t_1, P)) > 0$ because $A(P) \neq 0$, it is clear that there exists $a \in \mathbb{K}$ such that $S_{1,2}(a, P) = 0$, and $G_j(a, b, P) = 0$ for $j \in \{1, 2, 3\}$. On the other hand, if $G(t_1, b, Z, W, P)$ is not identically zero, it must depend on t_1 due to the fact that the resultant above vanishes. In this situation, by Theorem 4.3.3, p. 98 in Winkler (1996), there exists $a \in \mathbb{K}$ (note that $\deg_{t_1}(S_{1,2}(t_1, P)) > 0$) such that

$$S_{1,2}(a, P) = 0,\ \ G_j(a, b, P) = 0,\ \ j \in \{1, 2, 3\}.$$

In addition, let us see that $Q(b, Z, P) \neq 0$. Indeed, if $Q(b, Z, P) = 0$ then $a_i(b, P) = 0$ for every i. Hence, $D^*(\overline{W}, P) = 0$, but this is impossible because $D(P) \neq 0$. Now, let us see that $q_3(a,b) \neq 0$. Indeed, if $q_3(a,b) = 0$, since $G_1(a,b,P) = G_2(a,b,P) = 0$, and $Q(b,Z,P) \neq 0$, one has that $R(b,P) = 0$. Hence, since $T_{1,2}(b,P) = 0$, one gets that $\mathcal{M}(P) = 0$ which is impossible because $P \in \Omega^*$. Thus, $q_3(a,b) \neq 0$. In addition, since $P \in \Omega^*$, by Lemma 14, one has that $q_j(a,b) \neq 0$, for $j = 1,2$. Therefore, from $G_j(a,b,P) = 0$ for $j \in \{1,2,3\}$, we get that $P = \mathcal{P}(a,b)$. $\Omega^* \subset \mathcal{V}$. Therefore, taking into account that Ω^* is dense in $\mathcal{V}'$, taking the Zariski closure one has that $\mathcal{V}' \subset \mathcal{V}$.

Hence, we get that $\mathcal{V} = \mathcal{V}'$, and $F = M'$ up to multiplication by constants in $\mathbb{K}^\star$. Thus, since F is irreducible there exists $r \in \mathbb{N}$ such that $M(\overline{x}) = F(\overline{x})^r$. $\square$

Before stating the second main formula, we still need a lemma.

Lemma 16. *Let $h(\overline{x})$ be as in Theorem 11. Then,*

$$\mathrm{pp}_{x_3}(h(\overline{x})) = \mathrm{pp}_{x_3}\left(\prod_{U \in \pi_{1,2}(\mathcal{P})^{-1}(x_1,x_2)} p_3(U(x_1,x_2)) - x_3\, q_3(U(x_1,x_2))\right),$$

where the polynomials on the right size are considered as univariate polynomials in x_3 with coefficients in the algebraic closure of $\mathbb{K}[x_1,x_2]$.

Proof. First we recall that, by the hypotheses of Theorem 11, $S_{1,2}$ and $T_{1,2}$ are square-free. In addition, by Theorem 2(4),

$$\deg_{t_1}(S_{1,2}) = \deg_{t_2}(T_{1,2}) = \mathrm{Card}(\pi_{1,2}(\mathcal{P})^{-1}(x_1,x_2)).$$

Let $d_{1,2}$ be this quantity. By Corollary 1, since $\mathcal{P}(\overline{t})$ is $(1,2)$-settled, $d_{1,2} \geq 1$. In addition, by Remark 1(3) and (4), $\deg_{t_i}(G) > 0$, $i = 1,2$, where G is as in Theorem 10. Let $m = \deg_{t_1}(G)$ and $k = \deg_{t_2}(G)$. Now, let K be as in Theorem 10. Regarding $S_{1,2}$ and G as polynomials in $\mathbb{K}(t_2,Z,W,\overline{x})[t_1]$, and using the expression of the resultant of two univariate polynomials as the product of the evaluations of one of them in the roots of the other, one has that

$$K(t_2,Z,W,\overline{x}) = \mathrm{Res}_{t_1}(S_{1,2},G) = A(\overline{x})^m \prod_{i=1}^{d_{1,2}} G(\alpha_i,t_2,Z,W,\overline{x}),$$

where A is the leading coefficient of $S_{1,2}$ w.r.t. t_1, and $\{\alpha_1,\ldots,\alpha_{d_{1,2}}\}$ are the roots of $S_{1,2}$ (regarded as univariate polynomial in t_1) in the algebraic closure $\overline{\mathbb{K}(x_1,x_2)}$ of $\mathbb{K}(x_1,x_2)$. Since $S_{1,2}$ is square-free, $\alpha_i \neq \alpha_j$ for $i \neq j$. Similarly,

$$\mathrm{Res}_{t_2}(T_{1,2},\ K) = B(\overline{x})^k \prod_{j=1}^{d_{1,2}} K(\beta_j,Z,W,\overline{x}),$$

where now B is the leading coefficient of $T_{1,2}$ w.r.t. t_2, and $\{\beta_1,\ldots,\beta_{d_{1,2}}\}$ are the roots of $T_{1,2}$ (regarded as univariate polynomial in t_2) in $\overline{\mathbb{K}(x_1,x_2)}$. Since $T_{1,2}$ is square-free, $\beta_i \neq \beta_j$ for $i \neq j$. Therefore,

$$\mathrm{Res}_{t_2}(T_{1,2},\ K) = B^k\, A^{m \cdot d_{1,2}} \prod_{i=1}^{d_{1,2}} \prod_{j=1}^{d_{1,2}} G(\alpha_i,\beta_j,Z,W,\overline{x}).$$

By Theorem 2, there exist $d_{1,2}$ pairs of points (α_i,β_j) in $\pi_{1,2}(\mathcal{P})^{-1}(x_1,x_2)$, and for each $U(x_1,x_2) \in \pi_{1,2}(\mathcal{P})^{-1}(x_1,x_2)$, $G_1(U,x_1) = G_2(U,x_2) = 0$. Thus,

$$\mathrm{Res}_{t_2}(T_{1,2},\ K) = B^k\, A^{m\cdot d_{1,2}}\, Q(\overline{x}, Z, W) \prod_{U\in\pi_{1,2}(\mathcal{P})^{-1}(x_1,x_2)} G_3(U, x_3),$$

where

$$Q(\overline{x}, Z, W) = \prod_{\substack{1\le i,j\le d_{1,2}\\ (\alpha_i,\beta_j)\notin\pi_{1,2}(\mathcal{P})^{-1}(x_1,x_2)}} G(\alpha_i, \beta_j, Z, W, \overline{x}).$$

Since $T_{1,2}, S_{1,2}$ are square-free, for each α_i there exists exactly one b_j such that (α_i, β_j) is in the fibre. Moreover, for $(\alpha_i, \beta_j) \notin \pi_{1,2}(\mathcal{P})^{-1}(x_1, x_2)$, because of Theorem 2, either $G_1(\alpha_i, \beta_j, x_1) \neq 0$ or $G_2(\alpha_i, \beta_j, x_2) \neq 0$. Thus, $Q(\overline{x}, Z, W)$ depends on Z or W. Moreover, each factor $G(\alpha_i, \beta_j, Z, W, \overline{x})$ does depend on Z or W. Now, we will prove that $Q(\overline{x}, Z, W)$, regarded as polynomial in $\overline{\mathbb{K}[x_1, x_2]}[x_3, Z, W]$, is primitive w.r.t. $\{Z, W\}$. Indeed, let $N(x_3) \in \overline{\mathbb{K}[x_1, x_2]}[x_3]$ be the content of Q w.r.t. $\{Z, W\}$. Then, there exists $(\alpha_i, \beta_j) \notin \pi_{1,2}(\mathcal{P})^{-1}(x_1, x_2)$ such that N divides $G(\alpha_i, \beta_j, Z, W, \overline{x})$; i.e. it divides $G_3(\alpha_i, \beta_i, x_3) + ZG_1(\alpha_i, \beta_j, x_1) + WG_2(\alpha_i, \beta_j, x_2)$. So, $N(x_3)$ divides $G_1(\alpha_i, \beta_j, x_1)$ and $G_2(\alpha_i, \beta_j, x_2)$. Now, since at least one of them is not zero, $N \in \overline{\mathbb{K}[x_1, x_2]}$. Hence Q is primitive w.r.t. $\{Z, W\}$. In this situation, taking into account that

$$h(\overline{x}) = \mathrm{Content}_{\{Z,W\}}(\mathrm{Res}_{t_2}(T_{1,2}, K)),$$

we get that

$$h(\overline{x}) = B^k A^{m\cdot d_{1,2}} \cdot N(x_1, x_2) \cdot \prod_{U\in\pi_{1,2}(\mathcal{P})^{-1}(x_1,x_2)} G_3(U, x_3),$$

where $N \in \overline{\mathbb{K}[x_1, x_2]}$. Thus,

$$\mathrm{pp}_{x_3}(h(\overline{x})) = \mathrm{pp}_{x_3}\left(\prod_{U\in\pi_{1,2}(\mathcal{P})^{-1}(x_1,x_2)} p_3(U(x_1, x_2)) - x_3 q_3(U(x_1, x_2))\right). \quad \square$$

Remark 7. Note that, if the polynomials $T_{1,2},\ S_{1,2}$ are not square-free, then $\mathrm{pp}_{x_3}(h(\overline{x}))$ is a power of $\mathrm{pp}_{x_3}\left(\prod_{U\in\pi_{1,2}(\mathcal{P})^{-1}(x_1,x_2)} p_3(U(x_1, x_2)) - x_3 q_3(U(x_1, x_2))\right)$.

Now, we are ready to prove the second main implicitization formula.

Proof of the second main formula (Theorem 11). We use the notation introduced in the proof of Lemma 16. By Lemma 16, we have that $\deg_{x_3}(\mathrm{pp}_{x_3}(h(\overline{x}))) = d_{1,2}$. Indeed, clearly one has that $\deg_{x_3}(\mathrm{pp}_{x_3}(h(\overline{x}))) \le d_{1,2}$. If $\deg_{x_3}(\mathrm{pp}_{x_3}(h(\overline{x}))) < d_{1,2}$, then there exists $U \in \pi_{1,2}(\mathcal{P})^{-1}(x_1, x_2)$ such that $q_3(U) = 0$. Moreover, $U \notin \mathbb{K}^2$. But this is impossible; see the last part of the proof of Lemma 12. Now, by Theorem 6, $\deg_{x_3}(F) = \frac{d_{1,2}}{\deg(\mathcal{P})}$, and by Theorem 10, $\mathrm{pp}_{x_3}(h(\overline{x})) = F(\overline{x})^r$. Thus, $r = \deg(\mathcal{P})$. $\square$

Appendix. List of parametrizations

(1) $\mathcal{P}_1(\overline{t}) = \left(\frac{t_2^2}{t_1^2-1}, \frac{(t_1^2-1)^3}{t_2^2}, \frac{-82}{-40+21t_2^2t_1^2-42t_2t_1+21t_2^2-21t_2t_1^2}\right)$

(2) $\mathcal{P}_2(\bar{t}) = \left(\frac{-t_2 t_1^2(t_1^2-2)}{t_1^2-1}, \frac{-(t_1^2-1)^3 t_2}{t_1^2(t_1^2-2)}, \frac{t_2^4}{t_1^2-1}\right)$

(3) $\mathcal{P}_3(\bar{t}) = \left(\frac{t_2^4}{t_1^2-1}, \frac{(t_1^2-1)^3}{t_2^4}, t_1^6(t_1^2+1)^3 + t_2\right)$

(4) $\mathcal{P}_4(\bar{t}) = \left(\frac{t_1^6}{2t_1^4+3t_1^2+2t_1t_2-8t_1+t_2^2-8t_2+19}, (2t_1^2+2t_1t_2-8t_1)^2, t_2^3\right)$

(5) $\mathcal{P}_5(\bar{t}) = \left(\frac{-6+2t_1^3+6t_2^2-10t_1}{-5+4t_2^2+9t_1t_2}, 12-32t_1t_2+3t_1+3t_1^2-6t_2-4t_1^3, t_2t_1^2+1\right)$

(6) $\mathcal{P}_6(\bar{t}) = \left(t_2-(t_1-t_2+3)^3, t_1^2-t_2+4, t_2^3-4t_1^2-5t_1\right)$

(7) $\mathcal{P}_7(\bar{t}) = \left(\frac{7-2t_1t_2^2-4t_1t_2}{1-4t_1^2+2t_1}, \frac{t_1t_2}{t_1t_2+1-3t_1^2}, -54-6t_2t_1^4-4t_1-26t_1^2\right)$

(8) $\mathcal{P}_8(\bar{t}) = \left(t_2^2+\frac{1}{t_1^4-1}, t_1t_2-1+\frac{1}{t_2^2}, \frac{1}{t_1^7}\right)$

(9) $\mathcal{P}_9(\bar{t}) = \left(\frac{t_2^4}{t_1^2-1}, \frac{1}{(t_1^2-1)^2(t_2^4)+2}, t_1^6(t_1^2+1)^3+t_2\right)$

(10) $\mathcal{P}_{10}(\bar{t}) = \left(t_1^6(t_1^2+1)^3, \frac{4t_1}{1+t_2}+\frac{t_1}{t_2}, \frac{1}{t_2^2}\right)$

(11) $\mathcal{P}_{11}(\bar{t}) = \left(\frac{5(t_1^2+1)^3}{t_1^6}, \frac{(t_2t_1+t_1+1)t_1}{4(1+t_2)}, \frac{t_1}{t_2^2}+1\right)$

(12) $\mathcal{P}_{12}(\bar{t}) = \left(\frac{5t_1^2}{t_1^{10}+t_2t_1^3+t_2}, 5t_1^2+t_2+t_1t_2+4, \frac{t_2+t_1}{t_1+5t_2t_1+t_1^5}\right)$.

References

Adams, W.W., Loustaunau, P., 1994. An Introduction to Gröbner Bases. In: Graduate Studies in Mathematics, vol. 3. American Mathematical Society, Providence, RI.

Arrondo, E., Sendra, J., Sendra, J.R., 1997. Parametric generalized offsets to hypersurfaces. Journal of Symbolic Computation 23, 267–285.

Busé, L., 2001. Residual resultant over the projective plane and the implicitization problem. In: Mourrain, B. (Ed.), Proceedings of ISSAC 2001. London, Ontario. AMC Press, New York, pp. 48–55.

Busé, L., Cox, D., D'Andrea, C., 2003. Implicitization of surfaces in $\mathbb{P}^3$ in the presence of base points. Journal of Algebra and Applications 2, 189–214.

Castelnuovo, G., 1939. Sulle superficie di genere zero. Memorie scelte, Zanichelli. 307–334.

Chionh, E.W., Goldman, R.N., 1992a. Degree, multiplicity and inversion formulas for rational surfaces using u-resultants. Computer Aided Geometric Design 9 (2), 93–109.

Chionh, E.W., Goldman, R.N., 1992b. Using multivariate resultants to find the implicit equation of a rational surface. The Visual Computer 8 (3), 171–180.

Cox, D., Goldman, R., Zhang, M., 2000. On the validity of implicitization by moving quadrics for rational surfaces with no base points. Journal of Symbolic Computation 29, 419–440.

Cox, D., Little, J., O'Shea, D., 1997. Ideals, Varieties, and Algorithms, 2nd ed. Springer-Verlag, New York.

Cox, D., Little, J., O'Shea, D., 1998a. Using Algebraic Geometry. Springer-Verlag, New York.

Cox, D.A., Sederberg, T.W., Chen, F., 1998b. The moving line ideal basis of planar rational curves. Computer Aided Geometric Design 8, 803–827.

Cox, D., 2001. Equations of parametric curves and surfaces via syzygies. In: Symbolic Computation: Solving Equations in Algebra, Geometry and Engineering. In: Contemporary Mathematics, vol. 286. AMS, Providence, RI, pp. 1–20.

D'Andrea, C., 2001. Resultants and moving surfaces. Journal of Symbolic Computation 31, 585–602.

González-Vega, L., 1997. Implicitization of parametric curves and surfaces by using multidimensional Newton formulae. Journal of Symbolic Computation 23, 137–152.

Harris, J., 1995. Algebraic Geometry. A first Course. Springer-Verlag.

Kotsireas, I.S., 2004. Panorama of methods for exact implicitization of algebraic curves and surfaces. In: Chen, Falai, Wang, Dongming (Eds.), Geometric Computation. In: Lecture Notes Series on Computing, vol. 11. World Scientific Publishing Co., Singapore (Chapter 4).

Marco, A., Martínez, J.J., 2002. Implicitization of rational surfaces by means of polynomial interpolation. Computer Aided Geometry Design 19, 327–344.

Orecchia, F., 2001. Implicitization of a general union of parametric varieties. Journal of Symbolic Computation 31 (3), 343–356.

Pérez-Díaz, S., Sendra, J.R., Schicho, J., 2002. Properness and inversion of rational parametrizations of surfaces. Applicable Algebra in Engineering, Communication and Computing 13, 29–51.

Pérez-Díaz, S., Sendra, J.R., 2004. Computation of the degree of rational surface parametrizations. Journal of Pure and Applied Algebra 193 (1–3), 99–121.

Pérez-Díaz, S., Sendra, J.R., 2005. Partial degree formulae for rational algebraic surfaces. In: Proc. ISSAC-2005, Beijing, China, pp. 301–308.

Sederberg, T.W., Chen, F., 1995. Implicitization using moving curves and surfaces. In: Proceedings of SIGGRAPH, pp. 301–308.

Sendra, J.R., Winkler, F., 2001a. Computation of the degree of a rational map. In: Proc. ISSAC-2001, Ontario, Canada, pp. 317–322.

Sendra, J.R., Winkler, F., 2001b. Tracing index of rational curve parametrizations. Computer Aided Geometric Design 18 (8), 771–795.

Shafarevich, I.R., 1994. Basic Algebraic Geometry Schemes; 1 Varieties in Projective Space, vol. 1. Springer-Verlag, Berlin, New York.

Winkler, F., 1996. Polynomial Algorithms in Computer Algebra. Springer-Verlag, Wien, New York.