Inversion, Degree, Reparametrization and Implicitization of Improperly Parametrized Planar Curves Using μ-Basis

Sonia Pérez-Díaz[a], Li-Yong Shen[b,c,*]

[a] *Grupo ASYNACS, Dpto. de Física y Matemáticas, Universidad de Alcalá, 28871-Alcalá de Henares, Madrid, Spain*
[b] *School of Mathematical Sciences, University of Chinese Academy of Sciences, 100049, Beijing, China*
[c] *Key Laboratory of Big Data Mining and Knowledge Management, CAS, 100190, Beijing, China*

Abstract

The μ-basis of a rational curve/surface is a new algebraic tool which plays an important role in connecting the rational parametric form and the implicit form of a rational curve/surface. However, most results for μ-bases are presented for proper rational parametrizations. In this paper we consider the μ-basis for an improper rational planar curve. Based on the known properties and new results, we design two new proper reparametrization algorithms using μ-basis. The inversion, degree of the induced rational map and implicitization formulas are also derived.

Keywords: μ-basis; inversion; rational parametrization; algebraic curves; proper reparametrization; implicitization; fibre;

1. Introduction

The μ-basis was first introduced in [7] to provide a compact representation for the implicit equation of a rational parametric curve. The μ-basis can be used not only to recover the parametric equation of a rational curve/surface but also to derive its implicit equation. There are several methods based on Gröbner basis [28] or on vector elimination [4] to compute the μ-basis for rational curves by computing two moving lines which satisfy the required properties [7]. Later, the algorithms for computing μ-bases of univariate polynomials are extended for general rational curves in arbitrary dimensions, even with the coordinate functions having common factors [12, 26]. The μ-basis has also been generalized to rational surfaces [5], although the concept of a μ-basis for surfaces is still in flux and awaits further exploration [15, 21, 22]. Actually the situation for rational surfaces is quite different: the μ-basis is not unique and even the degrees of the μ-basis elements can be different. Currently, the only known algorithm to compute a weak μ-basis of a rational surface is designed based on polynomial matrix factorization [8]. However, for certain rational surfaces with special geometry, the μ-basis can be defined explicitly and there has been a lot of exploration on the μ-bases of such special surfaces: Steiner surfaces, surfaces of revolution, ruled surfaces, cyclides as well as canal surfaces (see [13]). Besides the bridge role between the parametric forms and implicit forms, the μ-basis has additional applications including inversion formulas and singularity computation.

A basic property of a rational parametrization is whether or not it is proper. If a rational parametrization is not proper, also called *improper*, then a generic point of the variety corresponds to more than one parameter. Much of the research about the rational parametrization, including almost all the above works about μ-bases, assume that the parametrization is proper. However, improper parametrizations can be found in theoretical and practical situations. If a rational parametrization is improper, naturally we would ask whether it can be reparameterized so that the new parametrization is proper. For algebraic curves, the

*Corresponding author
Email addresses: sonia.perez@uah.es (Sonia Pérez-Díaz), lyshen@ucas.ac.cn (Li-Yong Shen)

existence of a proper reparametrization for an improper rational parametrization is guaranteed by Lüroth's theorem [27]. Several typical methods to find a proper reparametrization for an improper parametrization of an algebraic curve are proposed in [10, 16, 17]. Among them the algorithm in [16] is best since this algorithm computes the improper rational function with the fewest GCD computations and involves the computation of an easy univariate resultant whereas the other two algorithms [10, 17] solve the problem by means of the method of undetermined coefficients.

The μ-basis as a new algebraic tool has shown different advantages but not in proper reparametrization. In this paper, we attempt to find a proper reparametrization for an improper parametrization of an algebraic curve by using μ-bases. We study the relationships between the μ-basis of a proper parametrization and the μ-basis of its improper parametrization. From the μ-basis of an improper parametrization, we give the degree of the rational map defined by the parametrization, i.e., the improper index of the improper parametrization. An inversion formula is then found for the case where the parametrization is proper. As an important result, we define an associated polynomial by μ-bases and prove that the associated polynomial is a bivariate alternating polynomial. Then the associated polynomial will induce a rational function of the parameter to properly reparameterize the given improper parametrization. After taking a deep look at the μ-basis of the improper parametrization, we derive a way to find a μ-basis for a proper reparametrization by solving linear systems. We also give a simple derivation for the implicitization formula for an improper algebraic curve using μ-bases.

This paper is organized as follows. In Section 2, we recall the definition, properties and an algorithm as well as two new lemmas for the μ-basis of rational curves. In Section 3, for an improper rational parametrization, we study the inversion computation, the degree of the induced rational map, the proper reparametrization and implicitization using μ-bases. Finally, we conclude our paper in Section 4 with a brief summary of our work. For the convenience of readers and for the consistency of concepts, we will introduce some necessary details directly from the references [4, 7, 13, 16].

2. μ-Bases for Rational Planar Curves

The μ-basis of a rational planar curve is defined in [7] as a special basis of the moving line ideal of the rational curve. The moving line ideal corresponding to the rational planar curve $\mathcal{C}$ defined by the rational parametrization $\mathcal{P}(t) = (\wp_1(t), \wp_2(t), \wp_3(t))$, $\gcd(\wp_1(t), \wp_2(t), \wp_3(t)) = 1$ is the ideal $I = \langle \wp_3(t)x_1 - \wp_1(t)x_3, \wp_3(t)x_2 - \wp_2(t)x_3 \rangle \subset \mathbb{K}[x_1, x_2, x_3, t]$ ($\mathbb{K}$ is an algebraically closed field of characteristic zero) that consists of all the moving curves following $\mathcal{P}(t)$. A μ-basis of the rational curve $\mathcal{C}$ defined by $\mathcal{P}(t)$ is a basis of the ideal I with the form:

$$p^{\mathcal{P}}(\overline{x}, t) = p_1(t)x_1 + p_2(t)x_2 + p_3(t)x_3, \quad q^{\mathcal{P}}(\overline{x}, t) = q_1(t)x_1 + q_2(t)x_2 + q_3(t)x_3, \quad \overline{x} = (x_1, x_2, x_3)$$

where $p_i(t)$, $q_i(t)$, $i = 1, 2, 3$, are polynomials in $\mathbb{K}[t]$, and $p^{\mathcal{P}}$ and $q^{\mathcal{P}}$ have the lowest possible degrees in t. Thus a μ-basis is two moving lines that form a basis of the moving line ideal I. Assuming that $\deg_t(p^{\mathcal{P}}) = \mu \leq \deg_t(q^{\mathcal{P}})$ (where $0 \leq \mu \leq [n/2]$ and $n = \deg(\mathcal{P})$), it is proven that $\deg_t(q^{\mathcal{P}}) = n - \mu$, and for any rational planar curve, μ is uniquely determined and such a μ-basis always exists (see [7]).

We recall that $\deg(\mathcal{P})$ is the maximum of the degrees of the components of the rational parametrization $\mathcal{P}(t)$. In general, for any vector $v := (a_1(t), a_2(t), \ldots, a_\ell(t)) \in \mathbb{K}[t]^\ell$, $\deg(v)$ is the maximum of $\deg(a_i)$, for $i = 1, \ldots, \ell$.

For a better understanding of μ-bases, syzygies can be used. A moving line $A(t)x_1 + B(t)x_2 + C(t)x_3 = 0$ corresponds to a three dimensional vector $(A(t), B(t), C(t)) \in \mathbb{K}[t]^3$, and a moving line $A(t)x_1 + B(t)x_2 + C(t)x_3 = 0$ following $\mathcal{P}(t)$ corresponds to a syzygy of $\mathcal{P}(t) = (\wp_1(t), \wp_2(t), \wp_3(t))$. Thus the set

$$M_{\mathcal{P}} := \{(A(t), B(t), C(t)) \in \mathbb{K}[t]^3 \mid \wp_1(t)A(t) + \wp_2(t)B(t) + \wp_3(t)C(t) \equiv 0\}$$

corresponds to all the moving lines following the rational curve $\mathcal{P}(t)$ (see e.g [13]). $M_{\mathcal{P}}$ is a syzygy module over $\mathbb{K}[t]$ which is free of rank two, and a μ-basis for the rational curve $\mathcal{P}(t)$ is just a basis of the syzygy

module $M_{\mathcal{P}}$ with the lowest possible degree (see [7]). More precisely, one has the following formal definition (see e.g. [7]).

Definition 1. *Two moving lines* $p^{\mathcal{P}}(\overline{x},t) = p_1(t)x_1 + p_2(t)x_2 + p_3(t)x_3 = 0$ *and* $q^{\mathcal{P}}(\overline{x},t) = q_1(t)x_1 + q_2(t)x_2 + q_3(t)x_3 = 0$, *or equivalently, two polynomial vectors* $\mathbf{p}(t) = (p_1(t), p_2(t), p_3(t)) \in \mathbb{K}[t]^3$ *and* $\mathbf{q}(t) = (q_1(t), q_2(t), q_3(t)) \in \mathbb{K}[t]^3$ *are a* μ*-basis of the curve defined by* $\mathcal{P}(t)$ *(or the syzygy module* $M_{\mathcal{P}}$*), if*

1. $\mathbf{p}(t)$ *and* $\mathbf{q}(t)$ *are a basis for the syzygy module* $M_{\mathcal{P}}$, *i.e., any moving line* $L(t) \in M_{\mathcal{P}}$ *can be expressed by*
$$L = h_1\mathbf{p} + h_2\mathbf{q} \tag{1}$$
with $h_1, h_2 \in \mathbb{K}[t]$; *and*
2. $\mathbf{p}(t)$ *and* $\mathbf{q}(t)$ *have the lowest degree among all the bases of* $M_{\mathcal{P}}$, *i.e., assuming that* $\deg(\mathbf{p}) \le \deg(\mathbf{q})$, *then there does not exist another basis* $\overline{\mathbf{p}}(t)$ *and* $\overline{\mathbf{q}}(t)$ *of* $M_{\mathcal{P}}$ *with* $\deg(\overline{\mathbf{p}}) \le \deg(\overline{\mathbf{q}})$ *such that* $\deg(\overline{\mathbf{p}}) < \deg(\mathbf{p})$ *or* $\deg(\overline{\mathbf{q}}) < \deg(\mathbf{q})$.

The following properties of μ-bases can easily be derived from the above definitions (see [4]).

Theorem 1. *Let* $\mathbf{p}(t)$, $\mathbf{q}(t)$ *be a* μ*-basis for* $\mathcal{P}(t)$ *with* $\deg(\mathbf{p}) \le \deg(\mathbf{q})$. *Then,*

1. $\mathbf{p}(t)$ *and* $\mathbf{q}(t)$ *are* $\mathbb{K}[t]$*-linearly independent.*
2. $\mathbf{p}(t_0)\mathbf{q}(t_0) \neq 0$ *for any parameter value* t_0.
3. $\mathbf{p}(t_0)$ *and* $\mathbf{q}(t_0)$ *are linearly independent for any parameter value* t_0.
4. $\mathrm{LV}(\mathbf{p})$ *and* $\mathrm{LV}(\mathbf{q})$ *are linearly independent, where* $\mathrm{LV}(\cdot)$ *returns the leading vector of a vector polynomial.*
5. *Expression (1) is unique for any moving line* L *of* $\mathcal{P}(t)$.
6. *Any moving line* L *of* $\mathcal{P}(t)$ *can be expressed in (1) with* $\deg(h_1\mathbf{p}) \le \deg(L)$ *and* $\deg(h_2\mathbf{q}) \le \deg(L)$.
7. $\mathbf{p} \times \mathbf{q} = k\mathcal{P}(t)$ *for some nonzero constant* k.
8. *The moving line ideal* $I = \langle \wp_3 x_1 - \wp_1, \wp_3 x_2 - \wp_2 \rangle = \langle p^{\mathcal{P}}, q^{\mathcal{P}} \rangle$.
9. $\deg(\mathbf{p}) + \deg(\mathbf{q}) = \deg(\mathcal{P})$.
10. *If* $\mathcal{P}(t)$ *is proper, then* $\mathrm{resultant}_t(p^{\mathcal{P}}, q^{\mathcal{P}})$ *is the implicit equation of the curve defined by* $\mathcal{P}(t)$.

Note that property 7 implies that any rational planar curve of degree n is the intersection of two families of lines whose degrees sum to n. On the other hand, by property 10, a μ-basis provides a compact representation for the implicit equation of the rational curve defined by a proper parametrization $\mathcal{P}(t)$. In fact, the Bézout resultant of p and q with respect to t gives the implicit equation of $\mathcal{P}(t)$ expressed as a determinant of size $(n-\mu) \times (n-\mu)$ (see [4]). For the generic case with $\mu = n/2$, the size of the determinant generated by a μ-basis is half of the size of the determinant generated by the classical method. In this regard, a μ-basis serves as a bridge to connect the parametric form and the implicit form of a rational curve. Note that all the above properties hold for improperly parameterized curves, except that the resultant in property 10 gives the implicit equation to some power. In the following section, we will analyze this power (see Theorem 6).

The naive approach to computing a μ-basis for a rational planar curve is by computing two moving lines that satisfy the required properties (see [7]). However, this method is a trial-and-error approach, and generally linear systems of equations of size $\mathcal{O}(n)$ have to be solved whose algorithmic complexity is $\mathcal{O}(n^3)$. Zheng and Sederberg presented an automatic algorithm based on Gröbner basis computation with an algorithmic complexity of $\mathcal{O}(n^2)$ (see [28]). An improved algorithm to compute a μ-basis based on vector elimination is provided by Chen and Wang and is described in [4]. Here, we review the algorithm to compute a μ-basis for rational planar curves presented in [4].

Algorithm 1 (Compute a μ-Basis for a Rational Curve Defined by $\mathcal{P}(t)$)**.**
Input *a rational parametrization* $\mathcal{P}(t) = (\wp_1(t), \wp_2(t), \wp_3(t)) \in \mathbb{K}[t]^3$ *of a plane algebraic curve* $\mathcal{C}$.
Output *a* μ*-basis for* $\mathcal{P}(t)$.
Steps

1. *Set* $\mathbf{u}_1 = (-\wp_2, \wp_1, 0), \mathbf{u}_2 = (-\wp_3, 0, \wp_1), \mathbf{u}_3 = (0, \wp_3, -\wp_2)$. *Set* $\mathbf{m}_i = \mathrm{LV}(\mathbf{u}_i)$ *for* $i = 1, 2, 3$.
2. *Set* $n_i = \deg(\mathbf{u}_i)$, $i = 1, 2, 3$. *Renumber* $\mathbf{u}_i$, $i = 1, 2, 3$, *if necessary, so that* $n_1 \geq n_2 \geq n_3$. *Find real numbers* $\alpha_1, \alpha_2, \alpha_3$ *(at least two of them are non-zeros) such that*

$$\alpha_1 \mathbf{m}_1 + \alpha_2 \mathbf{m}_2 + \alpha_3 \mathbf{m}_3 = \mathbf{0}.$$

If $\alpha_1 \neq 0$, *update* $\mathbf{u}_1$ *by*

$$\mathbf{u}_1 = \alpha_1 \mathbf{u}_1 + \alpha_2 t^{n_1 - n_2} \mathbf{u}_2 + \alpha_3 t^{n_1 - n_3} \mathbf{u}_3$$

and set $\mathbf{m}_1 = \mathrm{LV}(\mathbf{u}_1)$ *and* $n_1 = \deg(\mathbf{u}_1)$. *If* $\alpha_1 = 0$ *(then both* α_2 *and* α_3 *are non-zero), update* $\mathbf{u}_2$ *by*

$$\mathbf{u}_2 := \alpha_2 \mathbf{u}_2 + \alpha_3 t^{n_2 - n_3} \mathbf{u}_3$$

and set $\mathbf{m}_2 = \mathrm{LV}(\mathbf{u}_2)$ *and* $n_2 = \deg(\mathbf{u}_2)$.
3. *If one of* $\mathbf{u}_1, \mathbf{u}_2$ *and* $\mathbf{u}_3$ *is zero, say* $\mathbf{u}_1 = \mathbf{0}$, *then output* $\mathbf{u}_2$ *and* $\mathbf{u}_3$ *and stop; else, go to Step 2.*

Next, we prove two technical lemmas that analyze the behavior of a μ-basis under a change of variables. These results will play an important role in the next section.

Lemma 1. *Let* $\mathbf{p}(t)$, $\mathbf{q}(t)$ *be a* μ*-basis for* $\mathcal{P}(t)$ *with* $\deg(\mathbf{p}) \leq \deg(\mathbf{q})$. *Then,*

1. *if* $\deg(\mathbf{p}) < \deg(\mathbf{q})$, $\mathbf{p}(t)$ *is unique up to a nonzero constant scalar,*
2. *if* $\deg(\mathbf{p}) = \deg(\mathbf{q})$, $\{\mathbf{p}(t), \mathbf{q}(t)\}$ *is unique up to a linear combination.*

Proof. First, let us assume that $\deg(\mathbf{p}) < \deg(\mathbf{q})$, and suppose there exists $\tilde{\mathbf{p}}(t) \neq \mathbf{p}(t)$ that belongs to a μ-basis with $\deg(\tilde{\mathbf{p}}) = \deg(\mathbf{p})$. Then from statement 7 in Theorem 1, $\mathbf{p} \cdot \mathcal{P} = 0$ and $\tilde{\mathbf{p}} \cdot \mathcal{P} = 0$. Hence, we have that $\mathbf{p} \times \tilde{\mathbf{p}} = k(t)\mathcal{P}$, where $k(t) \in \mathbb{K}[t] \setminus \{0\}$. But this cannot happen since $\deg(\tilde{\mathbf{p}}) + \deg(\mathbf{p}) < \deg(\mathcal{P})$.

Now, let us assume that $\deg(\mathbf{p}) = \deg(\mathbf{q}) = \frac{\deg(\mathcal{P}(t))}{2}$, and suppose there exists $\tilde{\mathbf{p}}(t), \tilde{\mathbf{q}}(t)$ another μ-basis different from $\mathbf{p}(t)$, $\mathbf{q}(t)$ but with the same degrees. By the definition of a μ-basis, there exist $\alpha_i(t), \beta_i(t) \in \mathbb{K}[t] \setminus \{0\}, i = 1, 2$ such that $\tilde{\mathbf{p}}(t) = \alpha_1(t)\mathbf{p} + \alpha_2(t)\mathbf{q}, \tilde{\mathbf{q}}(t) = \beta_1(t)\mathbf{p} + \beta_2(t)\mathbf{q}$. According to the properties of a μ-basis, $\deg(\tilde{\mathbf{p}}) + \deg(\mathbf{q}) = \deg(\mathcal{P})$ and $\tilde{\mathbf{p}} \times \mathbf{q} = (\alpha_1(t)\mathbf{p} + \alpha_2(t)\mathbf{q}) \times \mathbf{q} = \alpha_1(t)\mathbf{p} \times \mathbf{q} = \alpha_1(t)\mathcal{P}(t)$. Thus, one deduces that $\alpha_1(t) \in \mathbb{K}$ since $\deg(\tilde{\mathbf{p}} \times \mathbf{q}) \leq \deg(\mathcal{P}(t))$. Similar results apply to the other coefficients. Hence $(\tilde{\mathbf{p}} \quad \tilde{\mathbf{q}})^T = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix} (\mathbf{p} \quad \mathbf{q})^T$ where the coefficient matrix is a nonsingular constant matrix. □

Lemma 2. *Let* $\tilde{\mathbf{p}}(t)$, $\tilde{\mathbf{q}}(t)$ *be a* μ*-basis for a parametrization* $\mathcal{Q}(t)$ *with* $\deg(\tilde{\mathbf{p}}) \leq \deg(\tilde{\mathbf{q}})$. *Let* $R(t) \in \mathbb{K}(t) \setminus \mathbb{K}$. *Then* $\mathbf{p}(t) = \tilde{\mathbf{p}}(R(t))$, $\mathbf{q}(t) = \tilde{\mathbf{q}}(R(t))$ *is a* μ*-basis for the reparametrization* $\mathcal{P}(t) = \mathcal{Q}(R(t))$ *with* $\deg(\mathbf{p}) \leq \deg(\mathbf{q})$.

Proof. First, we note that $\deg(\mathcal{P}) = \deg(R)\deg(\mathcal{Q})$, and similarly $\deg(\mathbf{p}) = \deg(R)\deg(\tilde{\mathbf{p}})$ and $\deg(\mathbf{q}) = \deg(R)\deg(\tilde{\mathbf{q}})$. Thus, it is clear that $\deg(\mathbf{p}) \leq \deg(\mathbf{q})$. In addition, since $\tilde{\mathbf{p}}(t)$, $\tilde{\mathbf{q}}(t)$ is a μ-basis for $\mathcal{Q}(t)$ with $\deg(\tilde{\mathbf{p}}) \leq \deg(\tilde{\mathbf{q}})$, it follows from Theorem 1 that $\tilde{\mathbf{p}} \times \tilde{\mathbf{q}} = k\,\mathcal{Q}$ for some non-zero constant k and $\deg(\tilde{\mathbf{p}}) + \deg(\tilde{\mathbf{q}}) = \deg(\mathcal{Q})$. Therefore, taking into account the first statement in this proof, we easily get that $\mathbf{p} \times \mathbf{q} = k\,\mathcal{P}$ for some non-zero constant k and $\deg(\mathbf{p}) + \deg(\mathbf{q}) = \deg(\mathcal{P})$. Hence, from Theorem 1, we conclude that $\mathbf{p}(t)$, $\mathbf{q}(t)$ is a μ-basis for $\mathcal{P}(t)$. □

Notice that we consider $\mathcal{Q}(R(t))$, with $R(t) = r_1(t)/r_2(t) \in \mathbb{K}(t) \setminus \mathbb{K}$, in homogenous form. Hence, in this paper, $\mathcal{P}(t) = \mathcal{Q}(R(t))$ means $\mathcal{P}(t) = \mathcal{Q}\left(\frac{r_1(t)}{r_2(t)}\right) r_2(t)^{\deg(\mathcal{Q})}$ which is a polynomial vector in homogenous form. Similar, $\mathbf{p}(t) = \tilde{\mathbf{p}}(R(t))$ means $\mathbf{p}(t) = \tilde{\mathbf{p}}\left(\frac{r_1(t)}{r_2(t)}\right) r_2(t)^{\deg(\tilde{\mathbf{p}})}$ and $\mathbf{q}(t) = \tilde{\mathbf{q}}(R(t))$ means $\mathbf{q}(t) = \tilde{\mathbf{q}}\left(\frac{r_1(t)}{r_2(t)}\right) r_2(t)^{\deg(\tilde{\mathbf{q}})}$.

3. Inversion, Degree, Reparametrization and Implicitization

In this section, we deal with four different problems that we solve using μ-bases: the inversion problem, the computation of the degree of the induced rational map, the reparametrization problem and the implicitization problem. More precisely, in Subsection 3.1, we show how μ-bases allow us to compute the inverse of a given proper parametrization $\mathcal{P}(t)$ of an algebraic curve. If $\mathcal{P}(t)$ is not proper, we show how the degree of the rational map induced by $\mathcal{P}(t)$ can be computed as well as the elements of the fibre.

In Subsection 3.2, we present an algorithm (Algorithm 2) that computes a proper parametrization from a given improper one. For this purpose, we use μ-bases and some ideas presented in [16]. Algorithm 2 outputs a proper reparametrization by a μ-basis without caring about the properness of the μ-basis. By Lemma 2, if we can construct a μ-basis, $\tilde{\mathbf{p}}(t)$, $\tilde{\mathbf{q}}(t)$, from the μ-basis, $\mathbf{p}(t) = \tilde{\mathbf{p}}(R(t))$, $\mathbf{q}(t) = \tilde{\mathbf{q}}(R(t))$, of $\mathcal{P}(t) = \mathcal{Q}(R(t))$, then we can recover the proper reparametrization $\mathcal{Q}(t) = \tilde{\mathbf{p}}(t) \times \tilde{\mathbf{q}}(t)$ from the properties of the μ-basis. In Subsection 3.3, we present Algorithm 3 generated from this idea.

Finally, in Subsection 3.4, we show how a μ-basis of an improper parametrization also allows us to compute the implicit equation of a given curve. More precisely, we show that the Bézout resultant of $p^{\mathcal{P}}(t, \overline{x}), q^{\mathcal{P}}(t, \overline{x})$, with respect to t gives the implicit equation of $\mathcal{P}(t)$ to some power. The power is $\deg(R)$, where $\mathcal{P}(t) = \mathcal{Q}(R(t))$ and $\mathcal{Q}(t)$ is a proper parametrization of the given curve.

3.1. Inversion and Degree of the Induced Rational Map

Let $\mathbb{K}$ be an algebraically closed field of characteristic zero. We denote by $f(x_1, x_2) \in \mathbb{K}[x_1, x_2]$ the defining polynomial of a rational affine irreducible curve $\mathcal{C}$, and let

$$\mathcal{P}(t) = \left(\frac{\wp_1(t)}{\wp_3(t)}, \frac{\wp_2(t)}{\wp_3(t)} \right) \in \mathbb{K}(t)^2,$$

be a rational parametrization of $\mathcal{C}$, where $\gcd(\wp_1, \wp_2, \wp_3) = 1$. In general, we write the parametrization as $\mathcal{P}(t) = (\wp_1(t), \wp_2(t), \wp_3(t)) \in \mathbb{K}[t]^3$. Under these conditions, we immediately get the corresponding projective curve defined implicitly by the homogeneous polynomial $f(\overline{x}) \in \mathbb{K}[\overline{x}]$, $\overline{x} = (x_1, x_2, x_3)$.

Besides implicitization, other applications of μ-bases include point inversion and singularity computation. The point inversion problem can be described as follows: given a point Q on a plane, decide whether or not the point is on a rational curve defined parametrically by $\mathcal{P}(t)$. In the affirmative case, compute the corresponding parameter value t. A singular point of the curve is a point where the tangent line is not unique. Singularities are critical points on a curve which help to classify the topology of the curve. Both point inversion and singularity computation are fundamental problems in Geometric Design. In the following discussion, we review efficient algorithms to compute point inversion and singular points of parametric curves by using μ-bases.

First we need to introduce some additional prior concepts. Associated with the parametrization $\mathcal{P}(t)$, we consider the induced rational map $\phi_{\mathcal{P}} : \mathbb{K} \longrightarrow \mathcal{C} \subset \mathbb{K}^2; t \longmapsto \mathcal{P}(t)$. We denote by $\deg(\phi_{\mathcal{P}})$ the degree of the rational map $\phi_{\mathcal{P}}$ (for further details see e.g. [20] pp.143, or [11] pp.80). As an important result, we recall that the birationality of $\phi_{\mathcal{P}}$, i.e. the properness of $\mathcal{P}(t)$, is characterized by $\deg(\phi_{\mathcal{P}}) = 1$ (see [11] and [20]). Also, we recall that the degree of a rational map is the cardinality of the fibre of a generic element (see Theorem 7, pp. 76 in [20]). Intuitively, the degree measures the number of times the parametrization traces the curve when the parameter takes values in $\mathbb{K}$. Finally, we denote by $\mathcal{F}_{\mathcal{P}}(Q)$ the fibre of a point Q on the given curve; that is $\mathcal{F}_{\mathcal{P}}(Q) = \mathcal{P}^{-1}(Q) = \{t \in \mathbb{K} \,|\, \mathcal{P}(t) = Q\}$, where the values are counted with multiplicity (see e.g. [18], [19]).

Given $\mathcal{P}(t)$ a rational parametrization of an algebraic curve $\mathcal{C}$, and $\mathbf{p}(t)$, $\mathbf{q}(t)$ a μ-basis for $\mathcal{P}(t)$ with $\deg(\mathbf{p}) \leq \deg(\mathbf{q})$, we consider the polynomials

$$p^{\mathcal{P}}(t, \overline{x}) = \mathbf{p}(t) \cdot Q \in \mathbb{K}[t, \overline{x}], \quad q^{\mathcal{P}}(t, \overline{x}) = \mathbf{q}(t) \cdot Q \in \mathbb{K}[t, \overline{x}], \quad \overline{x} = (x_1, x_2, x_3)$$

and

$$G^{\mathcal{P}}(t, \overline{x}) = \gcd(p^{\mathcal{P}}(t, \overline{x}), q^{\mathcal{P}}(t, \overline{x})) \in \mathbb{K}[t, \overline{x}],$$

where $Q = (x_1, x_2, x_3)$ is a generic point on the curve.

The computation of $G^{\mathcal{P}}(t, \overline{x})$ for a generic point $Q = (x_1, x_2, x_3)$ can be done in two different ways. First, one may assume that the implicit equation of the curve is known. We use the implicit equation of the curve to carry out the arithmetic over $\mathbb{K}(\mathcal{C})$ (where $\mathbb{K}(\mathcal{C})$ denotes the quotient field of rational functions of the curve $\mathcal{C}$). Note that, since $I(\mathcal{C}) = \langle f \rangle$ (where $I(\mathcal{C})$ denotes the ideal of $\mathcal{C}$), basic arithmetic on $\mathbb{K}[\mathcal{C}]$ can be carried out by computing polynomial remainders. Therefore the quotient field $\mathbb{K}(\mathcal{C})$ is computable. In addition, note that we compute resultants of polynomials in $\mathbb{K}(\mathcal{C})[t]$ that is a UFD, and we also calculate GCDs of univariate polynomials over $\mathbb{K}(\mathcal{C})$, and hence in a Euclidean domain. The second way avoids the requirement on the implicit equation. For this purpose, elements are represented (not uniquely) as functions of polynomials in the variables x_1, x_2, x_3. In order to check zero equality one may use the parametrization. However, this can be too time consuming. One may, for instance, test zero–equality by substituting a random point on the curve. The result of this zero test is correct with probability almost one. In addition, one may also test the correctness of the computation of the inverse by checking it on a randomly chosen point on the curve. Hence we can avoid computing the implicit equation.

Proposition 1. *(see [4] and [7]) The inversion formula of a particular point $Q_0 = (x_0, y_0, z_0)$ on the curve is given by the roots of the polynomial $G^{\mathcal{P}}(t) = \gcd(p^{\mathcal{P}}(t), q^{\mathcal{P}}(t)) \in \mathbb{K}[t]$, where $p^{\mathcal{P}}(t) = \mathbf{p}(t) \cdot Q_0$, $q^{\mathcal{P}}(t) = \mathbf{q}(t) \cdot Q_0$. In particular, if Q is not on the curve, $G^{\mathcal{P}}(t)$ is a nonzero constant polynomial. In addition, if $\mathcal{P}(t)$ is proper, then for a generic point $Q = (x_1, x_2, x_3)$ on the curve, $\deg_t(G^{\mathcal{P}}(t, \overline{x})) = 1$ and solving $G^{\mathcal{P}}(t, \overline{x}) = 0$ w.r.t the variable t, we get the inverse of $\mathcal{P}(t)$.*

Based upon proposition 1, one can decide whether or not a point is on a parametric curve and, in the affirmative case, the multiplicity of the point and the corresponding parameter values (i.e. the set $\mathcal{F}_{\mathcal{P}}(Q)$). Furthermore, we may compute $\deg(\phi_{\mathcal{P}})$ (apply the same reasoning as in [19]; see also [18]).

Proposition 2. *For a particular point $Q_0 = (x_0, y_0, z_0) \in \mathcal{C}$,*

$$\mathcal{F}_{\mathcal{P}}(Q_0) = \mathcal{P}^{-1}(Q_0) = \{t \in \mathbb{K} \mid G^{\mathcal{P}}(t) = Q_0\}.$$

In addition, for a generic point of the form $Q = (\wp_1(s), \wp_2(s), \wp_3(s))$,

$$\deg(\phi_{\mathcal{P}}) = \mathrm{Card}(\mathcal{F}_{\mathcal{P}}(\mathcal{P}(s))) = \deg_t(G^{\mathcal{P}}(t, s)).$$

Remark 1. *If $Q = (\wp_1(s), \wp_2(s), \wp_3(s))$ then,*

$$G^{\mathcal{P}}(t, s) = \gcd(p^{\mathcal{P}}(t, s), q^{\mathcal{P}}(t, s)) \in \mathbb{K}[t, s],$$

where $p^{\mathcal{P}}(t, s) = \mathbf{p}(t) \cdot \mathcal{P}(s)$, $q^{\mathcal{P}}(t, s) = \mathbf{q}(t) \cdot \mathcal{P}(s)$.

When the point Q is not given exactly, the above method fails. In this case, techniques for computing approximate GCD such as [2], [6] and [9], can be applied to compute the approximate inversion formula (see e.g. [23, 24]).

In [3], we show that, given a rational proper parametrization, $\mathcal{P}(t)$, the multiplicity of a given point, Q_0, is the cardinality of the fibre of $\mathcal{P}(t)$ at Q_0. That is, the multiplicity of $Q_0 = \mathcal{P}(s_0)$, $s_0 \in \mathbb{K}$, is given by the cardinality of the set

$$\mathcal{F}_{\mathcal{P}}(\mathcal{P}(s_0)) = \{t \in \mathbb{K} : \mathcal{P}(t) = \mathcal{P}(s_0)\}.$$

Observe that $s_0 \in \mathcal{F}_{\mathcal{P}}(\mathcal{P}(s_0))$ and hence, the cardinality of $\mathcal{F}_{\mathcal{P}}(\mathcal{P}(s_0))$ is greater than or equal to 1. Thus, $\mathcal{P}(s_0)$ is a singular point if and only if the cardinality of $\mathcal{F}_{\mathcal{P}}(\mathcal{P}(s_0))$ is greater than 1. In fact, the multiplicity of $\mathcal{P}(s_0)$ is the cardinality of $\mathcal{F}_{\mathcal{P}}(\mathcal{P}(s_0))$.

Example 1. *Let $\mathcal{C}$ be the rational curve defined by the parametrization*

$$\mathcal{P}(t) = (t^3 - t^2 - 1 - t^4, 2t^3 - 1, t^3 + t^2 + 1 - t) \in \mathbb{K}[t]^3.$$

First, we compute the polynomials

$$p^{\mathcal{P}}(t, \overline{x}) = \mathbf{p}(t) \cdot \overline{x} = (4 + t)x_1 + (-t^2 - 2 - t)x_2 + (3t^2 + 2 + 2t)x_3,$$

$$q^{\mathcal{P}}(t, \overline{x}) = \mathbf{q}(t) \cdot \overline{x} = -43tx_1 + (-13t^2 - 14 + 39t)x_2 + (-14 - 18t - 17t^2)x_3,$$

where the μ-basis is given as

$$\mathbf{p}(t) = (4 + t, -t^2 - 2 - t, 3t^2 + 2 + 2t), \qquad \mathbf{q}(t) = (-43t, -13t^2 - 14 + 39t, -14 - 18t - 17t^2).$$

Now, we determine $G^{\mathcal{P}}(t, \overline{x})$ (see paragraph before Proposition 1). We obtain

$$G^{\mathcal{P}}(t, \overline{x}) = (14x_1x_2 - 13x_2^2 + 36x_2x_3 - 28x_1x_3 - 5x_3^2)t + (13x_1x_2 - 3x_2^2 - 9x_2x_3 + 17x_1x_3 - 2x_3^2).$$

Since $\deg_t(G^{\mathcal{P}}) = 1$, we conclude that $\mathcal{P}$ is proper and the inverse is given as

$$\mathcal{I}(\overline{x}) = \frac{-(13x_1x_2 - 3x_2^2 - 9x_2x_3 + 17x_1x_3 - 2x_3^2)}{14x_1x_2 - 13x_2^2 + 36x_2x_3 - 28x_1x_3 - 5x_3^2} \in \mathbb{K}[\overline{x}].$$

3.2. Proper Reparametrization

We aim to compute a proper reparametrization for an improper algebraic curve using a μ-basis. This problem has been solved using alternative techniques such as resultants, Gröbner bases, numerical methods (see e.g. [16], [17], [23]), but the method presented in this paper is a new contribution and very novel.

In the following algorithm, we compute a rational proper reparametrization of an improperly parametrized algebraic plane curve. First we outline this approach, then we illustrate it with an example, and finally we provide a proof of correctness after the example.

Algorithm 2 (Proper Reparametrization for Curves using μ-Basis)**.**
Input *a rational parametrization $\mathcal{P}(t) = (\wp_1(t), \wp_2(t), \wp_3(t))$ of a plane algebraic curve $\mathcal{C}$.*
Output *a rational proper parametrization $\mathcal{Q}(t)$ of $\mathcal{C}$, and a rational function $R(t)$ such that $\mathcal{P}(t) = \mathcal{Q}(R(t))$.*
Steps

1. *Compute a μ-basis of $\mathcal{P}$. Let $\mathbf{p}(t)$, $\mathbf{q}(t)$ be this μ-basis.*
2. *Compute $p^{\mathcal{P}}(t, s) = \mathbf{p}(t) \cdot \mathcal{P}(s)$, $\quad q^{\mathcal{P}}(t, s) = \mathbf{q}(t) \cdot \mathcal{P}(s)$.*
3. *Determine the polynomial $G^{\mathcal{P}}(t, s) = \gcd(p^{\mathcal{P}}(t, s), q^{\mathcal{P}}(t, s)) = C_m(t)s^m + \cdots + C_0(t)$. Let $m := \deg_t(G^{\mathcal{P}}(t, s))$.*
4. *If $m = 1$, then return $\mathcal{Q}(t) = \mathcal{P}(t)$, and $R(t) = t$. Otherwise go to Step 5.*
5. *Consider a rational function $R(t) = \frac{C_i(t)}{C_j(t)} \in \mathbb{K}(t)$, such that $C_j(t)$, $C_i(t)$ are not associated polynomials (i.e. $C_j(t) \neq kC_i(t)$, $k \in \mathbb{K}$).*
6. *For $i = 1, 2$, determine the polynomials*

$$L_i(s, x_i) = \text{resultant}_t(x_i\wp_3(t) - \wp_i(t), sC_j(t) - C_i(t)) = (\tau_{i2}(s)x_i - \tau_{i1}(s))^{\deg(R)}.$$

7. *Return $\mathcal{Q}(t) = (\tau_{11}(t)/\tau_{12}(t), \tau_{21}(t)/\tau_{22}(t))$, and $R(t) = C_i(t)/C_j(t)$.*

We shall prove below that the validity of this algorithm follows directly from Theorem 2 in Step 3, Theorem 3 in Step 5, and Theorems 4 and 5 in Step 6. Step 4 is derived from previous results (see [17] or [19]). In the following example, we illustrate Algorithm 2 with an example.

Example 2. *Let $\mathcal{C}$ be the rational curve defined by the parametrization*

$$\mathcal{P}(t) = (3t^4 + 3t^2 + 1 - t^7 - 2t^5 - t^3 - t^9 - t^8,$$

$$-(t^3 - t^2 - 1)(t^6 + 2t^5 + 2t^4 + 2t^3 + 4t^2 + 2), t^6 + 6t^4 + 6t^2 + 2 + t^7 + 2t^5 + t^3 + t^9 - t^8).$$

In Step 2 of the algorithm, we compute the polynomials

$$p^{\mathcal{P}}(t,s) = (2\,s^6 - 8\,s^5 - 11\,s^4 - 8\,s^3 - 22\,s^2 - 11)(-t+s)(s^2t^2 + s^2 + ts + t^2),$$

$$q^{\mathcal{P}}(t,s) = (-t+s)(s^2t^2 + s^2 + ts + t^2)(86\,s^6t^3 + 35\,s^6t^2 + 89\,s^5t^3 + 20\,s^6t + 293\,s^5t^2 - 40\,s^4t^3 + 63\,s^6 - 80\,s^5t + 457\,s^4t^2 + 89\,s^3t^3 + 181\,s^5 - 110\,s^4t + 293\,s^3t^2 - 80\,s^2t^3 + 303\,s^4 - 80\,s^3t + 914\,s^2t^2 + 181\,s^3 - 220\,s^2t - 40\,t^3 + 606\,s^2 + 457\,t^2 - 110\,t + 303),$$

where the μ-basis is

$$\mathbf{p}(t) = \begin{pmatrix} -7\,t^3 + 16\,t^2 + 16 \\ 8\,t^3 - 13\,t^2 - 13 \\ t^3 + 5\,t^2 + 5 \end{pmatrix}^T$$

$$\mathbf{q}(t) = \begin{pmatrix} 132\,t^6 + 349\,t^5 - 656\,t^4 + 411\,t^3 - 948\,t^2 + 160\,t - 362 \\ -89\,t^6 - 419\,t^5 + 502\,t^4 - 437\,t^3 + 662\,t^2 - 130\,t + 240 \\ 43\,t^6 + 16\,t^5 - 119\,t^4 + 80\,t^3 - 188\,t^2 + 50\,t - 59 \end{pmatrix}^T.$$

Now we determine $G^{\mathcal{P}}(t,s)$,

$$G^{\mathcal{P}}(t,s) = C_0(t) + C_1(t)s + C_2(t)s^2 + C_3(t)s^3,$$

where $C_0(t) = -t^3$, $C_1(t) = 0$, $C_2(t) = -t^3$, and $C_3(t) = (t^2+1)$.

Since $m := \deg_t(G^{\mathcal{P}}) > 1$, we go to Step 5 of Algorithm 2, and we consider

$$R(t) = \frac{C_3(t)}{C_0(t)} = \frac{-1-t^2}{t^3}.$$

Note that $\gcd(C_0, C_3) = 1$. Now we determine the polynomials

$$L_1(s,x_1) = \text{resultant}_t(x_1\wp_3(t) - \wp_1(t), sC_0(t) - C_3(t)) = (-1 + s - s^2 - s^3 - x_1 - sx_1 - s^2x_1 + 2s^3x_1)^3,$$

$$L_2(s,x_2) = \text{resultant}_t(x_2\wp_3(t) - \wp_2(t), sC_0(t) - C_3(t)) = (-1 + s - 2s^3 - x_2 - sx_2 - s^2x_2 + 2s^3x_2)^3.$$

Finally, in Step 7, Algorithm 2 outputs the proper parametrization $\mathcal{Q}(t)$, and the rational function $R(t)$

$$\mathcal{Q}(t) = \left(1 - t + t^2 + t^3, 1 - t + 2t^3, -1 - t - t^2 + 2t^3\right), \qquad R(t) = \frac{-1-t^2}{t^3}.$$

Before we can provide the theorems that establish the validity of Algorithm 2, we first introduce two technical lemmas, Lemma 3 and Lemma 4, that can be found in [14] and [16].

Lemma 3. *Let $P, Q \in (\mathbb{K}[s])[t] \setminus \mathbb{K}$ be polynomials over $\mathbb{K}[s]$ with $\deg_t(P) = m$, and $\deg_t(Q) = n$. Let $R(t) = M(t)/N(t) \in \mathbb{K}(t)$ be a non–constant rational function in reduced form, such that $\deg_t(M - \beta N) = \deg_t(R)$ for every root β for the unknown t of the polynomial $P(t,s)Q(t,s)$. Let $P'(t,s) = P(R(t),s)N(t)^m$, and $Q'(t,s) = Q(R(t),s)N(t)^n$. If a, b are the leading coefficient of Q' and Q w.r.t the variable t, then*

$$\text{resultant}_t(P', Q') = \frac{a^{m(\deg(R)-\deg(N))}}{b^{\deg(R)m}} \cdot \text{resultant}_t(P,Q)^{\deg(R)} \cdot \text{resultant}_t(Q', N)^m.$$

Remark 2. *Observe that if the polynomial $P(t,s)Q(t,s)$ does not have factors in $\mathbb{K}[t]$, then every root β for the unknown t of the polynomials $P(t,s)Q(t,s)$ is in the algebraic closure of $\mathbb{K}(s)$ which implies that* $\deg_t(M-\beta N)=\deg_t(R)$.

Lemma 4. *Let $P,Q\in\mathbb{K}[t,s]\setminus\mathbb{K}$ be polynomials such that* $\gcd(P,Q)=1$, *and let $R(s)=M(s)/N(s)\in\mathbb{K}(s)$ be a non–constant rational function in reduced form such that* $\deg_s(M-\beta N)=\deg_s(R)$ *for every root β for the unknown s of the polynomial $P(t,s)Q(t,s)$. Let $P^\star(t,s)=P(t,R(s))N(s)^r$, and $Q^\star(t,s)=Q(t,R(s))N(s)^l$, where $r:=\deg_s(P)$, and $l:=\deg_s(Q)$. Then* $\gcd(P^\star,Q^\star)=1$.

By Lüroth's Theorem, there exists a rational proper parametrization

$$\mathcal{U}(t)=\left(\frac{u_1(t)}{u_3(t)},\frac{u_2(t)}{u_3(t)}\right)\in\mathbb{K}(t)^2$$

of $\mathcal{C}$, $\gcd(u_1,u_2,u_3)=1$ such that $\mathcal{P}(t)=\mathcal{U}(B(t))$, where $B(t)=M(t)/N(t)\in\mathbb{K}(t)\setminus\mathbb{K}$, and $\gcd(M,N)=1$.

In Lemma 5, we shall show a relation between the polynomials $G^{\mathcal{U}}(t,s)=\gcd(p^{\mathcal{U}},q^{\mathcal{U}})$, $G^{\mathcal{P}}(t,s)=\gcd(p^{\mathcal{P}},q^{\mathcal{P}})$ and the rational function $B(t)$. Recall that $p^{\mathcal{U}}(t,s)=\tilde{\mathbf{p}}(t)\cdot\mathcal{U}(s)$, $q^{\mathcal{U}}(t,s)=\tilde{\mathbf{q}}(t)\cdot\mathcal{U}(s)$, and $\tilde{\mathbf{p}}(t)$, $\tilde{\mathbf{q}}(t)$ is a μ-basis for $\mathcal{U}(t)$ with $\deg(\tilde{\mathbf{p}})\le\deg(\tilde{\mathbf{q}})$. Observe that since $\mathcal{U}$ is a proper parametrization, $G^{\mathcal{U}}(t,s)=t-s$ (see [17], [18] or [19]). Furthermore, $p^{\mathcal{P}}(t,s)=\mathbf{p}(t)\cdot\mathcal{P}(s)$, $q^{\mathcal{P}}(t,s)=\mathbf{q}(t)\cdot\mathcal{P}(s)$, where $\mathbf{p}=\tilde{\mathbf{p}}(B(t))N(t)^{\deg(\tilde{\mathbf{p}})},\mathbf{q}=\tilde{\mathbf{q}}(B(t))N(t)^{\deg(\tilde{\mathbf{q}})}$ is a μ-basis for $\mathcal{P}(t)$ with $\deg(\mathbf{p})\le\deg(\mathbf{q})$ (see Lemma 2).

Denote by $m_1=\deg_t(p^{\mathcal{U}})$, $m_2=\deg_t(q^{\mathcal{U}})$ (note that $m_j\ge1$). From $\mathcal{P}(t)=\mathcal{U}(B(t))$ and using Lemma 2, we deduce that

$$p^{\mathcal{P}}(t,s)=p^{\mathcal{U}}(B(t),B(s))N(t)^{m_1}N(s)^{m_1},\quad q^{\mathcal{P}}(t,s)=q^{\mathcal{U}}(B(t),B(s))N(t)^{m_2}N(s)^{m_2}.$$

Then,

$$G^{\mathcal{P}}(t,s)=\gcd(p^{\mathcal{P}}(t,s),\,q^{\mathcal{P}}(t,s))=\gcd(p^{\mathcal{U}}(B(t),B(s))N(t)^{m_1}N(s)^{m_1},\;q^{\mathcal{U}}(B(t),B(s))N(t)^{m_2}N(s)^{m_2}).\tag{2}$$

On the other hand, since $G^{\mathcal{U}}(t,s)=\gcd(p^{\mathcal{U}}(t,s),\;q^{\mathcal{U}}(t,s))$, we can write that

$$p^{\mathcal{U}}(t,s)=G^{\mathcal{U}}(t,s)A_1^{\mathcal{U}}(t,s),\quad q^{\mathcal{U}}(t,s)=G^{\mathcal{U}}(t,s)A_2^{\mathcal{U}}(t,s),$$

where $A_j^{\mathcal{U}}\in\mathbb{K}[t,s]$, $j=1,2$ and $\gcd(A_1^{\mathcal{U}},\,A_2^{\mathcal{U}})=1$.

Lemma 5. $G^{\mathcal{P}}(t,s)=(N(s)M(t)-M(s)N(t))\cdot$

$$\gcd(A_1^{\mathcal{U}}(B(t),B(s))N(t)^{m_1-1}N(s)^{m_1-1},A_2^{\mathcal{U}}(B(t),B(s))N(t)^{m_2-1}N(s)^{m_2-1}).$$

Proof. First, we observe that since $\mathcal{U}$ is a proper parametrization, $\deg_t(G^{\mathcal{U}})=1$ which implies that $\deg_t(A_j^{\mathcal{U}})=m_j-1$ (note that $m_j\ge1$). Moreover, the polynomials $A_j^{\mathcal{U}}$ do not have factors in $\mathbb{K}[t]$ or in $\mathbb{K}[s]$. Indeed, let us assume that $K(t)\in\mathbb{K}[t]$ is a factor of the polynomial $A_j^{\mathcal{U}}$. Then $K(t)$ is a factor of the polynomials $p^{\mathcal{U}}$, $q^{\mathcal{U}}$ which is impossible since $\tilde{\mathbf{p}}$ and $\tilde{\mathbf{q}}$ are $\mathbb{K}[t]$-linearly independent. Similarly we reason there is no factor in $\mathbb{K}[s]$ since $\gcd(u_1(s),u_3(s))=\gcd(u_2(s),u_3(s))=1$.

Under these conditions, and taking into account that up to constants in $\mathbb{K}^\star:=\mathbb{K}\setminus\{0\}$, $G^{\mathcal{U}}(t,s)=t-s$, we get

$$p^{\mathcal{U}}(B(t),B(s))N(t)^{m_1}N(s)^{m_1}=G^{\mathcal{U}}(B(t),B(s))\cdot A_1^{\mathcal{U}}(B(t),B(s))\cdot N(t)^{m_1}N(s)^{m_1}=$$
$$(N(s)M(t)-M(s)N(t))\cdot A_1^{\mathcal{U}}(B(t),B(s))\cdot N(t)^{m_1-1}N(s)^{m_1-1}.$$

Similarly,

$$q^{\mathcal{U}}(B(t),B(s))N(t)^{m_2}N(s)^{m_2}=G^{\mathcal{U}}(B(t),B(s))\cdot A_2^{\mathcal{U}}(B(t),B(s))\cdot N(t)^{m_2}N(s)^{m_2}=$$

$$(N(s)M(t) - M(s)N(t)) \cdot A_2^{\mathcal{U}}(B(t), B(s)) \cdot N(t)^{m_2-1}N(s)^{m_2-1}.$$

Therefore, from (2), we deduce that $G^{\mathcal{P}}(t,s) = (N(s)M(t) - M(s)N(t))\cdot$

$$\gcd(A_1^{\mathcal{U}}(B(t), B(s))N(t)^{m_1-1}N(s)^{m_1-1}, A_2^{\mathcal{U}}(B(t), B(s))N(t)^{m_2-1}N(s)^{m_2-1}).$$

□

Let $\mathbb{K}^\star := \mathbb{K} \setminus \{0\}$. We have the following lemma.

Lemma 6. *Up to constants in* $\mathbb{K}^\star$,

$$\gcd(A_1^{\mathcal{U}}(B(t), B(s))N(t)^{m_1-1}N(s)^{m_1-1}, A_2^{\mathcal{U}}(B(t), B(s))N(t)^{m_2-1}N(s)^{m_2-1}) = 1.$$

Proof. The statement of this lemma is equivalent to proving that $\mathcal{R}(s) \neq 0$, where

$$\mathcal{R}(s) := \text{resultant}_t(A_1^{\mathcal{U}}(B(t), B(s))N(t)^{m_1-1}N(s)^{m_1-1},\ A_2^{\mathcal{U}}(B(t), B(s))N(t)^{m_2-1}N(s)^{m_2-1}).$$

For this purpose, first note that if $m_j = 1$ for some j, then $A_j^{\mathcal{U}} \in \mathbb{K}^\star$, so the above statement follows trivially. Let us assume that $m_j \geq 2$, which implies that $\deg_t(A_j^{\mathcal{U}}) = m_j - 1 \geq 1$. Under these conditions, we apply Lemma 3 to

$$P(t,s) := A_1^{\mathcal{U}}(t, B(s))N(s)^{m_1-1},\ \ Q(t,s) := A_2^{\mathcal{U}}(t, B(s))N(s)^{m_2-1},\ \text{and}\ \ R(t) = B(t).$$

We observe that since the polynomials $A_j^{\mathcal{U}}(t,s)$ do not have factors in $\mathbb{K}[t]$, then $A_j^{\mathcal{U}}(t, B(s))N(s)^{m_j-1}$ do not have factors in $\mathbb{K}[t]$, which implies that $\deg_t(M - \beta N) = \deg_t(B)$ for every root β for the unknown t of $P \cdot Q$ (see Remark 2). Hence, from Lemma 3, we deduce that

$$\mathcal{R}(s) = \lambda \cdot \text{resultant}_t(P,Q)^{\deg(B)} \cdot \text{resultant}_t(A_2^{\mathcal{U}}(B(t), B(s))N(t)^{m_2-1}N(s)^{m_2-1},\ N(t))^{(m_1-1)},$$

where $\lambda := \frac{a^{(m_1-1)(\deg(B)-\deg(N))}}{b^{(m_1-1)\deg(B)}} \neq 0$, and a and b are the leading coefficients of $A_2^{\mathcal{U}}(B(t), B(s))N(t)^{m_2-1}N(s)^{m_2-1}$ and $Q(t,s)$ w.r.t the variable t. Under these conditions, we first observe that $\text{resultant}_t(P,Q) \neq 0$, since $\gcd(A_1^{\mathcal{U}}(t,s), A_2^{\mathcal{U}}(t,s)) = 1$, which implies that $\gcd(P,Q) = 1$ (see Lemma 4). Furthermore, we also have that

$$\text{resultant}_t(A_2^{\mathcal{U}}(B(t), B(s))N(t)^{m_2-1}N(s)^{m_2-1},\ N(t)) \neq 0.$$

Indeed, let $A_2^{\mathcal{U}}(t,s) := a_{m_2-1}(s)t^{m_2-1} + \cdots + a_0(s)$. Then,

$$A_2^{\mathcal{U}}(B(t), B(s))N(t)^{m_2-1}N(s)^{m_2-1} = a'_{m_2-1}(s)M(t)^{m_2-1} + \cdots + a'_0(s)N(t)^{m_2-1}.$$

Taking into account that $\gcd(M,N) = 1$, we deduce that $\gcd(A_2^{\mathcal{U}}(B(t), B(s))N(t)^{m_2-1}N(s)^{m_2-1},\ N(t)) = 1$. Therefore, we derive that $\mathcal{R}(s) \neq 0$. □

By Lemmas 5 and 6, we can conclude the following theorem.

Theorem 2. *Up to constants in* $\mathbb{K}^\star$, $G^{\mathcal{P}}(t,s) = N(s)M(t) - M(s)N(t)$.

In the following results, we express the polynomials N, M defining the rational function $B(t) = M(t)/N(t)$ as $M(t) = a_m t^m + \cdots + a_0$, $N(t) = b_m t^m + \cdots + b_0$, where $a_i, b_i \in \mathbb{K}$ and $a_m \neq 0$ or $b_m \neq 0$. By Theorem 2, we deduce that, up to constants in $\mathbb{K}^\star$,

$$G^{\mathcal{P}}(t,s) = C_m(t)s^m + C_{m-1}(t)s^{m-1} + \cdots + C_0(t),$$

where $C_j(t) = a_j N(t) - b_j M(t)$, for $j = 0, \ldots, m$. Under these conditions, we have the following theorem which is proved in [16].

Theorem 3. *The following statements are equivalent:* 1.) $a_jb_i \neq a_ib_j$. 2.) $\gcd(C_j, C_i) = 1$. 3.) $C_j(t)$, $C_i(t)$ *are not associated polynomials (i.e.* $C_j(t) \neq kC_i(t)$, $k \in \mathbb{K}$*). Moreover, if* $\gcd(M, N) = 1$*, there exist* $a_j, b_j, a_i, b_i \in \mathbb{K}$ *such that* $a_jb_i \neq a_ib_j$.

Let $H(t,s) = D_m(t)s^m + D_{m-1}(t)s^{m-1} + \cdots + D_0(t) \in (\mathbb{K}[t])[s]$ (we think of $H(t,s)$ as a polynomial in the variable s with coefficients in $\mathbb{K}[t]$) be such that there exist $i, j \in \{0, \ldots, m\}$ with $\gcd(D_i, D_j) = 1$, and $D_i \in \mathbb{K}[t] \setminus \mathbb{K}$ or $D_j \in \mathbb{K}[t] \setminus \mathbb{K}$. Then by Theorem 3, we may write $H(t,s) = M(t)N(s) - M(s)N(t)$ ($M(t), N(t) \in \mathbb{K}[t]$ are not both constant and $\gcd(M,N) = 1$) if and only if $D_i(t)D_j(s) - D_i(s)D_j(t) = c\,H(t,s)$, with $c \in \mathbb{K}^\star$.

Taking into account these results, we consider the rational function

$$R(t) = \frac{C_i(t)}{C_j(t)} = \frac{a_iN(t) - b_iM(t)}{a_jN(t) - b_jM(t)} \in \mathbb{K}(t) \setminus \mathbb{K}, \quad i \neq j,$$

where $a_ib_j \neq a_jb_i$, and C_i, C_j are coefficients of the polynomial $G^{\mathcal{P}}(t,s) = C_m(t)s^m + C_{m-1}(t)s^{m-1} + \cdots + C_0(t)$. Under these conditions, we have the following theorem.

Theorem 4. *There exists a proper parametrization* $\mathcal{Q}(t)$ *of the curve* $\mathcal{C}$ *satisfying* $\mathcal{P}(t) = \mathcal{Q}(R(t))$.

Proof. First, note that we may express $R(t) = g(B(t))$, where $g(t) = (b_it - a_i)/(b_jt - a_j)$. Since $a_jb_i \neq a_ib_j$ (see Theorem 3), we get that $g(t)$ is invertible. Then we consider $\mathcal{Q} = \mathcal{U}(g^{-1})$, and we prove that $\mathcal{Q}$ is a proper parametrization of $\mathcal{C}$. Indeed:

$$\mathcal{Q}(R(t)) = \mathcal{U}(g^{-1}(t)) \circ R(t) = \mathcal{U}(g^{-1}(t)) \circ g(B(t)) = \mathcal{U}(B(t)) = \mathcal{P}(t),$$

so $\mathcal{Q}$ parametrizes $\mathcal{C}$. In addition, since $\mathcal{U}$ and g are invertible, we get that $\mathcal{Q} = \mathcal{U}(g^{-1})$ is proper. □

Once the rational function $R(t) = r_1(t)/r_2(t)$, with $\gcd(r_1, r_2) = 1$, is computed, one has to determine the proper rational parametrization $\mathcal{Q}(t) \in \mathbb{K}(t)^2$ of the curve $\mathcal{C}$, satisfying $\mathcal{P} = \mathcal{Q}(R)$ (note that $\mathcal{Q}$ exists by Theorem 4). For this purpose, one may use the method of undetermined coefficients as in [10] or [17], or the following theorem where we establish an alternative method based on univariate resultants that provides running times more satisfactory than the known algorithms (see [16]).

Theorem 5. *For* $i = 1, 2$*, let* $L_i(s, x_i) = \text{resultant}_t(x_i\wp_3(t) - \wp_i(t), sr_2(t) - r_1(t))$*. Then, up to constants in* $\mathbb{K}^\star$*,* $L_i(s, x_i) = (\tau_{i2}(s)x_i - \tau_{i1}(s))^{\deg(R)}$*, and* $\mathcal{Q}(s) = (\tau_{11}(s)/\tau_{12}(s),\ \tau_{21}(s)/\tau_{22}(s))$ *is the proper parametrization, in reduced form, given by Theorem 4.*

3.3. Alternative Proper Reparametrization

In Algorithm 2, we compute a proper reparametrization using a μ-basis without caring about the properness of the μ-basis. Using the fact that $\mathbf{p}(t) = \tilde{\mathbf{p}}(R(t))$, $\mathbf{q}(t) = \tilde{\mathbf{q}}(R(t))$, where $\mathcal{P}(t) = \mathcal{Q}(R(t))$ (see Lemma 2), in the following discussion we show that we can recover the μ-basis $\tilde{\mathbf{p}}$, $\tilde{\mathbf{q}}$, and compute the proper reparametrization $\mathcal{Q}(t) = \tilde{\mathbf{p}}(t) \times \tilde{\mathbf{q}}(t)$ from the properties of μ-bases.

We observe that in this case, using $\tilde{\mathbf{p}}$, $\tilde{\mathbf{q}}$, we can get the implicit equation of the given curve as $\text{resultant}_t(p^{\mathcal{Q}}(t, \overline{x}), q^{\mathcal{Q}}(t, \overline{x})) = 0$ (see property 10 of Theorem 1).

We start with the following technical lemma.

Lemma 7. *Let* $\mathbf{p}(t)$, $\mathbf{q}(t), \deg(\mathbf{p}) \leq \deg(\mathbf{q})$ *be a* μ*-basis for* $\mathcal{P}(t) = \mathcal{Q}(R(t))$*, where* $R(t) \in \mathbb{K}(t) \setminus \mathbb{K}$*, and let* $\tilde{\mathbf{p}}(t), \tilde{\mathbf{q}}(t), \deg(\tilde{\mathbf{p}}) \leq \deg(\tilde{\mathbf{q}})$ *be a* μ*-basis for* $\mathcal{Q}(t)$*. Then,*

1. *if* $0 < \deg(\mathbf{p}) < \deg(\mathbf{q})$*, then* $\mathbf{p}(t) = k\tilde{\mathbf{p}}(R(t))$ *where* k *is a nonzero constant.*

2. *if* $0 < \deg(\mathbf{p}) = \deg(\mathbf{q})$, *then* $(\mathbf{p} \quad \mathbf{q})^T = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix} (\tilde{\mathbf{p}}(R(t)) \quad \tilde{\mathbf{q}}(R(t)))^T$, *where* $\begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix}$ *is a nonsingular constant matrix.*

Proof. These statements can be derived from Lemma 1. □

Remark 3. 1. *For the degenerate case where* $\deg(\mathbf{p}) = 0$, *i.e.* $\mathbf{p} = (k_1, k_2, k_3)$ *is a nonzero constant vector, the parametrization* $\mathcal{P}(t)$ *defines a line* $k_1x_1 + k_2x_2 + k_3x_3 = 0$. *Thus one can always easily write a proper parametrization. Hence we shall assume* $\deg(\mathbf{p}) > 0$.

2. *To simplify our notation, we write* $\mathbf{p}_1 = \mathbf{p}_2$ *instead of* $\mathbf{p}_1 = k\mathbf{p}_2$ *if* k *is a nonzero constant, since we consider these functions in homogenous form.*

3. *Since* $\begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix} (\tilde{\mathbf{p}} \quad \tilde{\mathbf{q}})^T$ *is still a mu-basis for* $\mathcal{Q}$, *statement 2 can be written as: there exists a* μ*-basis* $\tilde{\mathbf{p}}, \tilde{\mathbf{q}}$ *for* $\mathcal{Q}(t)$ *such that* $\mathbf{p} = \tilde{\mathbf{p}}(R(t))$, $\mathbf{q} = \tilde{\mathbf{q}}(R(t))$.

Given $\mathcal{P}(t)$ and its μ-basis, $\mathbf{p}(t)$, $\mathbf{q}(t), \deg(\mathbf{p}) \leq \deg(\mathbf{q})$, one can find the rational function $R(t)$ by Theorem 2 (see Steps 2-5 in Algorithm 2). By Lemma 7, there exists $\tilde{\mathbf{p}}$ such that $\deg(\tilde{\mathbf{p}}) = \deg(\mathbf{p})/\deg(R)$ and $\mathbf{p}(t) = \tilde{\mathbf{p}}(R(t))$. Set $\tilde{\mathbf{p}}$ to be a polynomial vector with undetermined coefficients. Then we get a linear system by comparing the coefficients with respect to the variable t of $\mathbf{p}(t) = \tilde{\mathbf{p}}(R(t))$. Solving this linear system, we get $\tilde{\mathbf{p}}$.

In order to find $\tilde{\mathbf{q}}$, we note that $\tilde{\mathbf{q}}(R(t))$ comes from the μ-basis $\mathbf{p} = \tilde{\mathbf{p}}(R)$, $\mathbf{q} = \tilde{\mathbf{q}}(R)$ of $\mathcal{P}(t)$. Thus, by the definition of a μ-basis, $\tilde{\mathbf{q}}(R(t)) = h_1(t)\mathbf{p}(t) + h_2(t)\mathbf{q}(t)$, where $h_1(t), h_2(t) \in \mathbb{K}[t]$, and $\deg(\tilde{\mathbf{q}}(R)) = \deg(\mathbf{q})$ (by the uniqueness of the degree of a μ-basis). Note that

$$k_1\mathcal{P} = \tilde{\mathbf{p}}(R) \times \tilde{\mathbf{q}}(R) = \mathbf{p} \times (h_1(t)\mathbf{p} + h_2(t)\mathbf{q}) = \mathbf{p} \times h_2(t)\mathbf{q} = k_2h_2(t)\mathcal{P},$$

where k_1, k_2 are nonzero constants. So $h_2(t)k_2 = k_1$ which implies that $h_2(t)$ must be a constant. Thus, we have

$$\tilde{\mathbf{q}}(R) = h_1(t)\mathbf{p} + \mathbf{q}, \quad \deg(h_1) + \deg(\mathbf{p}) \leq \deg(\tilde{\mathbf{q}}(R)).$$

Taking into account that $\deg(\mathcal{P}) = \deg(\tilde{\mathbf{p}}(R)) + \deg(\tilde{\mathbf{q}}(R)) = \deg(\mathbf{p}) + \deg(\tilde{\mathbf{q}}(R))$, we get that $\deg(h_1) \leq \deg(\mathcal{P}) - 2\deg(\mathbf{p})$. Therefore, by setting $\tilde{\mathbf{q}}$ and $h_1(t)$ to have undetermined coefficients and $\deg(h_1) \leq \deg(\mathcal{P}) - 2\deg(\mathbf{p})$, $\deg(\tilde{\mathbf{q}}) = \deg(\mathbf{q})/\deg(R)$, we can solve for $\tilde{\mathbf{q}}$ and $h_1(t)$ from the linear system derived from $\tilde{\mathbf{q}}(R) = h_1(t)\mathbf{p} + \mathbf{q}$.

Finally recall that we are considering the μ-basis and the parametrizations in homogeneous form. Therefore, the equalities to solve, $\mathbf{p} = \tilde{\mathbf{p}}(R)$, $\tilde{\mathbf{q}}(R) = h_1\mathbf{p} + \mathbf{q}$, have to be considered over the projective space of parameters. That is

$$\mathbf{p}(t) = \tilde{\mathbf{p}}(r_1(t), r_2(t)), \quad \tilde{\mathbf{q}}(r_1(t), r_2(t)) = h_1(t)\mathbf{p}(t) + \mathbf{q}(t).$$

Based on the above discussion, here we give an alternative proper reparametrization algorithm to Algorithm 2. In addition, we illustrate this algorithm with an example.

Algorithm 3 (Alternative Proper Reparametrization for Curves using μ-Bases)**.**
Input *a rational parametrization* $\mathcal{P}(t) = (\wp_1(t), \wp_2(t), \wp_3(t))$ *of a plane algebraic curve* $\mathcal{C}$.
Output *a rational proper parametrization* $\mathcal{Q}(t)$ *of* $\mathcal{C}$, *and a rational function* $R(t)$ *such that* $\mathcal{P}(t) = \mathcal{Q}(R(t))$.
Steps

1. *Compute a* μ*-basis* $\mathbf{p}(t), \mathbf{q}(t), \deg(\mathbf{p}) \leq \deg(\mathbf{q})$ *of* $\mathcal{P}(t)$.
2. *Compute* $R(t) = r_1(t)/r_2(t)$ *applying Steps 2-5 of Algorithm 2.*
3. *Compute a* μ*-basis,* $\tilde{\mathbf{p}}$, $\tilde{\mathbf{q}}$, *of* $\mathcal{Q}(t)$ *using* $\mathbf{p}, \mathbf{q}$ *and* $R(t)$ *as follows:*
   3.1. *Set* $\tilde{\mathbf{p}}(t)$ *to have undetermined coefficients with* $\deg(\tilde{\mathbf{p}}) = \deg(\mathbf{p})/\deg(R)$. *Consider the linear system generated by comparing the coefficients with respect to the variable* t *of* $\mathbf{p}(t) = \tilde{\mathbf{p}}(r_1(t), r_2(t))$. *Solving this linear system, we get* $\tilde{\mathbf{p}}(t)$.

3.2. Set $\tilde{\mathbf{q}}(t)$ *and* $h_1(t)$ *to have undetermined coefficients with* $\deg(h_1) \leq \deg(\mathcal{P}) - 2\deg(\mathbf{p})$, $\deg(\tilde{\mathbf{q}}) = \deg(\mathbf{q})/\deg(R)$. *Consider the linear system generated by comparing the coefficients with respect to the variable* t *of* $\tilde{\mathbf{q}}(r_1(t), r_2(t)) = h_1(t)\mathbf{p}(t) + \mathbf{q}(t)$. *Solving this linear system, we get* $\tilde{\mathbf{q}}(t)$.

4. Return $\mathcal{Q}(t) = \tilde{\mathbf{p}}(t) \times \tilde{\mathbf{q}}(t)$ *and* $R(t)$.

Example 3. *Let* $\mathcal{C}$ *be the rational curve considered in Example 2 and defined by the parametrization*

$$\mathcal{P}(t) = (3t^4 + 3t^2 + 1 - t^7 - 2t^5 - t^3 - t^9 - t^8,$$

$$-(t^3 - t^2 - 1)(t^6 + 2t^5 + 2t^4 + 2t^3 + 4t^2 + 2), t^6 + 6t^4 + 6t^2 + 2 + t^7 + 2t^5 + t^3 + t^9 - t^8).$$

We compute a μ*-basis and applying Steps 2-5 of Algorithm 2, we obtain the rational function* $R(t) = (-1 - t^2)/t^3$ *(reason as in Example 2).*

Now, we compute a μ*-basis,* $\tilde{\mathbf{p}}$, $\tilde{\mathbf{q}}$, *of* $\mathcal{Q}(t)$ *using* $\mathbf{p}, \mathbf{q}$ *and* $R(t)$. *For this purpose, we first set* $\tilde{\mathbf{p}}(t)$ *to have undetermined coefficients with* $\deg(\tilde{\mathbf{p}}) = \deg(\mathbf{p})/\deg(R) = 3/3 = 1$. *Consider the linear system generated by comparing the coefficients with respect to the variable* t *of* $\mathbf{p}(t) = \tilde{\mathbf{p}}(r_1(t), r_2(t))$. *Solving this linear system, we get*

$$\tilde{\mathbf{p}}(t) = (7 + 16t, -1 + 5t, -1 + 5t).$$

Set $\tilde{\mathbf{q}}(t)$ *and* $h_1(t)$ *to have undetermined coefficients with* $\deg(h_1) \leq \deg(\mathcal{P}) - 2\deg(\mathbf{p}) = 9 - 2 \cdot 3 = 3$, $\deg(\tilde{\mathbf{q}}) = \deg(\mathbf{q})/\deg(R) = 6/3 = 2$. *Consider the linear system generated by comparing the coefficients with respect to the variable* t *of* $\tilde{\mathbf{q}}(r_1(t), r_2(t)) = h_1(t)\mathbf{p}(t) + \mathbf{q}(t)$. *Solving this linear system, we get*

$$\tilde{\mathbf{q}}(t) = (-132 + 349t + 586t^2, -43 + 16t + 129t^2, -43 + 16t + 129t^2).$$

Finally, the algorithm outputs the proper parametrization $\mathcal{Q}(t)$, *and the rational function* $R(t)$

$$\mathcal{Q}(t) = \left(1 - t + t^2 + t^3, 1 - t + 2t^3, -1 - t - t^2 + 2t^3\right), \qquad R(t) = \frac{-1 - t^2}{t^3}.$$

We finish this subsection by comparing our methods (Algorithms 2 and 3 presented in this subsection and Subsection 3.2) with the methods in [10], [16] and [17].

In [16] a comparative discussion of the existing methods that solve the proper reparametrization problem for the case of plane curves is presented. We compare our algorithms to the algorithm in [17] (A1), the algorithm in [10] (A2), and the proper reparametrization algorithm presented in [16] (A3).

Algorithm A1 is heuristic, and the other two algorithms, A2 and A3, are deterministic. A1 finds the rational function $R(t)$ by computing several GCDs, and solving some linear systems of equations. Algorithms A2 and A3 require only computing a GCD. However, the GCD computed by A3 is more general, and allows one to determine the rational function $R(t)$ simply by choosing two of the coefficients of the GCD. In the case of A1, evaluations and computations of solutions of some linear systems of equations generated from the parametrization are required, and therefore A1 is not as direct as A2 and A3. In order to compute the proper rational parametrization $\mathcal{Q}(t)$, algorithm A3 is much better since A3 computes a simple univariate resultant whereas algorithms A1 and A2 solve the problem by means of the method of undetermined coefficients.

In the algorithms proposed here, the computation of the rational function $R(t)$ is also done by means of a GCD whose computational complexity in general is $\mathcal{O}(n^2)$ (see [1, 2]). But the polynomials used to compute the GCD are of smaller degree than those used in A3. However, first one needs to compute a μ-basis whose computational complexity is also $\mathcal{O}(n^2)$ (see [4, 8]). Then the complexity and efficiency of Algorithm 2 is similar to the algorithm presented in A3, since the computation of $\mathcal{Q}(t)$ is carried out using the method presented in A3. In Algorithm 3, avoiding the resultant computations of $\mathcal{Q}(t)$, we solve an expected μ-basis $\tilde{\mathbf{p}}, \tilde{\mathbf{q}}$ for $\mathcal{Q}(t)$ by solving a linear system and then computing $\mathcal{Q}(t) = \tilde{\mathbf{p}} \times \tilde{\mathbf{q}}$. Notice that the degrees of $\tilde{\mathbf{p}}$ and $\tilde{\mathbf{q}}$ are given exactly and smaller than in the other methods. One more advantage of Algorithm 3 is that we can easily get the implicit equation of the given curve as the $\text{resultant}_t(p^{\mathcal{Q}}(t, \overline{x}), q^{\mathcal{Q}}(t, \overline{x})) = 0$ (see property 10 of Theorem 1 and Example 4).

3.4. Implicitization

A μ-basis provides a compact representation for the implicit equation of the rational curve parametrized by $\mathcal{P}(t)$, with $\deg(\mathcal{P}) = n$. In fact, the Bézout resultant of $p^{\mathcal{P}}(t, \overline{x}), q^{\mathcal{P}}(t, \overline{x})$ with respect to t gives the implicit equation of $\mathcal{P}(t)$ expressed as a determinant of size $(n-\mu) \times (n-\mu)$ (see e.g. [13]). For the generic case with $\mu = n/2$, the size of the determinant computed from a μ-basis is half of the size of the determinant computed by the classical method. In this regard, a μ-basis serves as a bridge to connect the parametric form and the implicit form of a rational parametric curve. All the above properties hold for improperly parameterized curves, except that the resultant gives the implicit equation to some power. The power is $\deg(R)$ if $\mathcal{P} = \mathcal{Q}(R)$, where $\mathcal{Q}$ is a proper parametrization of the given curve, and $\deg(R)$ is in fact $\deg(\phi_{\mathcal{P}})$ (compare with [18, 19] and [25]). This fact is proved with subtle algebraic analysis in [7]. In the following theorem, we give a simple proof based on the properties of μ-bases and resultants.

Theorem 6. *Let $\mathbf{p}(t)$, $\mathbf{q}(t)$ be a μ-bases for the rational curve $\mathcal{C}$ defined by $\mathcal{P}(t)$ with $\deg(\mathbf{p}) \le \deg(\mathbf{q})$. Then*

$$\text{resultant}_t(p^{\mathcal{P}}(t, \overline{x}), q^{\mathcal{P}}(t, \overline{x})) = f(\overline{x})^{\deg(\phi_{\mathcal{P}})},$$

where $f(\overline{x})$ is the defining polynomial of the curve $\mathcal{C}$, and $p^{\mathcal{P}}(t, \overline{x}) = \mathbf{p}(t) \cdot \overline{x}$, $q^{\mathcal{P}}(t, \overline{x}) = \mathbf{q}(t) \cdot \overline{x}$.

Proof. From Lüroth's Theorem it is well known that there exists $R(t) = r_1(t)/r_2(t) \in \mathbb{K}(t) \setminus \mathbb{K}$ such that $\mathcal{P} = \mathcal{Q}(R)$, where $\mathcal{Q}$ is a proper parametrization of $\mathcal{C}$. In addition, from Lemma 2, $\mathbf{p}(t) = \tilde{\mathbf{p}}(R(t))$, $\mathbf{q}(t) = \tilde{\mathbf{q}}(R(t))$ is a μ-basis for $\mathcal{P}(t)$ with $\deg(\mathbf{p}) \le \deg(\mathbf{q})$, where $\tilde{\mathbf{p}}$, $\tilde{\mathbf{q}}$ is a μ-basis for $\mathcal{Q}$, with $\deg(\tilde{\mathbf{p}}) \le \deg(\tilde{\mathbf{q}})$. Since $\mathcal{Q}$ is proper, from property 10 of Theorem 1,

$$\text{resultant}_t(p^{\mathcal{Q}}(t, \overline{x}), q^{\mathcal{Q}}(t, \overline{x})) = f(\overline{x}),$$

where $p^{\mathcal{Q}}(t, \overline{x}) = \tilde{\mathbf{p}}(t) \cdot \overline{x}$, $q^{\mathcal{Q}}(t, \overline{x}) = \tilde{\mathbf{q}}(t) \cdot \overline{x}$. Note that by the properties of resultants (see e.g. Appendix in [18]),

$$f(\overline{x}) = \text{resultant}_t(p^{\mathcal{Q}}(t, \overline{x}), q^{\mathcal{Q}}(t, \overline{x})) = A^r \prod_{\substack{U(\overline{x}) \in \mathbb{L} \\ p^{\mathcal{Q}}(U(\overline{x}), \overline{x}) = 0}} q^{\mathcal{Q}}(U(\overline{x}), \overline{x}),$$

where $\mathbb{L}$ denotes the algebraic closure of $\mathbb{K}(\overline{x})$, A is the leading coefficient of $p^{\mathcal{Q}}(t, \overline{x})$ w.r.t. t and $r := \deg_t(q^{\mathcal{Q}})$. Similarly,

$$\text{resultant}_t(p^{\mathcal{P}}(t, \overline{x}), q^{\mathcal{P}}(t, \overline{x})) = B^s \prod_{\substack{V(\overline{x}) \in \mathbb{L} \\ p^{\mathcal{P}}(V(\overline{x}), \overline{x}) = 0}} q^{\mathcal{P}}(V(\overline{x}), \overline{x}),$$

where B is the leading coefficient of $p^{\mathcal{P}}(t, \overline{x})$ w.r.t. t and $s := \deg_t(q^{\mathcal{P}})$. Since $\mathbf{p}(t) = \tilde{\mathbf{p}}(R(t))$, $\mathbf{q}(t) = \tilde{\mathbf{q}}(R(t))$,

$$\text{resultant}_t(p^{\mathcal{P}}(t, \overline{x}), q^{\mathcal{P}}(t, \overline{x})) = B^s \prod_{\substack{V(\overline{x}) \in \mathbb{L} \\ p^{\mathcal{Q}}(R(V(\overline{x})), \overline{x}) = 0}} q^{\mathcal{Q}}(R(V(\overline{x})), \overline{x}).$$

Then $V(\overline{x}) = R^{-1}(U(\overline{x}))$ and thus

$$\text{resultant}_t(p^{\mathcal{P}}(t, \overline{x}), q^{\mathcal{P}}(t, \overline{x})) = B^s \prod_{\substack{V(\overline{x}) \in \mathbb{L} \\ R(V) = U,\ p^{\mathcal{Q}}(U(\overline{x}), \overline{x}) = 0}} q^{\mathcal{Q}}(U(\overline{x}), \overline{x})^{\deg(R)}.$$

Hence

$$\text{resultant}_t(p^{\mathcal{P}}(t, \overline{x}), q^{\mathcal{P}}(t, \overline{x})) = f(\overline{x})^{\deg(R)} = f(\overline{x})^{\deg(\phi_{\mathcal{P}})}.$$

□

Note that as an alternative to the approach in Theorem 6, we can find $\tilde{\mathbf{p}}(t)$ and $\tilde{\mathbf{q}}(t)$ from Algorithm 3 and compute the implicit equation from a resultant with smaller size.

Example 4. *Let $\mathcal{C}$ be the rational curve introduced in Example 2 defined by the parametrization*

$$\mathcal{P}(t) = (3t^4+3t^2+1-t^7-2t^5-t^3-t^9-t^8,$$

$$-(t^3-t^2-1)(t^6+2t^5+2t^4+2t^3+4t^2+2), t^6+6t^4+6t^2+2+t^7+2t^5+t^3+t^9-t^8).$$

We determine the polynomials $p^{\mathcal{P}}(t,\overline{x}) = \mathbf{p}(t)\cdot\overline{x}$, $q^{\mathcal{P}}(t,\overline{x}) = \mathbf{q}(t)\cdot\overline{x}$, where the μ-basis is computed in Example 2. Now we get

$$\text{resultant}_t(p^{\mathcal{P}}(t,\overline{x}), q^{\mathcal{P}}(t,\overline{x})) = (102x_1^3-265x_2x_1^2+237x_2^2x_1-73x_2^3+98x_3x_1^2-164x_2x_1x_3+70x_2^2x_3+23x_3^2x_1-18x_2x_3^2+2x_3^3)^3.$$

Thus Theorem 6 holds (note that in Example 2, we get that $\deg(R) = \deg(\phi_{\mathcal{P}}) = 3$) and

$$f(\overline{x}) = 102x_1^3-265x_2x_1^2+237x_2^2x_1-73x_2^3+98x_3x_1^2-164x_2x_1x_3+70x_2^2x_3+23x_3^2x_1-18x_2x_3^2+2x_3^3.$$

Alternatively, we can use the polynomials $p^{\mathcal{Q}}(t,\overline{x}) = \tilde{\mathbf{p}}(t)\cdot\overline{x}$, $q^{\mathcal{Q}}(t,\overline{x}) = \tilde{\mathbf{q}}(t)\cdot\overline{x}$, where $\tilde{\mathbf{p}}(t),\tilde{\mathbf{q}}(t)$ is the μ-basis given in Example 3 (see property 10 of Theorem 1). Then one gets

$$\text{resultant}_t(p^{\mathcal{Q}}(t,\overline{x}), q^{\mathcal{Q}}(t,\overline{x})) = -433f(\overline{x}).$$

4. Conclusion

We study the μ-bases of improper rational planar curves. Two proper reparametrization algorithms are given based on μ-bases. The theoretical complexities of the proposed methods are similar to the current best method [16]; however, the results are essential to the theoretical completeness of the theory of μ-bases. In addition, one can get additional benefits from μ-bases. In summary, we provide an interchange graph for the rational curves that are not necessarily proper (see Figure 1). The red parts can be found in previous works while the blue parts are proposed in this paper.

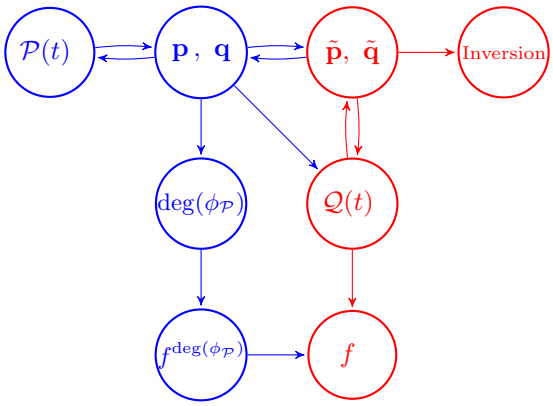

Figure 1: A μ-basis serves as a bridge for a planar curve

We show how μ-bases allow us to compute the inversion formula for a given proper parametrization $\mathcal{P}(t)$ of an algebraic curve. If $\mathcal{P}(t)$ is not proper, we show how the degree of the rational map induced by $\mathcal{P}(t)$ can be computed as well as the elements of the fibre. Directly from $\mathcal{P}(t)$, we propose a method to find a μ-basis for a proper reparametrization $\mathcal{Q}(t)$. Finally, we show how the μ-basis of a given improper parametrization also allows us to compute the implicit equation of a given curve. More precisely it is shown that the Bézout

resultant of $p^{\mathcal{P}}(t, \overline{x}), q^{\mathcal{P}}(t, \overline{x})$, with respect to t gives the implicit equation of $\mathcal{P}(t)$ to the power $\deg(R)$, where $\mathcal{P}(t) = \mathcal{Q}(R(t))$ and $\mathcal{Q}(t)$ is a proper parametrization of the given curve. We can also compute the implicit equation from the μ-basis constructed for $\mathcal{Q}(t)$.

Our methods can be generalized to rational curves in arbitrary dimensions, since the study of proper reparametrization still deals with one variable. The papers [12, 26] focus on applications of μ-basis for general proper rational curves in arbitrary dimensions. They generalize the μ-basis algorithm for the parametric forms whose coordinators having common factors. Combining our results with those in [12, 26], we could attempt to compute the μ-basis for a general rational curve in arbitrary dimensions, not necessarily proper, with the coordinate functions having common factors. In this case there will be some additional interesting properties that will require further study, so we leave these problems for future research.

Acknowledgements

This work has been partially supported by FEDER/Ministerio de Ciencia, Innovación y Universidades-Agencia Estatal de Investigación/MTM2017-88796-P (Symbolic Computation: new challenges in Algebra and Geometry together with its applications), Beijing Natural Science Foundation under Grant Z190004 and NSFC under Grant 61872332, 11731013. The first author belongs to the Research Group ASYNACS (Ref. CT-CE2019/683). We are grateful to the anonymous referees for the valuable suggestions and, in particular, for the careful grammar checking.

References

[1] Belhaj S., Kahla H. B. (2013). *On the complexity of computing the GCD of two polynomials via Hankel matrices.* ACM Communications in Computer Algebra, 46(3/4), 74-75.
[2] Bini D. A., Boito P. (2010). *A Fast Algorithm for Approximate Polynomial GCD Based on Structured Matrix Computations.* Numerical Methods for Structured Matrices and Applications: The Georg Heinig Memorial Volume, 155-173.
[3] Blasco A., Pérez-Díaz S. (2019). *An in Depth Analysis, via Resultants, of the Singularities of a Parametric Curve.* Computer Aided Geometric Design, 68, 22-47.
[4] Chen F., Wang W. (2003). *The μ-Basis of a Planar Rational Curve—Properties and Computation.* Graphcial Models, 64 (14), 368-381.
[5] Chen F., Cox D., Liu Y. (2005). *The μ-Basis and Implicitization of Rational Parametric Surfaces.* Journal of Symbolic Computation, 39, 689-706.
[6] Corless R., Watt S., Zhi L. (2004). *QR Factoring to computing the GCD of univariate approximate polynomials.* IEEE Transations on Signal Process, 52, 3394-3402.
[7] Cox D.A., Sederberg T.W., Chen F. (1998). *The Moving Line Ideal Basis of Planar Rational Curves.* Computer Aided Geometric Design, 15, 803-827.
[8] Deng J., Chen F., Shen L. (2005) *Computing μ-Basis of Rational Curves and Surfaces Using Polynomial Matrix Factorization*, in: Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation, ACM, 132-139.
[9] Emiris I., Galligo A., Lombardi H. (1997). *Certified Approximate Univariate GCDs.* Journal of Pure and Applied Algebra, 117, 229-251.
[10] Gutierrez J., Rubio R., Sevilla D. (2002). *On Multivariate Rational Decomposition.* Journal of Symbolic Computation, 33, 545-562.
[11] Harris J. (1995). *Algebraic Geometry. A First Course.* Springer-Verlag.
[12] Hoon H., Zachary H., Irina A. K. (2017). *Algorithm for computing μ-bases of univariate polynomials.* Journal of Symbolic Computation, 80(3), 844-874.
[13] Jia X., Shi X., Chen F. (2018). *Survey on the Theory and Applications of μ-Basis for Rational Curves and Surfaces.* Journal of Computational and Applied Mathematics, 329, 2-23.
[14] Jouanolou, J.-P. (1991). *Le Formalisme du Resultant.* Advaces in Mathematics, 90(2), 117-263.
[15] Lai Y., Chen F. (2016). *Implicitizing rational surfaces using moving quadrics constructed from moving planes.* Journal of Symbolic Computation, 77, 127-161.
[16] Pérez-Díaz S. (2006). *On the Problem of Proper Reparametrization for Rational Curves and Surfaces.* Computer Aided Geometric Design, 23(4), 307-323.
[17] Sederberg T.W. (1986), *Improperly Parametrized Rational Curves.* Computer Aided Geometric Design, 3, 67-75.
[18] Sendra J.R., Winkler F., Pérez-Díaz S. (2007), *Rational Algebraic Curves: A Computer Algebra Approach*, Series: Algorithms and Computation in Mathematics, 22, Springer Verlag.
[19] Sendra J.R., Winkler F. (2001). *Tracing Index of Rational Curve Parametrizations.* Computer Aided Geometric Design, 18(8), 771-795.
[20] Shafarevich I.R. (1994). *Basic Algebraic Geometry Schemes; Volume 1 Varieties in Projective Space.* Berlin New York : Springer-Verlag.

[21] Shen L., Goldman R. (2017). *Strong μ-Basis for Rational Tensor Product Surfaces and Extraneous Factors Associated to Bad Base Points and Anomalies at Infinity.* SIAM Journal on Applied Algebra and Geometry, 1(1), 328-351.
[22] Shen L., Goldman R. (2017). *Algorithms for Computing Strong μ-Basis for Rational Tensor Product Surfaces.* Computer Aided Geometric Design, 52-53, 48-62.
[23] Shen L., Pérez-Díaz S. (2015). *Numerical Proper Reparametrization of Parametric Plane Curves.* Journal of Computational and Applied Mathematics, 277, 138-161.
[24] Shen L., Pérez-Díaz S., Yang Z. (2019). *Numerical Proper Reparametrization of Space Curves and Surfaces.* Computer Aided-Design, 116, article 102732.
[25] Shen L., Yuan C. (2010). *Implicitization using univariate resultants.* Journal of Systems Science and Complexity, 23, 804–814.
[26] Song N., Goldman R. (2009). *μ-Bases for Polynomial Systems in One Variable.* Computer Aided Geometric Design, 26, 217–230.
[27] Walker R.J. (1950). *Algebraic Curves.* Princeton Univ. Press.
[28] Zheng J, Sederberg T. (2001). *A Direct Approach to Computing the μ-Basis of Planar Rational Curves.* Journal of Symbolic Computation, 31, 619-629.