Using a Bihomogeneous Resultant to Find the
Singularities of Rational Space Curves

Xiaoran Shi
Department of Mathematics, Harbin Institute of Technology, 150001, China
Beijing Computational Science Research Center, 100084, China
University of Science and Technology of China, Hefei, 230026, China

Xiaohong Jia
KLMM, NCMIS, Academy of Mathematics and Systems Science, Chinese Academy of Sciences,
100080, China

Ron Goldman
Computer Science Department, Rice University, 6100 Main St., MS-132, Houston, TX 77005,
USA

with an Appendix written by

Brendan Hassett
Department of Mathematics, Rice University, 6100 S. Main St., MS-136, Houston, TX
77251-1892, USA

Abstract

We provide a new technique to detect the singularities of rational space curves. Given a rational
parametrization of a space curve, we first compute a $\mu$-basis for the parametrization. From
this $\mu$-basis we generate three planar algebraic curves of different bidegrees whose intersection
points correspond to the parameters of the singularities. To find these intersection points, we
construct a new sparse resultant matrix for these three bivariate polynomials. We then compute
the parameter values corresponding to the singularities by applying Gaussian elimination to
this resultant matrix. Let $\nu_Q$ denote the multiplicity of the singular point $Q$, and let $n$ be
the degree of the curve. We find that when $\sum \nu_Q \leq 2n - 3$, the last nonzero row after Gaussian
elimination represents a univariate polynomial whose roots are exactly the parameter values of
the singularities with the correct multiplicity. Otherwise the last two nonzero rows represent two
bivariate polynomials whose common roots provide the parameter values of the singularities. We
also show that if $R$ is this resultant matrix, then $\text{size}(R) - \text{rank}(R)$ gives the total multiplicity
$\sum \nu_Q (\nu_Q - 1)$ of all the singular points including the infinitely near singular points of a rational

Preprint submitted to Elsevier 16 November 2012
space curve and we provide bounds on the expression $\sum \nu_Q(\nu_Q - 1)$ for the total multiplicity of all the singular points of a rational space curve. To verify our results, we present several examples to illustrate our methods.

Key words: Rational space curve, resultant matrix, $\mu$-basis, singularities, intersection number.
1. Introduction

Singularities are the most interesting and important points on curves and surfaces. These critical points contain a great deal of information about the geometry and topology of the curve, so detecting and analyzing singularities is very useful in geometric modeling and computer graphics.

Over the years, a great deal of research has been devoted to the study of the singularities of rational planar curves (see, for example, Chen and Sederberg (2002), Coolidge (1931), Fulton (1989), Hilton (1920), Perez-Diaz (2007), Walker (1950), Jia and Goldman (2009)). However, there is much less work on the detection and analysis of singularities for non-planar curves. Most techniques are based either on Groebner basis computations (Park (2002)) or on generalized resultants (Rubin, Serradilla and Velez (2009)).

Since \( \mu \)-bases were first introduced into geometric modeling by Cox, Sederberg and Chen (1998), many applications of \( \mu \)-bases have been investigated. Recently, Wang, Jia and Goldman (2009) applied \( \mu \)-bases to compute the singularities of three-dimensional space curves of low degree. Shi and Chen (2010) computed the singularities of rational space curves from the Smith form of two random combinations of \( \mu \)-basis functions. Busé and Luu Ba (2010) constructed a non-square Sylvester style matrix derived from a \( \mu \)-basis, for which the corresponding Smith form provides the parameter values and the multiplicities of all the singularities.

Here, using \( \mu \)-bases we shall reduce the problem of computing the singularities on a rational space curve to the problem of computing the intersection points of three related planar algebraic curves of different bidegrees. Resultants for bivariate polynomials can be used to compute the intersection of three planar algebraic curves. But most papers on multivariate resultants, such as (Chionh, Goldman and Zhang (1998); Dickenstein and Emiris (2003); Emiris and Pan (2002); Sturmfels and Zelevinsky (1994)), deal either with total degree polynomials or with polynomials of the same multidegree, while our algebraic curves are represented by three polynomials with different bidegrees. Therefore, to analyze the intersections of these three planar curves, we construct a new sparse resultant matrix for these three bivariate polynomials. Let \( R \) denote this resultant matrix and let \( \nu_Q \) denote the multiplicity of the singular point \( Q \). We show that \( \text{size}(R) - \text{rank}(R) = \sum \nu_Q(\nu_Q - 1) \), where the sum is taken over all the singularities including the infinitely near singularities of the space curve. We also show how to find the singularities of the rational space curve by applying Gaussian elimination to this sparse resultant matrix. Our square Sylvester style resultant matrix \( R \) is intimately related to the non-square Sylvester style matrix of Busé and Luu Ba, but the entries of our square matrix are constants, whereas the entries of their non-square matrix are univariate polynomials; for further details and comparisons, see the Remark in Section 5.

Compared with previous work by Shi and Chen (2010) and Busé and Luu Ba (2010), the main contributions of this paper are the following. First, since our work is based only on a sparse numerical matrix, our computations are simpler than previous methods. Second, since the expression \( \sum \nu_Q(\nu_Q - 1) \) for the total multiplicity of all the singular points of a rational space curve depends only on the size and rank of the resultant matrix, when there are only a small number of singularities, we can compute the number of singularities and their multiplicities without knowing the locations of the singularities.

We begin in Section 2 by introducing the notion of singularities for rational space curves and the blow up method which can be used to find all the infinitely near singular
points. In Section 3, we review the properties of $\mu$-bases for rational space curves and we show how to use $\mu$-bases to construct three planar algebraic curves whose intersection points correspond to the singularities of the corresponding rational space curve. To find these intersection points, we construct in Section 4 a resultant matrix for three polynomials of bidegrees $(\varsigma_1, \tau)$, $(\varsigma_2, \tau)$, $(\varsigma_3, \tau)$. By applying Gaussian elimination to this resultant matrix, we show in Section 5 how to generate a single univariate polynomial whose roots are exactly the parameter values of the singularities with the correct multiplicity whenever $\sum Q \nu_Q \leq 2n - 3$. Otherwise when $\sum Q \nu_Q > 2n - 3$, we apply Gaussian elimination to the resultant matrix to construct two bivariate polynomials whose common roots correspond to the singularities. We also show that if $R$ is this resultant matrix, then $\text{size}(R) - \text{rank}(R) = \sum \nu_Q (\nu_Q - 1)$. In Section 6 we provide an algorithm based on the results in Section 5 for finding all the singularities including all the infinitely near singularities of a rational space curve. We then present some examples to illustrate our methods and to confirm our results from Section 5. We close in Section 7 with a short summary of our work along with a brief discussion of the strengths and weaknesses of our method. We also include an Appendix by Brendan Hassett which uses sheaf cohomology to prove that $\text{size}(R) - \text{rank}(R) = \sum \nu_Q (\nu_Q - 1)$.

2. Singularities, infinitely near points and blow ups

We shall now briefly review some basic concepts related to singularities and $\mu$-bases. Much of this material is taken verbatim from a previous paper by one of the authors' (Shi and Chen (2010)). We repeat this material here for the sake of completeness.

Let $\mathbb{R}[s, u]$ be the set of homogeneous polynomials in the homogeneous parameter $s : u$ with real coefficients. A degree $n$ rational space curve $C$ is usually represented by a parametrization given in homogeneous form

$$P(s, u) = (a(s, u), b(s, u), c(s, u), d(s, u))$$

where $a(s, u), b(s, u), c(s, u), d(s, u)$ are degree $n$ homogeneous polynomials in $\mathbb{R}[s, u]$.

Throughout this paper we will assume that the four polynomials $a(s, u), b(s, u), c(s, u), d(s, u)$ are relatively prime and linearly independent. Furthermore, we shall assume that the parametrization of the rational space curve $P(s, u)$ is generically one-to-one.

In computer aided geometric design, people care mostly about real curves. Here we consider the parametrization $P(s, u)$ as a complex curve with real coefficients. The following analysis works over the complex field.

2.1. Singularities

Intuitively, a singular point is a point on a curve (surface) where the tangent line (plane) is not uniquely determined. More formally, we have the following definition:

**Definition 1.** Let $Q$ be a point on a rational space curve $C$, and let $\Pi$ be a plane containing $Q$. Then the point $Q$ is called a **singular point of order** $k \geq 2$, if the intersection multiplicity of $C$ with $\Pi$ at $Q$ is $k \geq 2$ for every generic choice of $\Pi$. A point on the curve is nonsingular if and only if $k = 1$. A point is not on the curve if and only if $k = 0$.
Definition 2. Let \( Q \) be a singular point of order \( k \geq 2 \) on a space curve \( C \) given by a rational parametrization \( P(s, u) \) as in (1). Let \( \Pi := a_0x + b_0y + c_0z + d_0w = 0 \) be a generic plane containing \( Q \). Define \( \Phi(s, u) := a_0a(s, u) + b_0b(s, u) + c_0c(s, u) + d_0d(s, u) \). Then \( \Phi(s, u) \) contains a factor \( h(s, u) \) which is independent of the choice of \( \Pi \). The polynomial \( h(s, u) \) has degree \( k \), and the roots of \( h(s, u) \) are the parameters (with proper multiplicity) corresponding to the point \( Q \). We call \( h(s, u) \) the inversion formula for the point \( Q \).

2.2. Infinitely near singularities and blow ups

Consider a rational space curve \( C \), given by the parametrization \( P(s, u) \). If a singular point \( Q \) is non-ordinary, there will be additional singularities \( Q^* \) arising from the singular point \( Q \) when the parametrization \( P(s, u) \) undergoes a small perturbation. We call the singularities \( Q^* \) infinitely near points arising from the point \( Q \).

Without loss of generality, we can move \( Q \) to the origin \((0, 0, 0, 1)\). Then the parametrization \( P(s, u) \) becomes

\[
P(s, u) = (a(s, u)h(s, u), b(s, u)h(s, u), c(s, u)h(s, u), d(s, u)),
\]

where \( \gcd(a, b, c) = 1 \), \( \gcd(h, d) = 1 \), and \( h(s, u) \) is the inversion formula for the point \( Q \). We can also ensure that \( \gcd(a, h) = 1 \) by a coordinate transformation.

Given a rational space curve with a parametrization in the form of (2), infinitely near singularities to the singular point \( Q = (0, 0, 0, 1) \) can be found by blowing up the parametrization at \( Q \). Let \( P^1(s, u) \) be the homogeneous form of the curve given by the parametrization

\[
\left( \frac{x}{w}, \frac{y}{x}, \frac{z}{x} \right) = \left( \frac{ah}{d}, \frac{b}{a}, \frac{c}{a} \right);
\]

then

\[
P^1(s, u) = (a^2h, bd, cd, ad).
\]

A point \( Q^* \) is an infinitely near singularity in the first neighborhood of \( Q \) if \( Q^* \) is a singularity on the blow up curve given by the parametrization \( P^1(s, u) \) and \( Q^* \) is related to \( Q \), i.e., all the parameters corresponding to \( Q^* \) form a subset of all the parameters corresponding to \( Q \). If we continue to blow up the space curve given by the parametrization \( P^1(s, u) \) to get \( P^2(s, u) \), the points on the curve given by the parametrization \( P^2(s, u) \) related to the point \( Q \) are said to be in the second neighborhood of \( Q \), and so on. Thus we have the following definition:

Definition 3. We say that there is an infinitely near singular point of multiplicity \( r \) arising from the \( i \)-th neighborhood of the point \( Q \), if there is a singularity \( Q^* \) of multiplicity \( r \) on the \( i \)-th level blow up space curve which is given by the parametrization \( P^i(s, u) \), whose parameters correspond to the parameters of the point \( Q \).

3. \( \mu \)-bases of rational space curves

A moving plane

\[
L(s, u; x, y, z, w) := A(s, u)x + B(s, u)y + C(s, u)z + D(s, u)w = 0
\]

(4)
is a set of planes with each homogeneous parameter $s : u$ corresponding to a plane, where $A(s, u), B(s, u), C(s, u)$ and $D(s, u)$ are homogeneous polynomials in $\mathbb{R}[s, u]$. We shall often write a moving plane $L(s, u)$ in vector form $L(s, u) = (A(s, u), B(s, u), C(s, u), D(s, u))$.

A moving plane $L(s, u)$ is said to follow the parametrization $P(s, u)$ if and only if

$$L(s, u) \cdot P(s, u) = aA + bB + cC + dD \equiv 0.$$  \hfill (5)

That is, for every homogeneous parameter $s_0 : u_0$, the plane

$$L(s_0, u_0; x, y, z, w) = A(s_0, u_0)x + B(s_0, u_0)y + C(s_0, u_0)z + D(s_0, u_0)w = 0$$

passes through the point $P(s_0, u_0) = (a(s_0, u_0), b(s_0, u_0), c(s_0, u_0), d(s_0, u_0))$ on the curve.

Let $M_p$ be the set of all the moving planes following the parametrization $P(s, u)$. Then $M_p$ is a free syzygy module of rank three (Cox, Sederberg and Chen (1998)).

**Definition 4.** The moving planes $p(s, u), q(s, u)$ and $r(s, u)$ are called a $\mu$-basis for the rational space curve given by the parametrization $P(s, u)$ if

- $p(s, u), q(s, u)$ and $r(s, u)$ form a basis for the syzygy module $M_p$, i.e., any moving plane $L(s, u) \in M_p$ can be written as

$$L(s, u) = \alpha(s, u)p(s, u) + \beta(s, u)q(s, u) + \gamma(s, u)r(s, u),$$

where $\alpha(s, u), \beta(s, u), \gamma(s, u) \in \mathbb{R}[s, u]$.

Every rational space curve has a $\mu$-basis. Moreover, there is a fast algorithm for computing a $\mu$-basis based on Gaussian elimination (Song and Goldman (2009)). Every $\mu$-basis has the following properties.

**Proposition 5.** (Cox, Sederberg and Chen (1998)) Let $P(s, u)$ be a parametrization of a rational space curve with $\mu$-basis $p(s, u), q(s, u), r(s, u)$. Then

1. $[p(s, u), q(s, u), r(s, u)] = \kappa P(s, u)$, where $\kappa$ is a nonzero constant, and $[p, q, r]$ is the outer product of $p, q, r$.
2. $\deg(p) + \deg(q) + \deg(r) = \deg(P)$.
3. $p(s, u), q(s, u), r(s, u)$ are linearly independent for every parameter $(s, u)$.

Let $\deg(p(s, u)) = \mu_1$, $\deg(q(s, u)) = \mu_2$, $\deg(r(s, u)) = \mu_3$, and if necessary reorder $p, q, r$ so that $\mu_1 \leq \mu_2 \leq \mu_3$. The $\mu$-basis elements $p, q, r$ for a rational space curve are not unique, but the degrees $\mu_1, \mu_2, \mu_3$ of the $\mu$-basis elements are unique (Cox, Sederberg and Chen (1998)). We call $(\mu_1, \mu_2, \mu_3)$ the type of the curve given by the parametrization $P(s, u)$.

**Lemma 6.** (Wang, Jia and Goldman (2009)) Let $p(s, u), q(s, u), r(s, u)$ be a $\mu$-basis for the rational space curve given by the parametrization $P(s, u)$. Then the inversion formula for a point $Q$ on the curve is given by the polynomial

$$h_Q(s, u) := \gcd(p(s, u), Q, q(s, u), Q, r(s, u), Q).$$  \hfill (6)

Let $p(s, u), q(s, u), r(s, u)$ be a $\mu$-basis for the rational space curve given by the parametrization $P(s, u)$. The following three bihomogeneous polynomials play a prominent role in our analysis of the singularities of the curve given by the parametrization...
\[ F(s, u; t, v) = \frac{p(s, u) \cdot P(t, v)}{sv - tu}, \]
\[ G(s, u; t, v) = \frac{q(s, u) \cdot P(t, v)}{sv - tu}, \]
\[ H(s, u; t, v) = \frac{r(s, u) \cdot P(t, v)}{sv - tu}. \]

**Theorem 7.** The parameters \((s_0, u_0; t_0, v_0)\) are a common root of \(F(s, u; t, v) = 0, G(s, u; t, v) = 0,\) and \(H(s, u; t, v) = 0\) if and only if the two parameter pairs \((s_0, u_0)\) and \((t_0, v_0)\) correspond to the same singularity on the curve given by the parametrization \(P(s, u).\)

**Proof.** Let \(P(t_0, v_0) = Q.\) Then \((s_0, u_0; t_0, v_0)\) is a common root of \(F(s, u; t, v) = 0, G(s, u; t, v) = 0,\) and \(H(s, u; t, v) = 0\) if and only if \((s_0, u_0)\) is a root of

\[
gcd(F(s, u; t_0, v_0), G(s, u; t_0, v_0), H(s, u; t_0, v_0)) =
\gcd(\frac{p(s, u) \cdot Q}{sv_0 - tu_0}, \frac{q(s, u) \cdot Q}{sv_0 - tu_0}, \frac{r(s, u) \cdot Q}{sv_0 - tu_0}).
\]

which is equivalent to

\[
(su_0 - sv_0)(sv_0 - tu_0)|gcd(p(s, u) \cdot Q, q(s, u) \cdot Q, r(s, u) \cdot Q). \quad (7)
\]

But by Lemma 6, Equation (7) holds if and only if the parameter values \((s_0, u_0)\) and \((t_0, v_0)\) are both parameters for the point \(Q\) relative to the parametrization \(P(s, u).\)

Suppose that the curve given by the parametrization \(P(s, u)\) is of degree \(n,\) and that the \(\mu\)-basis elements \(p(s, u), q(s, u), r(s, u)\) are of degrees \(\mu_1, \mu_2, \mu_3,\) where \(\mu_1 + \mu_2 + \mu_3 = n.\) Then the three polynomials \(F(s, u; t, v) = 0, G(s, u; t, v) = 0,\) and \(H(s, u; t, v) = 0\) are of bidegrees \((\mu_1 - 1, n - 1), (\mu_2 - 1, n - 1), (\mu_3 - 1, n - 1).\) Therefore, by Theorem 7, to determine whether the curve given by the parametrization \(P(s, u)\) has any singularities, we need to determine whether these three bivariate polynomials of bidegrees \((\mu_1 - 1, n - 1), (\mu_2 - 1, n - 1), (\mu_3 - 1, n - 1)\) have any common roots. This observation leads us to the study of resultants for three bivariate polynomials of bidegrees \((\zeta_1, \tau), (\zeta_2, \tau), (\zeta_3, \tau).\)

4. A resultant for three polynomials of bidegrees \((\zeta_1, \tau), (\zeta_2, \tau), (\zeta_3, \tau)\)

Consider the general case of three bihomogeneous polynomials,

\[
f(s, u; t, v) = \sum_{i=0}^{\zeta_1} \sum_{j=0}^{\tau} a_{i,j} s^i u^{\zeta_1-i} t^j v^{\tau-j} \quad \text{of bidegree} \( (\zeta_1, \tau), \)
\]
\[
g(s, u; t, v) = \sum_{i=0}^{\zeta_2} \sum_{j=0}^{\tau} b_{i,j} s^i u^{\zeta_2-i} t^j v^{\tau-j} \quad \text{of bidegree} \( (\zeta_2, \tau), \)
\]
\[
h(s, u; t, v) = \sum_{i=0}^{\zeta_3} \sum_{j=0}^{\tau} c_{i,j} s^i u^{\zeta_3-i} t^j v^{\tau-j} \quad \text{of bidegree} \( (\zeta_3, \tau). \)
\]
where \( \varsigma_1 \leq \varsigma_2 \leq \varsigma_3 \). There is a unique irreducible polynomial \( \text{Res}(f, g, h) \) in the coefficients of \( f, g, h \) such that \( f(s, u; t, v), g(s, u; t, v), h(s, u; t, v) \) have a common root in \( \mathbb{CP}^1 \times \mathbb{CP}^1 \) if and only if \( \text{Res}(f, g, h) = 0 \). The function \( \text{Res}(f, g, h) \) is called the resultant of \( f, g, h \).

We shall construct a simple Sylvester style matrix \( R \), and then prove that \( \det(R) \) is indeed the resultant of \( f, g, h \). We proceed in the following fashion:

1. multiply \( f(s, t) \) by the monomials \( s^{i_1+\varsigma_1-1}u^{t_1-1}v^{j_1-1} \), where \( i_1 = 1, ..., \varsigma_2 + \varsigma_3 \) and \( j_1 = 1, ..., \tau; \)
2. multiply \( g(s, t) \) by the monomials \( s^{i_2+\varsigma_2-1}u^{t_2-1}v^{j_2-1} \), where \( i_2 = 1, ..., \varsigma_1 + \varsigma_3 \) and \( j_2 = 1, ..., \tau; \)
3. multiply \( h(s, t) \) by the monomials \( s^{i_3+\varsigma_3-1}u^{t_3-1}v^{j_3-1} \), where \( i_3 = 1, ..., \varsigma_1 + \varsigma_2 \) and \( j_3 = 1, ..., \tau. \)

This approach generates \( 2\varsigma \tau \) polynomials, where \( \varsigma = \varsigma_1 + \varsigma_2 + \varsigma_3. \) If we put the coefficients of these polynomials into a matrix, we get a square matrix \( R \) of size \( 2\varsigma \times 2\varsigma \).

\[
\begin{pmatrix}
    s^{i_1+\varsigma_1-1}u^{t_1-1}f \\
    \vdots \\
    u^{i_2+\varsigma_2-1}v^{j_2-1}f \\
    s^{i_2+\varsigma_2-1}u^{t_2-1}g \\
    \vdots \\
    u^{i_3+\varsigma_3-1}v^{j_3-1}g \\
    s^{i_3+\varsigma_3-1}u^{t_3-1}h \\
    \vdots \\
    u^{i_3+\varsigma_3-1}v^{j_3-1}h
\end{pmatrix} = R \cdot 
\begin{pmatrix}
    s^{i_1+\varsigma_1-1}u^{t_1-1} \\
    \vdots \\
    s^{i_2+\varsigma_2-1}u^{t_2-1} \\
    \vdots \\
    s^{i_3+\varsigma_3-1}u^{t_3-1}
\end{pmatrix}
\]

Notice that if \( \varsigma_1 = \varsigma_2 = \varsigma_3 = \varsigma_\tau \), \( R \) is just the standard Dixon-Sylvester resultant matrix of order \( 6\varsigma, \varsigma \) (Dixon (1908)).

**Theorem 8.**

\[ \det(R) = \text{Res}(f, g, h). \]

**Proof.** It is enough to show that \( \det(R) \) has the following three properties:

i. \( f, g, h \) have a common root \( \Rightarrow \det(R) = 0. \)

ii. \( \det(R) \) has the same degrees in the coefficients of \( f, g, h \) as \( \text{Res}(f, g, h). \)

iii. \( \det(R) \) is not identically zero.

We now prove these three properties.

i. \( f, g, h \) have a common root \( \Rightarrow \det(R) = 0. \)

Suppose that \( f(s, u; t, v), g(s, u; t, v), h(s, u; t, v) \) have a common root \((s_0, u_0; t_0, v_0) \in \mathbb{CP}^1 \times \mathbb{CP}^1. \)
\( \mathbb{CP}^1 \times \mathbb{CP}^1 \). Then by Equation (8)
\[
\begin{pmatrix}
0 \\
\vdots \\
0 \\
0 \\
\vdots \\
0 \\
0 \\
\vdots \\
0
\end{pmatrix}
= R \cdot 
\begin{pmatrix}
\left( s_0 s_1 + s_1 s_2 - 1 \right) t_0^{2\tau - 1} \\
\left( s_0 s_1 + s_1 s_2 - 1 \right) t_0^{2\tau - 2} \\
\vdots \\
\left( s_0 s_1 + s_1 s_2 - 1 \right) t_0^{2\tau - 1} \\
\left( s_0 s_1 + s_1 s_2 - 2 \right) u_0 t_0^{2\tau - 1} \\
\vdots \\
\vdots \\
\left( s_0 s_1 + s_1 s_2 - 1 \right) t_0^{2\tau - 1} \\
\left( s_0 s_1 + s_1 s_2 - 2 \right) u_0 t_0^{2\tau - 1}
\end{pmatrix}.
\]

Therefore the columns of \( R \) are linearly dependent, so \( \det(R) = 0 \). Hence \( \text{Res}(f, g, h) \) divides \( \det(R) \).

ii. \( \det(R) \) has the same degree in the coefficients of \( f, g, h \) as \( \text{Res}(f, g, h) \).

Let \( \deg_f(R), \deg_g(R), \deg_h(R) \) denote the degree of \( R \) in the coefficients of \( f, g, h \) and let \( \deg_f(\text{Res}(f, g, h)), \deg_g(\text{Res}(f, g, h)), \deg_h(\text{Res}(f, g, h)) \) denote the degree of \( \text{Res}(f, g, h) \) in the coefficients of \( f, g, h \). Then by construction:

\[
\deg_f(R) = (\varsigma_1 + \varsigma_2)\tau, \\
\deg_g(R) = (\varsigma_1 + \varsigma_3)\tau, \\
\deg_h(R) = (\varsigma_1 + \varsigma_2)\tau.
\]

Moreover by (Cox, Little and O’Shea (1998))

\[
\deg_f(\text{Res}(f, g, h)) = MV(\text{NP}(g), \text{NP}(h)), \\
\deg_g(\text{Res}(f, g, h)) = MV(\text{NP}(f), \text{NP}(h)), \\
\deg_h(\text{Res}(f, g, h)) = MV(\text{NP}(f), \text{NP}(g)),
\]

where \( \text{NP} \) denotes a Newton Polygon and \( \text{MV} \) denotes the mixed volume. But by (Goldman (2003))

\[
MV(\text{NP}(g), \text{NP}(h)) = (\varsigma_1 + \varsigma_3)\tau, \\
MV(\text{NP}(f), \text{NP}(h)) = (\varsigma_1 + \varsigma_3)\tau, \\
MV(\text{NP}(f), \text{NP}(g)) = (\varsigma_1 + \varsigma_2)\tau.
\]

Therefore \( \det(R) \) has the same degree in the coefficients of \( f, g, h \) as \( \text{Res}(f, g, h) \). Since \( \text{Res}(f, g, h) \) divides \( \det(R) \), it follows that there is a constant \( c \) such that \( \det(R) = c\text{Res}(f, g, h) \). It remains only to show that \( c \neq 0 \) or equivalently that \( \det(R) \) is not identically zero.
Jia and Goldman (2009)). Therefore in this section we shall consider only those space

5. Singularities and resultants

Clearly these three polynomials have no common root in \( \mathbb{C}P^1 \times \mathbb{C}P^1 \). We will now prove that for these three polynomials \( \det(R) \neq 0 \). Observe that

\[
\begin{pmatrix}
\tau_1^{s_3 + s_1 - 1} f \\
\vdots \\
\tau_1^{s_3 + s_1 - 1} g
\end{pmatrix}
= I_{(s_3 + s_1) \tau} \cdot s_1 t^\tau
\begin{pmatrix}
\tau_1^{s_3 + s_1 - 1} f \\
\vdots \\
\tau_1^{s_3 + s_1 - 1} g
\end{pmatrix},
\]

where \( I_k \) denotes the \( k \times k \) identity matrix. Moreover,

\[
\begin{pmatrix}
\tau_1^{s_3 + s_1 - 1} f \\
\vdots \\
\tau_1^{s_3 + s_1 - 1} g
\end{pmatrix} = (A_{(s_3 + s_1) \tau} \cdot I_{(s_3 + s_1) \tau} \cdot C_{(s_3 + s_1) \tau}) \cdot (g_a \ g_b \ g_c),
\]

where \( A_{(s_3 + s_1) \tau}, C_{(s_3 + s_1) \tau} \) are two coefficient matrices with sizes \( (s_3 + s_1) \tau \times (s_3 + s_1) \tau \), \( (s_1 + s_2) \tau \times (s_1 + s_2) \tau \), and

\[
\begin{align*}
A & = \tau_1^{s_3 + s_1 - 1} f (s^{s_3 + s_1 - 1} \tau - 1, \ldots, s^{s_3 + s_1 - 1} \tau - 1, \ldots, s^{s_3 + s_1 - 1} \tau - 1), \\
C & = \tau_1^{s_3 + s_1 - 1} g (s^{s_3 + s_1 - 1} \tau - 1, \ldots, s^{s_3 + s_1 - 1} \tau - 1, \ldots, s^{s_3 + s_1 - 1} \tau - 1).
\end{align*}
\]

Thus after some elementary column operations, we get

\[
\det(R) = \det \begin{pmatrix}
I_{(s_3 + s_1) \tau} & 0 & 0 \\
A & I_{(s_1 + s_3) \tau} & C \\
0 & 0 & I_{(s_1 + s_2) \tau}
\end{pmatrix},
\]

so \( \det(R) = \pm 1 \). Hence \( \det(R) \) is not identically zero. Therefore \( \det(R) \) is equal to \( \text{Res}(f, g, h) \) up to a nonzero constant multiple. □

5. Singularities and resultants

It is easy to find the singularities of a space curve of type \((1, 1, n - 2)\) - see (Wang, Jia and Goldman (2009)). Therefore in this section we shall consider only those space
curves that satisfy \( \mu_1 + \mu_2 \geq 3 \).

Let \( \mathbf{P}(s, u) \) be a parametrization of a degree \( n \) rational space curve with a \( \mu \)-basis \( \mathbf{p}(s, u), \mathbf{q}(s, u), \mathbf{r}(s, u) \) such that \( \text{deg}_{u}(\mathbf{p}(s, u)) = \mu_1, \text{deg}_{u}(\mathbf{q}(s, u)) = \mu_2, \text{deg}_{u}(\mathbf{r}(s, u)) = \mu_3, \) and \( \mu_1 \leq \mu_2 \leq \mu_3 \). Recall that by Theorem 7, the space curve given by the
parametrization \( \mathbf{P}(s, u) \) has a singularity if and only if the three polynomials

- \( F(s, u; t, v) \)-bidegree\((\mu_1 - 1, n - 1)\)
- \( G(s, u; t, v) \)-bidegree\((\mu_2 - 1, n - 1)\)
- \( H(s, u; t, v) \)-bidegree\((\mu_3 - 1, n - 1)\)

have a common root — that is, if and only if \( \text{Res}(F, G, H) = 0 \).

By Equation (8), we can construct the resultant matrix \( R \) of \( F, G, H \) in the following fashion: let \( c_1 = \mu_1 - 1, c_2 = \mu_2 - 1, c_3 = \mu_3 - 1 \), and \( \tau = n - 1 \).

1. multiply \( F(s, u; t, v) \) by the monomials \( s^{\phi_1} \mu_1 - 1 t^{\phi_2} \mu_2 - 1, \) where \( i = 1, \ldots, c_2 + 1 \) and \( j = 1, \ldots, \tau \);
2. multiply \( G(s, u; t, v) \) by the monomials \( s^{\phi_1} \mu_1 - 1 t^{\phi_2} \mu_2 - 1, \) where \( i = 1, \ldots, c_2 + 1 \) and \( j = 1, \ldots, \tau \);
3. multiply \( H(s, u; t, v) \) by the monomials \( s^{\phi_1} \mu_1 - 1 t^{\phi_2} \mu_2 - 1, \) where \( i = 1, \ldots, c_2 + 1 \) and \( j = 1, \ldots, \tau \);

This approach generates \( 2\tau \) polynomials, where \( \zeta = c_1 + c_2 + c_3 \). If we put the coefficients of these polynomials into a matrix, we get a square matrix \( R \).

\[
\begin{pmatrix}
(s^{\phi_1} \mu_1 - 1 t^{\phi_2} \mu_2 - 1, \ldots, u^{\phi_1} \mu_1 - 1 v^{\phi_2} \mu_2 - 1)T, \\
(s^{\phi_1} \mu_1 - 1 t^{\phi_2} \mu_2 - 1, \ldots, u^{\phi_1} \mu_1 - 1 v^{\phi_2} \mu_2 - 1)T, \\
(s^{\phi_1} \mu_1 - 1 t^{\phi_2} \mu_2 - 1, \ldots, u^{\phi_1} \mu_1 - 1 v^{\phi_2} \mu_2 - 1)T
\end{pmatrix}
= R:
\begin{pmatrix}
(s^{\phi_1} \mu_1 - 1 t^{\phi_2} \mu_2 - 1)R_1 \\
(s^{\phi_1} \mu_1 - 1 t^{\phi_2} \mu_2 - 1)R_2 \\
(s^{\phi_1} \mu_1 - 1 t^{\phi_2} \mu_2 - 1)R_3
\end{pmatrix}
\]

Since \( \zeta = c_1 + c_2 + c_3 = \mu_1 + \mu_2 + \mu_3 - 3 \) and \( \mu_1 + \mu_2 + \mu_3 = \text{deg}(\mathbf{P}) = n \), \( R \) is a resultant matrix for the polynomials \( F, G, H \) of size \( 2(n - 3)(n - 1) \times 2(n - 3)(n - 1) \).

**Theorem 9.** The space curve given by the parametrization \( \mathbf{P}(s, u) \) is singular if and only if \( \text{det}(R) = 0 \).

**Proof.** This result is an immediate consequence of Theorem 7 and Theorem 8. \( \square \)

**Remark:** The matrix \( R \) can be generated in two steps. First, define a matrix \( RM_1 \) whose entries depend on \( t \):

\[
\begin{pmatrix}
(s^{\phi_1} \mu_1 - 1 t^{\phi_2} \mu_2 - 1, \ldots, u^{\phi_1} \mu_1 - 1 v^{\phi_2} \mu_2 - 1)T, \\
(s^{\phi_1} \mu_1 - 1 t^{\phi_2} \mu_2 - 1, \ldots, u^{\phi_1} \mu_1 - 1 v^{\phi_2} \mu_2 - 1)T, \\
(s^{\phi_1} \mu_1 - 1 t^{\phi_2} \mu_2 - 1, \ldots, u^{\phi_1} \mu_1 - 1 v^{\phi_2} \mu_2 - 1)T
\end{pmatrix}
= RM_1 \cdot \begin{pmatrix}
(s^{\phi_1} \mu_1 - 1 t^{\phi_2} \mu_2 - 1)R_1 \\
(s^{\phi_1} \mu_1 - 1 t^{\phi_2} \mu_2 - 1)R_2 \\
(s^{\phi_1} \mu_1 - 1 t^{\phi_2} \mu_2 - 1)R_3
\end{pmatrix}
\]

where \( \text{size}(RM_1) = 2(c_1 + c_2 + c_3) \times (c_1 + c_2 + c_3) = 2(n - 3) \times (n - 3) \). Since the entries are polynomials with degree \( n - 1 \) in \( t \), construct

\[
RM_2 := [t^{\phi_2} \mu_2 - 1, \ldots, t^{\phi_2} \mu_2 - 1]T \otimes RM_1.
\]

Here for a column matrix \( C = (c_1, \ldots, c_\alpha)^T \) and a rectangular matrix \( M = (m_{ij}) \),

\[
(C \otimes M)_{(i-1)d+k,j} = (c_k m_{ij}).
\]
Then the intersection multiplicity of $f$ and let $S$ be the ideal of $C[\mathbf{s}, \mathbf{t}]$ generated by $s, t$. By Bezout's theorem, if $f(s, t), g(s, t)$ be two bivariate polynomials with no common factors, and let $S^* = (s^*, t^*)$ be a common root of $f(s, t)$ and $g(s, t)$. Denote by $(f(s, t), g(s, t))$ the ideal of $C[\mathbf{s}, \mathbf{t}]$ generated by $f(s, t), g(s, t)$. Then the intersection multiplicity of $f(s, t), g(s, t)$ at $S^* = (s^*, t^*)$ is given by

$$I_{S^*}(f, g) = \dim(C[\mathbf{s}, \mathbf{t}]/(f, g))_{S^*}.$$ 

that is, the dimension of the quotient localized at $S^*$, where

$$(C[\mathbf{s}, \mathbf{t}]/(f, g))_{S^*} = \frac{(h_1)}{h_2}h_1, h_2 \in C[\mathbf{s}, \mathbf{t}]/(f, g), h_2(S^*) \neq 0).$$

The total intersection multiplicity is

$$I(f, g) = \sum_{(s^*, t^*)} I_{(s^*, t^*)}(f, g),$$

where the sum is taken all the common roots of $f(s, t), g(s, t)$.

By Bezout's theorem, if $f(s, t), g(s, t)$ have bidegrees $(m_1, n_1), (m_2, n_2)$, then $I(f, g) = m_1n_2 + m_2n_1$.

**Definition 11.** Similarly, let $F(s, t), G(s, t), H(s, t)$ be three bivariate polynomials with no common factors, and let $S^* = (s^*, t^*)$ be a common root of $F(s, t), G(s, t), H(s, t)$. Denote by $(F(s, t), G(s, t), H(s, t))$ the ideal of $C[\mathbf{s}, \mathbf{t}]$ generated by $F(s, t), G(s, t), H(s, t)$. Then the intersection multiplicity of $F(s, t), G(s, t), H(s, t)$ at $S^* = (s^*, t^*)$ is given by

$$I_{S^*}(F(s, t), G(s, t), H(s, t)) = \dim(C[\mathbf{s}, \mathbf{t}]/(F(s, t), G(s, t), H(s, t))_{S^*}).$$

Once again the total intersection multiplicity is

$$I(F, G, H) = \sum_{(s^*, t^*)} I_{(s^*, t^*)}(F, G, H),$$

Thus $RM_2$ is of size $2(n - 3)(n - 1) \times (n - 3)$ with entries of degree $2n - 3$ in $t$. Now eliminate the parameter $t$ from the matrix $RM_2$ by expanding each entry $RM_2(i, j)$ to a row vector $[RM_2(i, j), 2n - 3], \ldots, RM_2(i, j, 0)]$, where $RM_2(i, j, k)$ is the coefficient of $t^k$ in the polynomial $RM_2(i, j)$. The column size is multiplied by $2n - 2$, so we get a numerical square matrix which is the matrix $R$ we just constructed. Busé and Liu Ba (2010) uses a submatrix of $RM_1$ to analyze the singularities of the curve parametrized by $P(s, u)$ whereas we focus on the matrix $R$.  

5.1. Intersection multiplicity for planar algebraic curves

In this section we briefly review the formal notion of intersection multiplicity for two and three planar algebraic curves.

Consider the polynomial ring $C[\mathbf{s}, \mathbf{t}]$. Fix a point $S^* = (s^*, t^*)$. A basic local invariant of the point $S^*$ is its local ring

$$C[\mathbf{s}, \mathbf{t}]_{S^*} = \{ f/g | f, g \in C[\mathbf{s}, \mathbf{t}], g(S^*) \neq 0 \}.$$ 

$C[\mathbf{s}, \mathbf{t}]_{S^*}$ is a subring of the field $C(s, t)$. This construction can be applied to an arbitrary commutative function ring $A$: $A$ localized at $S^*$ is $A_{S^*} = \{ f/g | f, g \in A, g(S^*) \neq 0 \}$, see (Shafarevich (1994)).

**Definition 10.** Let $f(s, t), g(s, t)$ be two bivariate polynomials with no common factors, and let $S^* = (s^*, t^*)$ be a common root of $f(s, t)$ and $g(s, t)$. Denote by $(f(s, t), g(s, t))$ the ideal of $C[\mathbf{s}, \mathbf{t}]$ generated by $f(s, t), g(s, t)$. Then the intersection multiplicity of $f(s, t), g(s, t)$ at $S^* = (s^*, t^*)$ is given by

$$I_{S^*}(f, g) = \dim(C[\mathbf{s}, \mathbf{t}]/(f, g))_{S^*}.$$ 

- that is, the dimension of the quotient localized at $S^*$, where

$$(C[\mathbf{s}, \mathbf{t}]/(f, g))_{S^*} = \left\{ \frac{h_1}{h_2}h_1, h_2 \in C[\mathbf{s}, \mathbf{t}]/(f, g), h_2(S^*) \neq 0 \right\}.$$ 

The total intersection multiplicity is

$$I(f, g) = \sum_{(s^*, t^*)} I_{(s^*, t^*)}(f, g),$$

where the sum is taken all the common roots of $f(s, t), g(s, t)$.
Proposition 12. Let $f_1(s, t)$, $f_2(s, t)$, $g(s, t)$ and $h(s, t)$ be polynomials vanishing at $S^* = (s^*, t^*)$, such that gcd($h, g) = 1$ and gcd($f_1, f_2, g) = 1$. Then

$$I_{S^*}(f_1 h, f_2 h, g) = I_{S^*}(h, g) + I_{S^*}(f_1, f_2, g).$$

Proof. Let $R = C[s, t]/(g)$. Multiplication by $h$ is an $R$-linear map:

$$m_h : R/(f_1, f_2) → R/(f_1 h, f_2 h)$$

with image $(h)$. We claim that $m_h$ is injective. Indeed,

$$\ker(m_h) = \{ p : hp = af_1 h + bf_2 h + cg \},$$

so $g(h(p - af_1 - bf_2))$. Since by assumption $g$ has no factor dividing $h$, we have $g(p - af_1 - bf_2)$. Hence $p$ is trivial in $R/(f_1, f_2)$. Since $m_h$ is injective, the rank-nullity theorem gives

$$\dim(R/(f_1, f_2)) + \dim(R/(h)) = \dim(R/(f_1 h, f_2 h)),$$

which implies that $I_{S^*}(f_1 h, f_2 h, g) = I_{S^*}(h, g) + I_{S^*}(f_1, f_2, g)$. $\square$

5.2. Intersection multiplicity for the singularities of rational space curves

Let $Q$ be a singular point on the rational space curve represented by the parametrization $P(s, u)$, and let $(s_i, u_i), i = 1, ..., k$ be all the distinct homogeneous parameters corresponding to the point $Q$. Based on Theorem 7, we can define the intersection multiplicity of $F(s, u; t, v) = 0$, $G(s, u; t, v) = 0$ and $H(s, u; t, v) = 0$ contributed by the singularity $Q$ as

$$I_Q(F, G, H) \triangleq \sum_{i,j} I_{S_{ij}}(F, G, H),$$

where $S_{ij} = (s_i, u_i; s_j, u_j), i, j = 1, ..., k$.

Theorem 13. The intersection multiplicity of $F, G, H$ gives the proper multiplicity for each singularity $Q$ on the curve represented by the parametrization $P(s, u)$:

$$I_Q(F, G, H) = \sum_{Q^*} \nu_{Q^*}(\nu_{Q^*} - 1),$$

where $\nu_{Q^*}$ denotes the multiplicity of an infinitely near point $Q^*$ of the singular point $Q$, and the sum is taken over all the infinitely near singularities of $Q$ including $Q$ itself.

In order to prove Theorem 13, we first need some lemmas. Let $\tilde{p}, \tilde{q}, \tilde{r}$ be three syzygies that are linearly independent for any parameter $(s, u)$ corresponding to the singularity $Q$. Construct three polynomials $\tilde{F}, \tilde{G}, \tilde{H}$ in the same way as $F, G, H$. Then for each singularity $Q$ on the space curve given by the parametrization $P(s, u)$, we have:

Lemma 14.

$$I_Q(F, G, H) = I_Q(\tilde{F}, \tilde{G}, \tilde{H}).$$
Proof. Since $\tilde{p}, \tilde{q}, \tilde{r}$ are syzygies for the curve given by the parametrization $P(s, u)$, there must be polynomials $\alpha_i(s, u), \beta_i(s, u), \gamma_i(s, u), i = 1, 2, 3$ such that

$$\tilde{p} = \alpha_1(s, u)P(s, u) + \alpha_2(s, u)Q(s, u) + \alpha_3(s, u)r(s, u),$$

$$\tilde{q} = \beta_1(s, u)P(s, u) + \beta_2(s, u)Q(s, u) + \beta_3(s, u)r(s, u),$$

$$\tilde{r} = \gamma_1(s, u)P(s, u) + \gamma_2(s, u)Q(s, u) + \gamma_3(s, u)r(s, u).$$

Since $\tilde{p}, \tilde{q}, \tilde{r}$ are linearly independent for any parameter $(s, u)$ corresponding to the singularity $Q$,

$$\begin{vmatrix}
\alpha_1(s, u) & \alpha_2(s, u) & \alpha_3(s, u) \\
\beta_1(s, u) & \beta_2(s, u) & \beta_3(s, u) \\
\gamma_1(s, u) & \gamma_2(s, u) & \gamma_3(s, u)
\end{vmatrix} \neq 0$$

for all parameters $(s, u)$ corresponding to the point $Q$. Therefore since

$$\tilde{F} = \alpha_1(s, u)F(s, u; t, v) + \alpha_2(s, u)G(s, u; t, v) + \alpha_3(s, u)H(s, u; t, v),$$

$$\tilde{G} = \beta_1(s, u)F(s, u; t, v) + \beta_2(s, u)G(s, u; t, v) + \beta_3(s, u)H(s, u; t, v),$$

$$\tilde{H} = \gamma_1(s, u)F(s, u; t, v) + \gamma_2(s, u)G(s, u; t, v) + \gamma_3(s, u)H(s, u; t, v),$$

we conclude that

$$I_Q(F, G, H) = I_Q(\tilde{F}, \tilde{G}, \tilde{H}).$$

Therefore, to prove Theorem 13, we can examine another three obvious syzygies for the curve given by the parametrization $P(s, u)$. Without loss of generality, we shall assume that the singularity $Q = (0, 0, 0, 1)$. Then the curve has the following parametrization:

$$P(s, u) = (a(s, u)h(s, u), b(s, u)h(s, u), c(s, u)h(s, u), d(s, u)),$$

where $gcd(a, b, c) = 1, gcd(h, d) = 1, gcd(a, h) = 1$, and $h(s, u)$ is the inversion formula for the singular point $Q$. Now we have the following three syzygies that are linearly independent for any parameter $(s, u)$ corresponding to $Q$:

$$L(s, u) = (-c, 0, a, 0), M(s, u) = (-b, a, 0, 0), N(s, u) = (-d, 0, 0, ah).$$

We construct three polynomials from the syzygies $L, M, N$:

$$L(s, u; t, v) = \frac{L(s, u) \cdot P(t, v)}{sv - tu} = \frac{a(s, u)c(t, v) - c(s, u)a(t, v)}{sv - tu}h(t, v) = L(s, u; t, v)h(t, v),$$

$$M(s, u; t, v) = \frac{M(s, u) \cdot P(t, v)}{sv - tu} = \frac{a(s, u)b(t, v) - b(s, u)a(t, v)}{sv - tu}h(t, v) = M(s, u; t, v)h(t, v),$$

$$N(s, u; t, v) = \frac{N(s, u) \cdot P(t, v)}{sv - tu} = \frac{a(s, u)b(s, u)d(t, v) - a(t, v)h(t, v)d(s, u)}{sv - tu}.$$

Lemma 15. Suppose that $Q = (0, 0, 0, 1)$ is an order $m$ singularity. Then

$$I_Q(h(t, v), N(s, u; t, v)) = m(m - 1).$$
Proof. Let \((s_i, u_i)\) be all the distinct parameters corresponding to the point \(Q\) and let \(S_{ij} = (s_i, u_i; s_j, u_j)\). If \(m_i\) is the multiplicity of \((s_i, u_i)\) as a root of \(h(s, u)\), then

\[
I_{S_{ij}}(h, N) = I_{S_{ij}}(h(t, v), a(s, u)d(t, v) - a(t, v)d(s, u) h(t, v) + a(s, u)d(t, v) h(s, u) - h(t, v) h(s, u) - h(t, v) )_{sv - tu} = I_{S_{ij}}(h(t, v), a(s, u)d(t, v) h(s, u) - h(t, v)_{sv - tu} = I_{S_{ij}}(h(t, v), h(s, u) - h(t, v)_{sv - tu} = \left\{ \begin{array}{ll} m_i(m_i - 1), & i = j \\ m_i m_j, & i \neq j \end{array} \right.
\]

Therefore

\[
I_Q(h, N) = \sum_{i,j} I_{S_{ij}}(h, N) = \sum_{i=1}^{k} m_i (m_i - 1) + \sum_{i \neq j} m_i m_j = \sum_{i=1}^{k} m_i m_j - \sum_{i=1}^{k} m_i = m^2 - m = m(m - 1).
\]

\(\square\)

**Theorem 16.** Let \(\nu_{Q^*}\) denote the multiplicity of an infinitely near point \(Q^*\) of a singular point \(Q\). Then

\[
I_Q(L, M, N) = \sum_{Q^*} \nu_{Q^*} (\nu_{Q^*} - 1),
\]

where the sum is taken over all the infinitely near singularities of \(Q\) including \(Q\) itself.

*Proof.* Without loss of generality, we can assume that \(Q = (0, 0, 0, 1)\). Set

\[
P^0 = P = (ah, bh, ch, d),
\]

where \(gcd(a, b, c) = 1, gcd(h, d) = 1\). We can also make a coordinate transformation so that \(gcd(a, h) = 1\). Set \(a_0 = a, b_0 = b, c_0 = c, d_0 = d, h_0 = h\). We assume that the curve given by the parametrization \(P^0(s, u)\) has no infinitely near singularities after \(k\) blow ups, and we prove the theorem by induction on \(k\). Blowing up the curve given by the parametrization \(P^0(s, u)\) at the singularity \(Q = (0, 0, 0, 1)\), we get

\[
P^1(s, u) = (a_0^2 h_0, b_0 d_0, c_0 d_0, a_0 d_0).
\]  

(10)

Assume that \(Q^*\) is a singular point related to \(Q\). To blow up the curve given by the parametrization \(P^1(s, u)\) at the singularity \(Q^*\), we translate the coordinates so that the point \(Q^*\) is moved to \((0, 0, 0, 1)\). Then we have the following parametrization

\[
P^1(s, u) = (a_1 h_1, b_1 h_1, c_1 h_1, d_1),
\]  

(11)

where \(gcd(a_1, b_1, c_1) = 1, gcd(h_1, d_1) = 1\), and the roots of \(h_1\) are the parameters of the point \(Q^*\) with the correct multiplicity.
There are three obvious syzygies for the parametrization $\mathbf{P}^1(s, u)$:
\[
\begin{align*}
    S_1(s, u) & \triangleq (0, a_0, 0, -b_0), \\
    T_1(s, u) & \triangleq (0, 0, a_0, -c_0), \\
    U_1(s, u) & \triangleq (d_0, 0, 0, -a_0 h_0).
\end{align*}
\]

We construct three polynomials from $S_1(s, u), T_1(s, u)$ and $U_1(s, u)$:
\[
\begin{align*}
    S_1(s, u; t, v) & \triangleq \frac{S_1(s, u) \cdot \mathbf{P}^1(t, v)}{sv - tu} = \frac{a_0(s, u)b_0(t, v) - b_0(s, u)a_0(t, v)}{sv - tu} d_0(t, v), \\
    T_1(s, u; t, v) & \triangleq \frac{T_1(s, u) \cdot \mathbf{P}^1(t, v)}{sv - tu} = \frac{a_0(s, u)c_0(t, v) - c_0(s, u)a_0(t, v)}{sv - tu} d_0(t, v), \\
    U_1(s, u; t, v) & \triangleq \frac{U_1(s, u) \cdot \mathbf{P}^1(t, v)}{sv - tu} = \frac{d_0(s, u)a_0(t, v)b_0(t, v) - a_0(s, u)h_0(s, u)d_0(t, v)}{sv - tu} a_0(t, v).
\end{align*}
\]

There are also three obvious syzygies for parametrization $\tilde{\mathbf{P}}^1(s, u)$:
\[
\begin{align*}
    L_1(s, u) & \triangleq (c_1, 0, -a_1, 0), \\
    M_1(s, u) & \triangleq (b_1, -a_1, 0, 0), \\
    N_1(s, u) & \triangleq (d_1, 0, 0, -a_1 h_1).
\end{align*}
\]

Define:
\[
\begin{align*}
    L_1(s, u; t, v) & \triangleq \frac{L_1(s, u) \cdot \tilde{\mathbf{P}}^1(t, v)}{sv - tu} = \frac{c_1(s, u)a_1(t, v) - a_1(s, u)c_1(t, v)}{sv - tu} h_1(t, v) \\
                     & = \frac{L_1(s, u; t, v)h_1(t, v),}{sv - tu} \\
    M_1(s, u; t, v) & \triangleq \frac{M_1(s, u) \cdot \tilde{\mathbf{P}}^1(t, v)}{sv - tu} = \frac{b_1(s, u)a_1(t, v) - a_1(s, u)b_1(t, v)}{sv - tu} h_1(t, v) \\
                     & = \frac{M_1(s, u; t, v)h_1(t, v),}{sv - tu} \\
    N_1(s, u; t, v) & \triangleq \frac{N_1(s, u) \cdot \tilde{\mathbf{P}}^1(t, v)}{sv - tu} = \frac{d_1(s, u)a_1(t, v)h_1(t, v) - a_1(s, u)h_1(s, u)d_1(t, v)}{sv - tu} h_1(t, v).
\end{align*}
\]

Note that $S_1(s, u), T_1(s, u), U_1(s, u)$ and $L_1(s, u), M_1(s, u), N_1(s, u)$ are both independent collections of syzygies (for the parameters corresponding to the point $Q = (0, 0, 0, 1)$). By Lemma 14, for each infinitely near point $Q^*$ in the first neighborhood of the point $Q$,
\[
I_{Q^*}(S_1, T_1, U_1) = I_{Q^*}(L_1, M_1, N_1) = I_{Q^*}(L_1, M_1, N_1) + I_{Q^*}(h_1, N_1) \quad (12)
\]

where the second equality follows from Proposition 12. Let
\[
\begin{align*}
    L_0(s, u; t, v) & \triangleq L(s, u; t, v) = \frac{c_0(s, u)a_0(t, v) - a_0(s, u)c_0(t, v)}{sv - tu} h_0(t, v) \\
                    & = \frac{L_0(s, u; t, v)h_0(t, v),}{sv - tu} \\
    M_0(s, u; t, v) & \triangleq M(s, u; t, v) = \frac{b_0(s, u)a_0(t, v) - a_0(s, u)b_0(t, v)}{sv - tu} h_0(t, v) \\
                    & = \frac{M_0(s, u; t, v)h_0(t, v),}{sv - tu} \\
    N_0(s, u; t, v) & \triangleq N(s, u; t, v) = \frac{d_0(s, u)a_0(t, v)h_0(t, v) - a_0(s, u)h_0(s, u)d_0(t, v)}{sv - tu} h_0(t, v).
\end{align*}
\]

A parameter pair $(s, u; t, v)$ corresponds to an infinitely near singularity in the first neighborhood of $Q$ if and only if $L_0(s, u; t, v) = 0$, $M_0(s, u; t, v) = 0$, $N_0(s, u; t, v) = 0$. Hence
the intersection of $L_0(s, u; t, v), M_0(s, u; t, v), N_0(s, u; t, v) = 0$ provides all the parameters of infinitely near singular points in the first neighborhood of $Q$ whereas the intersection of $h_0(t, v) = 0$ provides all the parameters corresponding to the singularity $Q$. Comparing the expressions for $L_0, M_0, N_0$ and $S_1, T_1, U_1$ and using the fact that $\gcd(a(s, u), h(s, u)) = 1, \gcd(d(s, u), h(s, u)) = 1$, we find that

$$I_Q(S_1, T_1, U_1) = I_Q(L_0d_0(t, v), M_0d_0(t, v), N_0d_0(t, v))$$

$$= I_Q(L_0, M_0, N_0) + I_Q(d_0(t, v), N_0)$$

$$= I_Q(L_0, M_0, N_0).$$

Thus

$$I_Q(L_0, M_0, N_0) = \sum_{Q^*} I_Q^*(S_1, T_1, U_1),$$

where the sum is taken over all the infinitely near singularities $Q^*$ in the first neighborhood of $Q$. From Equation 12 and Lemma 15, we find that

$$I_Q(L_0, M_0, N_0) = \sum_{Q^*} (I_Q^*(L_1, M_1, N_1) + I_Q^*(h_1(t, v), N_1))$$

$$= \sum_{Q^*} (I_Q^*(L_1, M_1, N_1) + \nu_{Q^*}(\nu_{Q^*} - 1)).$$

For each infinitely near singularity $Q^*$ in the first neighborhood of $Q$, continue to examine $I_Q^*(L_1, M_1, N_1)$ by blowing up the curve $P^1(s, u)$ at the point $Q^*$. After $k$ blow ups we will conclude that

$$I_Q(L_0, M_0, N_0) = \sum_{Q^*} \nu_{Q^*}(\nu_{Q^*} - 1),$$

where the sum is taken over all the infinitely near singularities in all the neighborhoods of the point $Q$ (not including $Q$ itself). Finally,

$$I_Q(L_0, M_0, N_0) = I_Q(L_0, M_0, N_0) + I_Q(h_0, N_0) = \sum_{Q^*} \nu_{Q^*}(\nu_{Q^*} - 1),$$

where the sum is taken over all the infinitely near singularities in all the neighborhoods of the point $Q$ including $Q$ itself. $\square$

Theorem 13 follows directly from Theorem 16 because

$$I_Q(F, G, H) = I_Q(L, M, N) = \sum_{Q^*} \nu_{Q^*}(\nu_{Q^*} - 1).$$

Also we get

$$I(F, G, H) = \sum_{Q} \nu_{Q}(\nu_{Q} - 1),$$

where the sum is taken over all the singular points including all the infinitely near singularities.

The expression $\sum_{Q} \nu_{Q}(\nu_{Q} - 1)$ describes the total multiplicity of all the singularities, which is an important geometric invariant. Using $\mu$-bases, we can bound this expression for space curves of degree $n$. 

17
Theorem 17.  
\[ I(F, G, H) = \sum_Q \nu_Q (\nu_Q - 1) \leq (n-1)(\mu_1 + \mu_3 - 2) \leq (n-1)(n-2). \]

Proof. We can assume that \( \mu_1 \geq 1 \), since by assumption the curve given by the parametrization \( P(s, t) \) is a non-planar curve. By construction, \( F \) has bidegree \( (\mu_1 - 1, n-1) \), \( G \) has bidegree \( (\mu_2 - 1, n-1) \) and \( H \) has bidegree \( (\mu_3 - 1, n-1) \). If \( \gcd(F, G) = 1 \), by Bezout’s Theorem, \[ I(F, G, H) \leq I(F, G) = (\mu_1 + \mu_2 - 2)(n-1). \]

On the other hand, if \( F, G \) have a common component \( h(s; t, v) \) of bidegree \( (k_1, k_2) \), where \( 0 \leq k_1 \leq \mu_1 - 1, 0 \leq k_2 \leq n-1 \), then \( F = hF', G = hG', \gcd(F', G') = 1 \). So by Proposition 12

\[ I(F, G, H) = I(F', G', H) + I(h, H) \leq I(F', G') + I(h, H), \]

where \( F' \) has bidegree \( (\mu_1 - 1 - k_1, n-1-k_2) \), \( G' \) has bidegree \( (\mu_2 - 1 - k_1, n-1-k_2) \), \( h \) has bidegree \( (k_1, k_2) \), and \( H \) has bidegree \( (\mu_3 - 1, n-1) \). Moreover, \( F', G' \) have no common components and \( h, H \) have no common components, so

\[ I(F', G') = (\mu_1 - 1 - k_1)(n-1-k_2) + (\mu_2 - 1 - k_1)(n-1-k_2), \]

\[ I(h, H) = k_1(n-1) + k_2(\mu_3 - 1). \]

\[ I(F', G') + I(h, H) = (n-1)(\mu_1 + \mu_2 - 2 - k_1) + k_2(\mu_3 - \mu_1 - \mu_2 + 1 + 2k_1) = \oplus \]

(1) if \( \mu_1 + \mu_2 + 1 + 2k_1 \geq 0 \)
\[ \oplus \leq (n-1)(\mu_1 + \mu_2 - 2 - k_1) + (n-1)(\mu_3 - \mu_1 - \mu_2 + 1 + 2k_1) = (n-1)(\mu_3 - 1 + k_1) \]
\[ \leq (n-1)(\mu_1 + \mu_3 - 2). \]

(2) if \( \mu_1 + \mu_2 + 1 + 2k_1 < 0 \)
\[ \oplus \leq (n-1)(\mu_1 + \mu_2 - 2 - k_1) + 0(\mu_3 - \mu_1 - \mu_2 + 1 + 2k_1) = (n-1)(\mu_1 + \mu_2 - 2 - k_1) \]
\[ \leq (n-1)(\mu_1 + \mu_2 - 2). \]

Because \( \mu_2 \leq \mu_3 \), in both cases we get \( \oplus \leq (n-1)(\mu_1 + \mu_3 - 2) \), so
\[ I(F, G, H) \leq (n-1)(\mu_1 + \mu_3 - 2) \leq (n-1)(n-2). \]

If a degree \( n \) rational space curve has type \( (\mu_1 = 1, \mu_2 = \mu_3) \) and has just two singularities of order \( \mu_3 \) without infinitely near singular points, then \( \sum_Q \nu_Q (\nu_Q - 1) = (n-1)(\mu_1 + \mu_3 - 2) \). So \( (n-1)(\mu_1 + \mu_3 - 2) \) is a tight upper bound for the total multiplicity of all the singularities.

5.3. Applications of the resultant matrix

The determinant of the resultant matrix \( R \) of \( F, G, H \) is equal to zero if and only if the polynomials \( F, G, H \) have a common root. So we expect all the solutions (counting multiplicity) of \( R \cdot X = 0 \) to be from roots of the polynomials \( F, G, H \). Indeed, every common root \((\sigma, \zeta)\) of the polynomials \( F, G, H \) corresponds to an element of the kernel of \( R \) because by Equation (9)

\[ R \cdot (\sigma^{n-4}, \zeta^{2n-3}, ..., 1)^T = 0. \]

Therefore by Theorem 13 we should expect a close connection between

\[ \text{size(kernel}(R)) = \text{size}(R) - \text{rank}(R) \text{ and } I(F, G, H) = \sum_Q \nu_Q (\nu_Q - 1). \]

In fact, this connection is even tighter than one might initially expect.
Theorem 18. Let $R$ be the resultant matrix of $F,G,H$ defined by (9). Then

$$\text{size}(R) - \text{rank}(R) = \sum Q \nu_Q (\nu_Q - 1),$$

where the sum is taken over all the singularities including infinitely near singular points.

Proof. The proof is a bit complicated, so we defer this proof to the Appendix. \qed

Next we show how to compute the singularities of a space curve from the resultant matrix $R$. First we assume that there is no singularity at $(s = 1, u = 0)$ (If there is, by a coordinate transformation the singularity can be moved to another point). Hence by assumption $F,G,H$ have no common root at $(s = 1, u = 0; t = s, v = s)$ or $(s = s, u = s; t = 1, v = 0)$. The numerical matrix $R$ is of size $2(n - 1)(n - 3)$. Let $Gauss(R)$ denote the matrix generated by applying Gaussian elimination to $R$, and set

$$Gauss(R)_i(s,t) := Gauss(R)[i] \cdot (s^{n-4}t^{2n-3}, s^{n-4}t^{2n-4}, \ldots, t, 1)^T,$$

where $Gauss(R)[i]$ is the $i$-th row of the matrix $Gauss(R)$.

Proposition 19. If $(s^*, t^*)$ is a common root of $F, G, H$, then

$$Gauss(R)_i(s^*, t^*) = 0, \quad i = 1, \ldots, 2(n - 1)(n - 3).$$

Proof. This result follows because each polynomial $Gauss(R)_i(s,t)$ is a polynomial combination of $F, G, H$. \qed

By Proposition 19, to compute all the singularities of a rational space curve, we can first find all the common roots of the two bivariate polynomials given by the last two nonzero rows of $Gauss(R)$, and then use Lemma 6 to check whether the candidate roots actually correspond to singularities on the space curve. Since these two polynomials have the lowest degree of all the nonzero polynomials in the matrix $Gauss(R)$, this algorithm is quite efficient. Our examination of many examples, however, reveals a much more efficient variation of this algorithm.

Let $r$ denote the rank of the resultant matrix $R$. The $r$-th row of the matrix $Gauss(R)$ is its last nonzero row. For the order $s > t$, $Gauss(R)_r(s,t)$ has the smallest degree among the polynomials $Gauss(R)_i(s,t)$, $i = 1, \ldots, r$, since $(s^{n-4}t^{2n-3}, s^{n-4}t^{2n-4}, \ldots, t, 1)^T$ are all the monomials with bidegree less than $(n - 4, 2n - 3)$ sorted lexicographically with $s > t$. Thus the last $2n - 2$ terms contain only a single variable: $t^{2n-3}, t^{2n-4}, \ldots, t, 1$. Therefore one might hope that if $\sum Q \nu_Q \leq 2n - 3$, then the polynomial $Gauss(R)_r(s,t)$ is a univariate polynomial in $t$ whose roots are exactly the parameters corresponding to the singularities of the rational space curve. This statement holds for all the examples we have tried so far. Moreover, when $\sum Q \nu_Q > 2n - 3$, we find that the roots of the polynomial $\text{Res}_s(Gauss(R)_r(s,t), Gauss(R)_{r-1}(s,t))$ are once again exactly the parameters corresponding to the singularities of the rational space curve. Thus we are lead to the following conjecture.

Conjecture 20. The polynomial $Gauss(R)_r(s,t)$ is a univariate polynomial in $t$ if and only if $\sum Q \nu_Q \leq 2n - 3$ where the sum is taken over all the singularities including the infinitely near singular points. Moreover in this case $Gauss(R)_r(s,t)$ is the product of the inversion formulas of all the singularities including the infinitely near singularities, and $\deg_t(Gauss(R)_r(s,t)) = \sum Q \nu_Q$. Thus the roots of $Gauss(R)_r(t) = 0$ include all the parameters corresponding to all the singularities.
• Otherwise, define $\text{Gauss}(R)_{r,r-1}(t) = \text{Res}_t(\text{Gauss}(R)_r(s,t), \text{Gauss}(R)_{r-1}(s,t))$. Then $\deg_t(\text{Gauss}(R)_{r,r-1}) = \sum Q v_Q$, and $\text{Gauss}(R)_{r,r-1}(t)$ is the product of the inversion formulas of all the singularities including the infinitely near singularities. Thus the roots of $\text{Gauss}(R)_{r,r-1}(t) = 0$ include all the parameters corresponding to all the singularities.

6. Algorithm and Examples

Next we present an algorithm for finding the singularities of a rational space curve, based on the theorems and conjecture in Section 5.

Algorithm for Finding the Singularities of a Rational Space Curve

Input: A rational space curve given by a proper parametrization

\[ P(s,u) = (a(s,u), b(s,u), c(s,u), d(s,u)). \]

1. Compute a $\mu$-basis $p(s,u), q(s,u), r(s,u)$ for $P(s,u)$.
2. Compute the three auxiliary polynomials:
   \[ F(s,u;t,v) = \frac{b(s,u)P(t,v)}{s-1}, G(s,u;t,v) = \frac{q(s,u)P(t,v)}{s-1}, H(s,u;t,v) = \frac{r(s,u)P(t,v)}{s-1}. \]
3. Set $R$ to the resultant matrix of $F, G, H$ defined by (9).
4. Perform Gaussian elimination on the rows of $R$ to get the matrix $\text{Gauss}(R)$.
5. If the last row of $\text{Gauss}(R)$ is not all zeros, there are no singularities.
   Otherwise let $r = \text{rank}(R)$, and
   \[ \text{Gauss}(R)_r(s,t) := \text{Gauss}(R)[r] \cdot (s^{n-4}t^{2n-3}, s^{n-4}t^{2n-4}, \ldots, t, 1)^T. \]
   • If $\text{Gauss}(R)_r$ is a univariate polynomial in $t$, then $\text{Gauss}(R)_r = \kappa(t-t_1)^{m_1} \ldots (t-t_l)^{m_l}; \text{ and } s = t_1, \ldots, t_l; u = 1$ correspond to the singularities of the curve.
   • Otherwise let
     \[ \text{Gauss}(R)_{r-1}(s,t) := \text{Gauss}(R)[r-1] \cdot (s^{n-4}t^{2n-3}, s^{n-4}t^{2n-4}, \ldots, t, 1)^T. \]
     Compute the resultant $R(t)$ of $\text{Gauss}(R)_r, \text{Gauss}(R)_{r-1}$ with respect to $s$. Then $R(t) = \kappa(t-t_1)^{m_1} \ldots (t-t_l)^{m_l}$, and $s = t_1, \ldots, t_l; u = 1$ correspond to the singularities of the curve.
6. Let $m = \deg(\text{Gauss}_r(R)) = m_1 + \ldots + m_l$. Use $\sum Q v_Q = m(\text{Conjecture 20})$ and $\sum Q v_Q(v_Q - 1) = \text{size}(R) - \text{rank}(R)$ to analyze the multiplicity of each root. If there are too many singularities to easily determine their multiplicities, then substitute each $t_k$ into the parametric equation for $P(s,u)$ to determine the coordinates $Q_k = P(t_k, 1)$. Then the multiplicity $v_k$ is equal to the degree of $gcd(p \cdot Q_k, q \cdot Q_k, r \cdot Q_k)$.
7. If $\sum k=1 v_k(v_k - 1) < \text{size}(R) - \text{rank}(R)$, there are infinitely near singularities. Blow up the curve at each singularity to get the infinitely near singular points. Also test whether the point $Q^s = P(s = 1, u = 0)$ corresponds to a singularity by computing the inversion formula $gcd(p \cdot Q^s, q \cdot Q^s, r \cdot Q^s)$.

Otherwise there are no infinitely near singular points.

Output: A list of singularities with their order, their infinitely near singularities (singularity tree) and the parameter values corresponding to each singularity.
Example 1: (A curve with two double points)
Consider a rational space curve with parametrization
\[ P(s, u) := (s^5, s^3(s - u)^2, s^2(s - u)^3, (s - u)^5). \]
This curve has type \((1, 2, 2)\) with a \(\mu\)-basis
\[ p = (0, s - u, -s, 0); \quad q = ((s - u)^2, -s^2, 0, 0); \quad r = (0, 0, (s - u)^2, -s^2). \]
Therefore
\[ F = t^2(t - v)^2, \quad G = (-sv + 2ts - tu)t^3, \quad H = (-sv + 2ts - tu)(t - v)^3. \]
For the resultant matrix \(R(F,G,H)\), \(\text{size} = 16, \text{rank} = 12\). After Gaussian elimination, the last nonzero row represents the polynomial: \(t^2(t - 1)^2\). So \(s = 0\) and \(s = 1\) correspond to singularities. There are two double points \(Q_1 = P(s = 0, 1) = (0, 0, 0, 1)\) and \(Q_2 = P(s = 1, 1) = (1, 0, 0, 0)\). Since
\[
\text{size} - \text{rank} = 4, \quad \sum \nu_Q(\nu_Q - 1) = 2 \ast (2 - 1) + 2 \ast (2 - 1) = 4,
\]
there are no infinitely near singular points for either of the double points \(Q_1\) or \(Q_2\).

Example 1b: (A curve with a singularity at \(P(s = 1, u = 0)\))
Consider a rational space curve with parametrization
\[ P(s, u) := (u^5, u^3(s - u)^2, u^2(s - u)^3, (s - u)^5). \]
This curve has type \((1, 2, 2)\) with a \(\mu\)-basis
\[ p = (0, s - u, -u, 0); \quad q = ((s - u)^2, -u^2, 0, 0); \quad r = (0, 0, (s - u)^2, -u^2). \]
Therefore
\[ F = v^2(t - v)^2, \quad G = (-sv^2 + stv + 3uv^2 - 3utv + u^2)(t - v)^2, \quad H = v^2(sv^2 - 6stv + 3st^2 + 6uv^2 - 6utv + 2u^2). \]
For the resultant matrix \(R(F,G,H)\), \(\text{size} = 16, \text{rank} = 12\). After Gaussian elimination, the last nonzero row represents the polynomial: \((t - 1)^2\). So \((s = 1, u = 1)\) corresponds to a double point \(Q_1 = (1, 0, 0, 0)\). But observe that
\[
\text{size} - \text{rank} = 4, \quad \sum \nu_Q(\nu_Q - 1) = 2 \ast (2 - 1) < 4,
\]
Test the point \(Q_2 = P(s = 1, u = 0) = (0, 0, 0, 1)\). Since \(\gcd(p \cdot Q_2, q \cdot Q_2, r \cdot Q_2) = u^2\), \(Q_2\) is a double point. Moreover since \(\sum \nu_Q(\nu_Q - 1) = 4 = \text{size} - \text{rank}\), there are no infinitely near singular points for either of the double points \(Q_1\) or \(Q_2\).

Example 2: (A curve with one singularity of order four)
Consider a rational space curve with parametrization
\[ P(s) := (s^7, (s^3 + u^3)(s - u)^4, (s^2 + su + u^2)(s - u)^5, (s - u)^7). \]
This curve has type \((1, 2, 4)\) with a \(\mu\)-basis
\[ p = (0, 3u - 3s, u + s, 2u + 2s); \quad q = (0, -3u^2 + 3su, -3u^2 + 3su - 2s^2, 2s^2); \quad r = (0, 0, 0, 0). \]
Therefore
\[ F = -(u - v + t^2)(t - v)^4, \quad G = (st - sv - ut)t(t - v)^4, \]
\[ H = (-s^3v^3 + 4s^3tv^2 - 6s^2t^2v + 4s^2utv^2 + 4s^2ut^2v - 6s^2ut^3 - su^2t^2v + 4su^2t^3 - u^3t^3)t^3. \]

For the resultant matrix \( R(F, G, H), \) \( \text{size} = 48, \text{rank} = 36. \) After Gaussian elimination, the last nonzero row represents the polynomial: \((t - 1)^4,\) so \( s = 1 \) corresponds to a singularity \( Q = P(s = 1) = (1, 0, 0, 0). \) Since
\[ \text{size} - \text{rank} = 12 = 4 \times 3, \deg((t - 1)^4) = 4, \]
the point \( Q \) is a singularity of order four, and there are no infinitely near singular points in the neighborhood.

**Example 3:** *(A curve with a double point that has an infinitely near double point)*

Consider a rational space curve with parametrization
\[ P(s) := (s^7, (s^5 + su^4 + u^5)(s - u)^2, (s^3 + u^3)(s - u)^4, (s - u)^7). \]

This curve has type \((2, 2, 3)\) with a \( \mu\)-basis
\[ p = (-33s^2 + 66su - 33a^3, 17s^2 + 21su - 27u^2, 103su + 27a^2 - 29s^2, 45s^2 + 43su); \]
\[ q = (0, 8s^2 - 16su + 8u^2, 20su - 19u^2 - 13s^2, -5su - 11u^2 + 5s^2); \]
\[ r = (-1125s^2u + 2250su^2 - 1125u^3, 2309s^2u - 2743su^2 + 809u^3, -2378s^3 + 3335s^2u + 701s - 809, 2378s^3 + 2615s^2 + 385s). \]

Therefore
\[ F = -57sv^6 + \ldots, \quad G = (t - v)^2(-10sv^4 + \ldots), \quad H = -4756s^2v^6 + \ldots \]

For the resultant matrix \( R(F, G, H), \) \( \text{size} = 48, \text{rank} = 44. \) After Gaussian elimination, the last nonzero row represents the polynomial: \((t - 1)^4,\) so \( s = 1 \) corresponds to the singularity \( Q = P(s = 1) = (1, 0, 0, 0). \) Since
\[ \text{size} - \text{rank} = 4 = 2 \times 1 + 2 \times 1, \deg((t - 1)^4) = 4, \]
\( Q \) is a double point and there is a double point in the first neighborhood of the point \( Q. \)

**Example 4:** *(A curve where the last nonzero row is not a univariate polynomial)*

Consider a rational space curve with parametrization
\[ P(s, u) := ((s - u)^5(s + 2u)^5, (s - u)^5(s - 2u)^5, (s + u)^5(s + 2u)^5, (s + u)^5(s - 2u)^5). \]

This curve has type \((3, 3, 4)\) with a \( \mu\)-basis
\[ p = (-2781s^3 + 34425s^2u + 13770su^2 + 8640u^3, \ldots, \ldots); \]
\[ q = (-13365s^3u - 8262u^3 - 30375su^2, \ldots, \ldots); \]
\[ r = (640s^3u + 2485s^2u^2 + 3275su^3 + 1466u^4, \ldots, \ldots). \]

Therefore
\[ F = -1536000u^2v^9 - 86400s^2v^9 - 4454400u^2t^2v^7 + \ldots, \quad G = \ldots, \quad H = \ldots. \]
For the resultant matrix $R(F, G, H)$, size = 126, rank = 94. After Gaussian elimination, the last nonzero row represents the polynomial:

$Gauss(R) := -19205s^{14} - 76592st^{12} - 2954755st^{10} - 3212171st^8 - 19884820t^6 + 3798736t^4 + 9106240t^2 + 422400s - 605t^17 - 56975t^{15} - 270405t^{13} + 1861855t^{11} + 9005214t^9 + 4630180t^7 + 26101456t^5 + 2287040t^3 - 997120t$.

$Gauss(R)$ is a bivariate polynomial, so let $Gauss(R)_{r-1}$ be the polynomial represented by the next to the last nonzero row of $Gauss(R)$,

$Gauss(R)_{r-1} = 150s^{15} - 1105st^{13} - 52099st^{11} - 2855st^9 - 301441st^7 - 6020st^5 + 112976st^3 + 11840st - 55t^{16} - 4675t^{14} - 5325t^{12} + 165155t^{10} - 3456t^8 + 389780t^6 + 103376t^4 + 15040t^2 + 14080$.

To find the common roots of $Gauss(R)_{r}, Gauss(R)_{r-1}$, compute

$Syl(Gauss(R)_{r}, Gauss(R)_{r-1}, s) = (25t^8 + 50t^6 + 1005t^4 - 1720t^2 + 1936)(121t^8 - 430t^6 + 1005t^4 + 200t^2 + 400)(t^8 + 98t^6 + 789t^4 + 392t^2 + 16)(t^8 + 2t^6 - 11t^4 + 8t^2 + 16)$. 

Therefore the roots of $(25t^8 + 50t^6 + 1005t^4 - 1720t^2 + 1936)(121t^8 - 430t^6 + 1005t^4 + 200t^2 + 400)(t^8 + 98t^6 + 789t^4 + 392t^2 + 16)(t^8 + 2t^6 - 11t^4 + 8t^2 + 16) = 0$ correspond to singularities. Since

$size - rank = 32, \sum \nu_Q = 32$

the singularities are all double points on the space curve, and there are 16 double points.

7. Conclusions

In this paper we focus on computing the intersection points for three planar algebraic curves that correspond to the parameters of singularities of rational space curves. The main technique is to construct a new sparse resultant matrix for three bivariate polynomials with bidegrees $(\varsigma_1, \tau), (\varsigma_2, \tau), (\varsigma_3, \tau)$. Using this resultant, we can compute the parameters of the singularities, and bounds for the expression $\sum_Q \nu_Q(\nu_Q - 1)$ of the total multiplicity of all the singularities including infinitely near singular points of a rational space curve.

The main advantage of our method is that our computations are based mainly on Gaussian elimination in a numerical matrix, which is a simple and stable calculation. Also, using Theorem 18, we can estimate the total multiplicities of the singularities before we actually compute the singularities. The main weakness of our technique is that the size of our resultant matrix is quite large when the degree of the curve is large. For curves of degree less than or equal to 10, our computation times are competitive with those of Shi and Chen (2010), but for larger degrees our computation times are considerably slower than these alternative techniques.

8. Acknowledgements

We would like to thank Brendan Hassett for many thoughtful conversations concerning the singularities of rational space curves. This paper is much improved both by his insight and his suggestions.

Xiaoran Shi was partially supported by a National Key Basic Research Project of China (2011CB302400), the NSF of China (11031007) and the ”111” project (b07033).
Xiaohong Jia was partially supported by a National Key Basic Research Project of China (2011CB302404), by grants from NSFC (11201463), (60821002) and (91118001) and by the National Center for Mathematics and Interdisciplinary Sciences.

References


Appendix

The purpose of this Appendix is to prove Theorem 18, using techniques from sheaf cohomology. Our inspiration is the formulation of the resultant from Gelfand et al. (2008), in the language of homological algebra. However, the argument here is self-contained and does not rely on theorems from Gelfand et al. (2008). Nevertheless, we do freely use results on schemes and sheaf cohomology from Hartshorne (1977); for the most part, we follow Hartshorne’s notation. We work over the complex numbers \( \mathbb{C} \), although most of what we do readily extends to arbitrary fields.

To fix our notation, let \( S = \mathbb{C}[s, u] \otimes \mathbb{C}[t, v] \) denote the polynomial ring interpreted as a bigraded ring, i.e.,

\[
S = \bigoplus_{(a,b) \in \mathbb{Z}^2} S_{(a,b)}, \quad S_{(a,b)} = \mathbb{C}[s, u]^a \otimes \mathbb{C}[t, v]^b,
\]

where \( S_{(a,b)} \) consists of forms homogeneous in \((s, u)\) of degree \( a \) and homogeneous in \((t, v)\) of degree \( b \), and has dimension \((a+1)(b+1)\). By convention, \( S_{(a,b)} = 0 \) if \( a < 0 \) or \( b < 0 \). For each \((d,e) \in \mathbb{Z}^2\), we have the twisted graded \( S \)-module

\[
S(d,e) = \bigoplus_{(a,b) \in \mathbb{Z}^2} S_{(a,b)}(d,e), \quad S_{(d,e)}(a,b) = S_{(d+a,e+b)}.
\]

Thus \( S(d,e) \) is isomorphic to \( S \) as an \( S \)-module, but with the grading shifted by \((d,e)\).

The main result of this Appendix is the following theorem.

**Theorem 21.** Choose forms \( F_i \in S_{(a_i,b_i)} \) for \( i = 1, 2, 3 \) without common factors in \( S \). Let \( R \) be the resultant matrix of \( F_1, F_2, \) and \( F_3 \), as defined in Section 4, and let \( I(F_1, F_2, F_3) \) denote the total multiplicity of

\[
\{F_1 = F_2 = F_3 = 0\} \subset \mathbb{P}^1 \times \mathbb{P}^1
\]

as defined in Section 5. Then

\[
\text{size}(R) - \text{rank}(R) = I(F_1, F_2, F_3).
\]

Combining this result with Theorem 13 yields Theorem 18.

To prove Theorem 21, we interpret \( Z = \{F_1 = F_2 = F_3 = 0\} \subset \mathbb{P}^1 \times \mathbb{P}^1 \) as a closed subscheme with sheaf of regular functions \( \mathcal{O}_Z \). Note that \( Z \) is zero-dimensional because \( F_1, F_2, \) and \( F_3 \) have no common factors. The scheme structure encodes algebraic data beyond the points where \( F_1, F_2, \) and \( F_3 \) all vanish, including the relevant multiplicity data. In particular, the definition of \( I(F_1, F_2, F_3) \) is expressed as the sum of the intersection multiplicities over the common zeros of \( F_1, F_2, \) and \( F_3 \), i.e.,

\[
I(F_1, F_2, F_3) = \sum_{p \in \{F_1 = F_2 = F_3 = 0\}} \dim_{\mathbb{C}}(\mathcal{O}_{Z,p}).
\]

Here \( \mathcal{O}_{Z,p} \) is the localization of \( \mathcal{O}_Z \) at the maximal ideal corresponding to \( p \).

In the following proposition, we recast the total multiplicity in terms more amenable to global computation.

**Proposition 22.** Let \( Z \) be a zero-dimensional closed subscheme. Then the following are equal:

- the degree of \( Z \), as computed with respect to any embedding \( Z \hookrightarrow \mathbb{P}^N \) into projective space;
the codimension of the subspace
\[ \Gamma(I_Z(m)) \subset \Gamma(O_{\mathbb{P}^N}(m)) \]
for \( m \gg 0 \), where \( I_Z \) is the ideal sheaf of \( Z \);
* the sum of local multiplicities \( \sum_{p \in Z} \dim_C(O_{Z,p}) \).

We use \( \deg(Z) \) to denote any of these expressions.

Thus the global definition of the degree of a projective variety is compatible with the local formulation via multiplicities. This proposition is a fundamental result in intersection theory, see (Fulton, 1998, §1.4-1.5, Ex. 2.5.2), but we offer a proof below.

**Proof.** Given a \( d \)-dimensional closed subscheme \( Z \subset \mathbb{P}^N \), consider the Euler characteristic

\[ \chi(O_{\mathbb{P}^N}(m)|Z) = \chi(O_Z(m)) = \sum_{i=0}^{N} (-1)^i h^i(O_Z(m)), \]

i.e., the alternating sum of the dimensions of the sheaf cohomology groups of \( O_Z(m) \). This expression is a polynomial \( p_Z(m) \), known as the Hilbert polynomial of \( Z \); this polynomial has leading term

\[ \deg(Z \subset \mathbb{P}^N) \frac{m^d}{d!}. \]

For \( m \gg 0 \), we have Serre vanishing (Hartshorne, 1977, III.5.2)

\[ h^i(I_Z(m)) = h^i(O_Z(m)) = 0, \quad i > 0, \]

which implies

\[ p_Z(m) = \chi(O_Z(m)) = h^0(O_Z(m)) = \text{codim}(\Gamma(I_Z(m)) \subset \Gamma(O_{\mathbb{P}^N}(m))). \]

When \( d = 0 \), \( p_Z(m) \) is constant in \( m \) and equal to the degree of \( Z \subset \mathbb{P}^N \), as well as the codimension of

\[ \Gamma(I_Z(m)) \subset \Gamma(O_{\mathbb{P}^N}(m)) \]

for \( m \gg 0 \). Finally, the local ring \( O_{Z,p} \) is finite dimensional (since \( Z \) is zero-dimensional) and thus can be spanned by polynomials of sufficiently large degree \( m \). \( \square \)

We return to the case where

\[ Z := \{ F_1 = F_2 = F_3 = 0 \} \subset \mathbb{P}^1 \times \mathbb{P}^1. \]

We can also consider the bivariate Hilbert function

\[ h_Z(d, e) := \dim(S/\langle F_1, F_2, F_3 \rangle)_{(d,e)} \]

and the bigraded Hilbert polynomial

\[ p_Z(d, e) := \chi(O_Z(d, e)); \]

Serre vanishing implies \( h_Z(d, e) = p_Z(d, e) \) for \( d, e \gg 0 \). As \( Z \) is finite, Proposition 22 shows that

\[ \deg(Z) = I(F_1, F_2, F_3) = p_Z(d, e), \]

for each \( (d, e) \in \mathbb{Z}^2 \).
Our strategy is to interpret the square matrix $R$ used to define $\text{Res}(F_1, F_2, F_3)$ in Section 4 through the Koszul complex associated with $F_1, F_2$, and $F_3$. This complex takes the form

$$0 \to S(-a_1 - a_2 - a_3, -3b) \xrightarrow{M_3}$$

$$S(-a_1 - a_2, -2b) \oplus S(-a_1 - a_3, -2b) \oplus S(-a_2 - a_3, -2b) \xrightarrow{M_2}$$

$$S(-a_1, -b) \oplus S(-a_2, -b) \oplus S(-a_3, -b) \xrightarrow{M_1} S \to 0,$$

(13)

where

$$M_1 = \begin{pmatrix} F_1 & F_2 & F_3 \end{pmatrix}$$

$$M_2 = \begin{pmatrix} F_2 & F_1 & 0 \\ -F_1 & 0 & F_3 \\ 0 & -F_1 & -F_2 \end{pmatrix}$$

$$M_3 = \begin{pmatrix} F_3 \\ 0 \\ -F_2 \end{pmatrix}$$

and the entries of the matrix correspond to multiplication by the indicated polynomial.

We can restrict (13) to the forms of fixed bidegree

$$0 \to S(d-a_1 - a_2 - a_3, -3b) \to S(d-a_1 - a_2, -2b) \oplus S(d-a_1 - a_3, -2b) \oplus S(d-a_2 - a_3, -2b) \xrightarrow{M_2}$$

$$\to S(d-a_1, -b) \oplus S(d-a_2, -b) \oplus S(d-a_3, -b) \to S(d,e) \to 0.$$  

(14)

Sheafifying the terms of complex (13) yields a complex of coherent sheaves on $\mathbb{P}^1 \times \mathbb{P}^1$:

$$0 \to \mathcal{O}(-a_1 - a_2 - a_3, -3b) \xrightarrow{M_3}$$

$$\mathcal{O}(-a_1 - a_2, -2b) \oplus \mathcal{O}(-a_1 - a_3, -2b) \oplus \mathcal{O}(-a_2 - a_3, -2b) \xrightarrow{M_2}$$

$$\mathcal{O}(-a_1, -b) \oplus \mathcal{O}(-a_2, -b) \oplus \mathcal{O}(-a_3, -b) \xrightarrow{M_1} \mathcal{O} \to 0,$$

where $\mathcal{O} = \mathcal{O}_{\mathbb{P}^1 \times \mathbb{P}^1}$. Tensoring by the line bundle $\mathcal{O}(d,e)$ yields

$$0 \to \mathcal{O}(d-a_1 - a_2 - a_3, e - 3b) \to$$

$$\mathcal{O}(d-a_1 - a_2, e - 2b) \oplus \mathcal{O}(d-a_1 - a_3, e - 2b) \oplus \mathcal{O}(d-a_2 - a_3, e - 2b) \to$$

$$\mathcal{O}(d-a_1, e - b) \oplus \mathcal{O}(d-a_2, e - b) \oplus \mathcal{O}(d-a_3, e - b) \to \mathcal{O}(d,e) \to 0.$$  

(15)

To implement our strategy, we seek $d$ and $e$ such that

- complex (14) has just two non-trivial terms and thus is given by a single matrix;
- the determinant of complex (14) computes the resultant in the sense of (Gelfand et al., 2008, p. 106).

The first condition is very explicit, as $S(a,b) = 0$ if and only if $a < 0$ or $b < 0$. For the second condition, Theorem 4.2 in (Gelfand et al., 2008, ch. 3) expresses the GKZ-resultant as the determinant of the complex, provided all the sheaves appearing in complex (15) have vanishing higher cohomology:

$$H^j(\mathcal{O}_{\mathbb{P}^1 \times \mathbb{P}^1}(d-a_1 - \cdots - a_i, e - rb)) = 0,$$

(16)

where $j > 0, r = 0, \ldots, 3$, and $1 \leq i_1 < \cdots < i_r \leq 3$. This condition is the notion of ‘stably twisted complexes’ of (Gelfand et al., 2008, p. 116).

Here is the crucial point: From now on, assume $d = a_1 + a_2 + a_3 - 1$ and $e = 2b - 1$. The vanishing (16) occurs for these values by the K"unneth formula

$$H^j(\mathcal{O}_{\mathbb{P}^1 \times \mathbb{P}^1}(m_1, m_2)) = \oplus_{j_1 + j_2 = j} H^{j_1}(\mathcal{O}_{\mathbb{P}^1}(m_1)) \otimes H^{j_2}(\mathcal{O}_{\mathbb{P}^1}(m_2))$$

(17)
and the fact that $H^1(\mathcal{O}_\mathbb{P}(m)) = 0$ for $m \geq -1$. Thus $\text{Res}(F_1, F_2, F_3)$ coincides with the GKZ-resultant up to a nonzero constant. Moreover, complex (14) specializes to

$$S_{(a_2+a_3-1,b-1)} \oplus S_{(a_1+a_2+a_3-1,b-1)} \oplus S_{(a_1+a_2+a_3-1,2b-1)} \rightarrow R_{(a_1+a_2+a_3-1,2b-1)},$$

where $R$ is the square matrix of size $(a_1 + a_2 + a_3) \cdot 2b$ used to define $\text{Res}(F_1, F_2, F_3)$ in Section 4. Our interpretation of Section 4. Our interpretation of

This complex is not exact since

$$h_Z(a_1 + a_2 + a_3 - 1, 2b - 1) = (a_1 + a_2 + a_3) \cdot 2b - \text{rank}(R).$$

To complete the proof of Theorem 21, it suffices to establish the following claim:

$$h_Z(a_1 + a_2 + a_3 - 1, 2b - 1) = \deg(Z).$$

Using (15), we obtain a complex

$$0 \rightarrow \mathcal{O}(d - a_1 - a_2 - a_3, e - 3b) \rightarrow$$

$$\mathcal{O}(d - a_1 - a_2, e - 2b) \oplus \mathcal{O}(d - a_1 - a_3, e - 2b) \oplus \mathcal{O}(d - a_2 - a_3, e - 2b) \rightarrow$$

$$\mathcal{O}(d - a_1, e - b) \oplus \mathcal{O}(d - a_2, e - b) \oplus \mathcal{O}(d - a_3, e - b) \rightarrow$$

$$\mathcal{O}(d, e) \rightarrow \mathcal{O}_Z(d, e) \rightarrow 0.$$

This complex is not exact since \{F_1, F_2, F_3\} is not a regular sequence, but the failure of exactness can be quantified using the fact that any two of the polynomials do form a regular sequence, since they lack common factors. The leftmost non-trivial arrow is injective (see (Eisenbud, 1995, Cor. 17.12)) and we have short exact sequences

$$0 \rightarrow \mathcal{O}(d - a_1 - a_2 - a_3, e - 3b) \rightarrow$$

$$\mathcal{O}(d - a_1 - a_2, e - 2b) \oplus \mathcal{O}(d - a_1 - a_3, e - 2b) \oplus \mathcal{O}(d - a_2 - a_3, e - 2b) \rightarrow \mathcal{Q} \rightarrow 0$$

(17)

$$0 \rightarrow \mathcal{K} \rightarrow \mathcal{O}(d - a_1, e - b) \oplus \mathcal{O}(d - a_2, e - b) \oplus \mathcal{O}(d - a_3, e - b) \rightarrow \mathcal{I}_Z(d, e) \rightarrow 0$$

(18)

$$0 \rightarrow \mathcal{I}_Z(d, e) \rightarrow \mathcal{O}(d, e) \rightarrow \mathcal{O}_Z(d, e) \rightarrow 0,$$

(19)

where $\mathcal{Q}$ and $\mathcal{K}$ are defined as the kernel and cokernel of the corresponding boundary maps. We also have

$$0 \rightarrow \mathcal{Q} \rightarrow \mathcal{K} \rightarrow \mathcal{K}/\mathcal{Q} \rightarrow 0.$$ 

(20)

The mapping from $\mathcal{Q}$ to $\mathcal{K}$ exists because we have a complex, and the quotient $\mathcal{K}/\mathcal{Q}$ measures the failure of our complex to be exact. As such, it is supported along $Z$.

To establish our claim, it suffices to show that $H^1(\mathcal{I}_Z(d, e)) = 0$; this implies

$$(S/(F_1, F_2, F_3))_{d,e} = \Gamma(\mathcal{O}(d, e)) \rightarrow \Gamma(\mathcal{O}_Z(d, e))$$

is surjective, by the long exact sequence in cohomology arising from short exact sequence (19). We have vanishing

$$H^r(\mathcal{O}(d - a_i, e - b)) = 0, \quad r \geq 1, \quad i = 1, 2, 3$$

since $d = a_3 + a_2 + a_3 - 1$ and $e = 2b - 1$. Thus the long exact sequence arising from (18) reduces us to showing that $H^2(\mathcal{K}) = 0$. The quotient $\mathcal{K}/\mathcal{Q}$ has finite support so

$$H^r(\mathcal{K}/\mathcal{Q}) = 0, \quad r \geq 1.$$
Hence the long exact sequence arising from (20) reduces us to proving that $H^2(\mathcal{Q}) = 0$. Finally, the long exact sequence from (17) includes

$$H^2(\mathcal{O}(d - a_1 - a_2, e - 2b)) \oplus \mathcal{O}(d - a_1 - a_3, e - 2b) \oplus \mathcal{O}(d - a_2 - a_3, e - 2b)) \to H^2(\mathcal{Q}) \to 0,$$

and

$$H^2(\mathcal{O}(d - a_{i_1} - a_{i_2}, e - 2b)) = H^2(\mathcal{O}(a_{i_3} - 1, -1)) = 0$$

for each permutation $\{i_1, i_2, i_3\}$ of $\{1, 2, 3\}$. Consequently, $H^2(\mathcal{Q}) = 0$ and our claim is proved.

Acknowledgements

Brendan Hassett is partially supported by NSF grants 0968349 and 0901645.

References


