

# Inherently Improper Parametric Supports for Unirational Varieties

Li-Yong Shen<sup>1</sup>, Eng-Wee Chionh<sup>2</sup>, Xiao-Shan Gao<sup>1\*</sup>, Jia Li<sup>1</sup>

<sup>1</sup> *KLMM, Institute of Systems Science, AMSS, Chinese Academy of Sciences, Beijing 100080, China*

<sup>2</sup> *School of Computing, National University of Singapore, Singapore 117543*

---

## Abstract

A class of parametric supports in the lattice space  $\mathbf{Z}^m$  is found to be inherently improper because any rational parametrization from  $\mathbf{C}^m$  to  $\mathbf{C}^n$  defined on such a support is improper. For a generic rational parametrization defined on an inherently improper support, we prove that its improper index is the gcd of the normalized volumes of all the simplex sub-supports and give an algorithm to obtain a proper reparametrization. Properties of non-degenerate rational parametrizations defined on an inherently improper parametric support with coefficients from some subfield of  $\mathbf{C}$  are also considered. Finally, the coordinate and lattice structures of inherently improper parametric supports are analyzed and a reparametrization algorithm of better complexity is given.

*Key words:* Inherently improper supports, improper rational parametrizations, support transformation, reparametrization, Chow form, lattice reduction, BKK bound.

---

## 1 Introduction

Algebraic varieties admitting rational parametric representations are not only interesting in theory but also important in practice: they are one of the main tools for representing shapes in computer modeling and processing ([Farin et al., 2002](#)). An algebraic variety admitting a rational parametrization is called

---

\* Corresponding author.

*Email addresses:* shenly@amss.ac.cn (Li-Yong Shen<sup>1</sup>),  
chionhew@comp.nus.edu.sg (Eng-Wee Chionh<sup>2</sup>), xgao@mmrc.iss.ac.cn  
(Xiao-Shan Gao<sup>1</sup>), lijia@mmrc.iss.ac.cn (Jia Li<sup>1</sup>).

*unirational*. A basic property of a rational parametrization is whether it is *proper* (one-to-one) or *improper* (many-to-one). Improper parametrizations are undesirable because the parametric degree could be unnecessarily high. An algebraic variety admitting a proper rational parametric representation is *rational*. If a rational parametrization  $RP$  is not proper, then a generic point of the variety corresponds to  $\mu > 1$  parameters. The integer  $\mu$ , denoted as  $IX(RP)$ , is called the *improper index* of the rational parametrization (Zariski, 1971; Van der Waerden, 1973).

If a rational parametrization is improper, naturally we would ask whether it can be reparameterized so that the new parametrization is proper. In general, the answer is negative. For algebraic curves, the existence of a proper reparametrization for an improper rational parametrization is guaranteed by Lüroth's theorem (Walker, 1950). Effective methods to find a proper reparametrization for an improper parametrization of an algebraic curve were proposed in (Sommerville, 1959; Sederberg, 1986; Gao and Chou, 1992; Diaz, 2006). For algebraic surfaces, if the base field is the field of complex numbers, then there always exists a proper reparametrization for an improper parametrization (Castelnuovo, 1894). However, if the dimension of the implicit variety determined by a parametric representation is greater than two, there exist improper parametrizations that do not have proper reparametrizations even over the field of complex numbers (Artin and Mumford, 1972). Related to this topic, an algorithm to compute all algebraic intermediate subfields in a unirational field extension was given in (Gutierrez and Sevilla, 2006).

The problem of finding a proper reparametrization for surfaces and varieties of higher dimensions is open in the general case (Schinzel, 2000) but there are several partial results. In (Diaz, 2006), a proper reparametrization algorithm was proposed for rational parametrizations which are improper in each parameter independently, that is, the proper reparametrization can be found by replacing each parameter with a rational function in itself. In (Li and Gao, 2006), a proper reparametrization algorithm was proposed for rational parametrizations which are improper in only one of the parameters. In (Chionh et al., 2006), a class of improper parametric supports for spatial surfaces was identified and the value called improper index  $IX(S)$  for any parametric support  $S$  was defined. Furthermore, for any non-degenerate rational parametric representation  $RP$  defined on a parametric support  $S$ ,  $IX(S)$  is a factor of  $IX(RP)$ .

In this paper, we consider the inherently improper parametric supports in the general case, that is, rational parametric mappings defined on these supports from  $\mathbf{C}^m$  to  $\mathbf{C}^n$  for any  $m < n$  are always improper. For a given finite parametric support  $S$  in  $\mathbf{Z}^m$ , we define its improper index  $IX(S)$  to be  $IX(RP)$  where  $RP$  is a generic rational parametrization defined on  $S$ . We then design an algorithm to compute  $IX(S)$  which needs only integer gcd computa-

tion. We further design an algorithm to find a proper reparametrization when  $IX(S) > 1$ . The algorithm needs only integer arithmetic operations and hence is very fast comparing to the usual methods based on symbolic computation. For rational parametrization  $RP$  defined on  $S$  with numerical coefficients, we prove that  $IX(S)$  is a factor of  $IX(RP)$ . We further design an algorithm to find a reparametrization whose improper index is  $IX(RP)/IX(S)$  and prove that for almost all coefficients the reparametrization is proper.

We also analyze the lattice structure of improper parametric supports. We show that improper parametric supports can be described with a set of linear congruent equations. As a result, we give a reparametrization algorithm with better complexities.

The rest of the paper is organized as follows. In Section 2, notations and preliminary results are given. In Section 3, generic rational parametrizations, which are rational parametrizations with indeterminate coefficients, are discussed. In Section 4, rational parametrizations with numerical coefficients are studied. In Section 5, the structure of improper parametric supports is analyzed. Section 6 concludes the paper with a summary.

## 2 Preliminaries

In this section we introduce the terminology and notation needed in the paper. The most important concepts defined are *improper indices* and *support transformations*. Support transformations lead to reparametrizations and improper supports can be shrunk by support transformations.

### 2.1 Parametric Supports of Rational Parametrizations

Let  $\mathbf{Z}$  be the set of integers and  $\mathbf{R}$  be the set of reals. For an integer  $m \geq 1$ , the set  $\mathbf{Z}^m$  is the set of lattice points and the set  $\mathbf{R}^m$  is the Euclidean space. For any set  $S \subseteq \mathbf{Z}^m$ , the Newton polytope  $NP(S)$  is the convex hull of  $S$ . For any convex set  $P \subseteq \mathbf{R}^m$ , the *normalized volume*  $NV(P)$  is  $m! \text{Vol}_m(P)$  where  $\text{Vol}_m(P)$  is the Euclidean volume of  $P$ .

A finite set  $S \subset \mathbf{Z}^m$  is a *parametric support* if  $NV(NP(S)) > 0$ . For example, the total degree  $d \geq 1$  parametric support is

$$T_d = \{\mathbf{p} = (p_1, \dots, p_m) \in \mathbf{Z}^m : 0 \leq p_1, \dots, 0 \leq p_m, |\mathbf{p}| = \sum_{i=1}^m p_i \leq d\}.$$

Note that  $NV(NP(T_d)) = d^m$ .

Let  $S$  be a parametric support in the following discussions.

Any set  $S' \subseteq S$  is a *parametric sub-support* of  $S$  if  $S'$  is also a parametric support. In particular, a sub-support  $S'$  is *simplex* if  $|S'| = m + 1$ . Simplex sub-supports turn out to be significant in the study of improper supports.

Let  $\mathbf{C}$  be the field of complex numbers. A *rational parametrization on a parametric support*  $S$ , written  $RP(S)$ , is a set of rational equations defining a map from  $\mathbf{C}^m$  to  $\mathbf{C}^n$ ,  $m < n$ :

$$(X_1(\mathbf{t}), \dots, X_n(\mathbf{t})) = \left( \frac{x_1(\mathbf{t})}{x_0(\mathbf{t})}, \dots, \frac{x_n(\mathbf{t})}{x_0(\mathbf{t})} \right) = \frac{\sum_{\mathbf{p} \in S} (x_{1,\mathbf{p}}, \dots, x_{n,\mathbf{p}}) \mathbf{t}^{\mathbf{p}}}{\sum_{\mathbf{p} \in S} x_{0,\mathbf{p}} \mathbf{t}^{\mathbf{p}}} \quad (1)$$

where  $0 \neq (x_{0,\mathbf{p}}, \dots, x_{n,\mathbf{p}}) \in \mathbf{K}^{n+1}$  are coefficients from some field  $\mathbf{K} \subseteq \mathbf{C}$ ; and  $\mathbf{t} = (t_1, \dots, t_m)$ ,  $\mathbf{p} = (p_1, \dots, p_m)$ ,  $\mathbf{t}^{\mathbf{p}} = t_1^{p_1} \dots t_m^{p_m}$ .

Since the parametric equations are rational, a rational parametrization on  $S$  is invariant under integer translations of  $S$ . Thus for any parametric support  $S$ , we may translate  $S$  such that either  $S$  contains the origin or  $S$  is non-negative meaning the coordinates of the lattice points in  $S$  are non-negative. The following proposition ensures that we may assume simultaneously a support contains the origin and is non-negative without loss of generality.

**Proposition 1** *Let  $S$  be a non-negative parametric support. The rational parametrization  $RP(S)$  on  $S$  has a bi-rational reparametrization on a parametric support  $S'$  such that  $S'$  contains the origin and is non-negative.*

Proof

Suppose  $0 \notin S$ .

Consider the monomials  $\mathbf{t}^{\mathbf{p}}$ ,  $\mathbf{p} \in S$ , of least total degree  $|\mathbf{p}| = d$ . We can assume  $t_1$  appears in some of these monomials. (For otherwise, there is some  $t_k$  that appears in these monomials. The bi-rational transformation

$$t_1 = s_k; \quad t_k = s_1; \quad t_i = s_i, i \neq 1, k;$$

would have  $s_1$  appear in these monomials.) Consider the bi-rational transformation

$$t_1 = s_1, \quad t_2 = s_1 s_2, \quad \dots, \quad t_m = s_1 s_m. \quad (2)$$

After the transformation, the least degree of  $s_1$  in all the transformed monomials of  $S$  is  $d$ . After dividing out  $s_1^d$ , the least total degree of all the transformed monomials of  $S$  is at most  $d - 1$ .

The above process can be repeated and eventually the least total degree has to become zero. That is, the eventual transformed  $S'$  contains the origin and is non-negative.  $\square$

In the rest of this paper, we always assume that a parametric support contains the origin.

A non-degenerate rational parametrization  $RP(S)$  on a parametric support  $S$  defines an  $m$  dimensional unirational variety when  $m < n$ . For the rest of the paper we restrict our discussion to non-degenerate unirational varieties when the coefficients of  $RP(S)$  are in a subfield of  $\mathbf{C}$ . This loses no generality as we can always check if a rational parametrization is non-degenerate (Chionh and Goldman, 1992; Gao and Chou, 1992).

## 2.2 Shrinking Support Transformations and Shrinkable Supports

Let  $T : \mathbf{R}^m \rightarrow \mathbf{R}^m$  be an invertible affine transformation with

$$T(p_1, \dots, p_m) = (a_{1,0} + a_{1,1}p_1 + \dots + a_{1,m}p_m, \dots, a_{m,0} + a_{m,1}p_1 + \dots + a_{m,m}p_m). \quad (3)$$

Transformation  $T$  is a *support transformation with respect to a parametric support*  $S$  if  $T(S)$  is also a parametric support; that is,  $T(S) \subseteq \mathbf{Z}^m$  and  $T$  is non-singular. The absolute value of the determinant of the Jacobian matrix of  $T$  is written as

$$J(T) = \text{abs} \begin{vmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \dots & a_{m,m} \end{vmatrix}.$$

Given a support transformation  $T$  for a parametric support  $S$ , it is a well-known fact in calculus that

$$J(T) = \frac{NV(NP(T(S)))}{NV(NP(S))}.$$

For obvious reasons, a support transformation  $T$  with  $J(T) < 1$  is called a *shrinking support transformation*, and a support that admits a shrinking transformation is called a *shrinkable support*.

The following proposition states that a support transformation reparametrizes a rational parametrization.



**Proposition 3** *The apparent algebraic degree of a generic rational parametrization (1) is  $NV(NP(S))$ .*

Proof

Consider the solutions of the polynomial equations obtained by substituting (1) into (5) and multiplying  $x_0(\mathbf{t})$ :

$$\begin{cases} u_{10}x_0(\mathbf{t}) + u_{11}x_1(\mathbf{t}) + u_{12}x_2(\mathbf{t}) + \cdots + u_{1n}x_n(\mathbf{t}) = 0 \\ \vdots \\ u_{m0}x_0(\mathbf{t}) + u_{m1}x_1(\mathbf{t}) + u_{m2}x_2(\mathbf{t}) + \cdots + u_{mn}x_n(\mathbf{t}) = 0 \end{cases} \quad (6)$$

The intersection points of (5) and (1) are the solutions of (6) by removing the solutions

$$\begin{cases} u_{11}x_1(\mathbf{t}) + u_{12}x_2(\mathbf{t}) + \cdots + u_{1n}x_n(\mathbf{t}) = 0 \\ \vdots \\ u_{m1}x_1(\mathbf{t}) + u_{m2}x_2(\mathbf{t}) + \cdots + u_{mn}x_n(\mathbf{t}) = 0 \\ x_0(\mathbf{t}) = 0 \end{cases} \quad (7)$$

Since (7) has  $m + 1$  equations with  $m$  variables, (7) has common solutions if and only if its resultant is zero (Cox et al., 1998), which is impossible because the equations in (7) have generic coefficients. So the intersection points of (5) and (1) are exactly the solutions of (6) for a generic rational parametrization.

According to a modified version of Bernstein's Theorem (Li and Wang, 1996), for an equation system on a support  $S$  containing the origin and with generic coefficients, its number of solutions is  $NV(NP(S))$  which is known as the *BKK bound*.  $\square$

By Proposition 3, the BKK bound allows us to use the explicit value  $NV(NP(S))$  for the apparent algebraic degree of a support in this paper. Consequently, we define the *improper index* of  $S$  to be

$$IX(S) = \frac{NV(NP(S))}{AD(S)}.$$

For a generic parametrization (1) on  $S$ , the improper index  $IX(S)$  gives the number  $\mu$  of parameter points  $(t_1, \dots, t_m)$  corresponding to a generic point  $(X_1, \dots, X_n)$  of the unirational variety defined by  $RP(S)$ . We state this fun-

damental property as a proposition.

**Proposition 4** *Let  $S$  be a parametric support with improper index  $IX(S)$ . For a generic parametrization on  $S$ , there are  $IX(S)$  parametric points corresponding to a generic variety point.*

Thus  $S$  is *proper* if  $IX(S) = 1$  and *improper* if  $IX(S) > 1$ . The following proposition asserts that a shrinkable support is improper.

**Proposition 5** *If there is a support transformation  $T$  for a parametric support  $S$  with  $J(T) < 1$ , then  $S$  is an improper parametric support and*

$$\frac{IX(S)}{IX(T(S))} = \frac{1}{J(T)}.$$

Proof

By Proposition 2, the induced parametrization on the support  $T(S)$  is a reparametrization of the parametrization on the support  $S$ . Thus  $AD(T(S)) = AD(S)$  and

$$\frac{IX(S)}{IX(T(S))} = \frac{NV(NP(S))AD(T(S))}{NV(NP(T(S)))AD(S)} = \frac{NV(NP(S))}{NV(NP(T(S)))} = \frac{1}{J(T)}.$$

Since  $IX(T(S)) \geq 1$ , we have  $IX(S) > 1$  and  $S$  is improper.  $\square$

2.3.1 *Example:  $m = 2, n = 3, S = \{(0, 0), (2, 0), (1, 1), (0, 2), (2, 2)\}$*

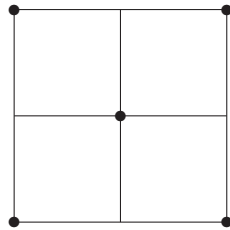


Fig. 1. parametric support of  $m = 2$

By the technique of random coefficients or otherwise, we find  $AD(S) = 4$  (Chionh et al., 2006). Thus

$$IX(S) = \frac{2! \times 2^2}{4} = 2.$$

Indeed, two parameter points  $(t_1, t_2), (-t_1, -t_2)$  correspond to a generic surface point  $(X_1, X_2, X_3)$ .

2.3.2 *Example:*  $m = 3$ ,  $n = 4$ ,  $S = \{ (0, 0, 0), (2, 0, 0), (0, 2, 0), (0, 0, 2), (0, 2, 2), (2, 0, 2), (2, 2, 0), (1, 1, 1), (2, 2, 2) \}$

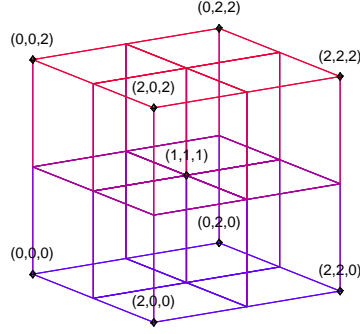


Fig. 2. parametric support of  $m = 3$

Again by using random coefficients or otherwise, we find  $AD(S) = 12$ . Thus  $IX(S) = \frac{3! \times 2^3}{12} = 4$ . Indeed, four parameter points  $(t_1, t_2, t_3)$ ,  $(t_1, -t_2, -t_3)$ ,  $(-t_1, t_2, -t_3)$ ,  $(-t_1, -t_2, t_3)$  correspond to a generic variety point  $(X_1, \dots, X_4)$ .

2.3.3 *Example:* Simplex supports  $|S| = m + 1$

Let  $S = \{ \mathbf{p}_j \in \mathbf{Z}^m : \mathbf{p}_j = (p_{j,1}, \dots, p_{j,m}), j = 1, \dots, m + 1 \}$  be a simplex support, that is,  $NV(NP(S)) > 0$  and  $|S| = m + 1$ . It is easily verified that a generic rational parametrization on  $S$  gives a hyperplane, thus  $AD(S) = 1$  and

$$IX(S) = NV(NP(S)) = \text{abs} \begin{vmatrix} p_{1,1} & \cdots & p_{1,m} & 1 \\ \vdots & \ddots & \vdots & \vdots \\ p_{m+1,1} & \cdots & p_{m+1,m} & 1 \end{vmatrix}. \quad (8)$$

This means that the improper index of a simplex support is simply its normalized volume. Consequently, a simplex support is improper if and only if its normalized volume is greater than 1.

### 3 Generic Rational Parametrization on Improper Supports

In this section, we will prove the main result of this paper for a parametric support  $S$ :

$$IX(S) = \gcd\{NV(NP(S')) : S' \subseteq S, |S'| = m + 1\}.$$



Consider a sub-support  $S' \subseteq S$ . The sub-support  $S'$  can be obtained from  $S$  by setting indeterminate coefficients  $x_{0,\mathbf{p}}, \dots, x_{n,\mathbf{p}}$  to zero for each  $\mathbf{p} \in S \setminus S'$ . Correspondingly, the Chow form  $F'$  of  $S'$  can be obtained from the Chow form  $F$  of  $S$  by successively setting these indeterminate coefficients in  $F$  to zero. Let  $f_l^{\mu}$  be the Chow form obtained after setting  $l$  indeterminate coefficients to zero and the next indeterminate coefficient to be set to zero is  $c$ . Then we can write  $f_l = cg + ef_{l+1}^{\nu_{l+1}}$  where  $\nu_{l+1} \geq 1$ ,  $e$  is extraneous factors and  $f_{l+1}$  is a factor of the Chow form after setting  $l+1$  indeterminate coefficients to zero. We see that the Chow form after setting  $l+1$  indeterminate coefficients to zero is  $f_{l+1}^{\mu\nu_{l+1}}$ . Consequently we have

$$F' = f_L^{\mu\nu_1 \cdots \nu_L}$$

where  $\nu_j \geq 1$  and  $L$  is the number of indeterminate coefficients that have been set to zero to obtain  $S'$  from  $S$ . It follows that  $IX(S') = \mu\nu_1 \cdots \nu_L$  and thus  $IX(S)|IX(S')$ .  $\square$

The following corollaries are immediate consequences of the above theorem.

**Corollary 1** *Every sub-support of an improper parametric support is improper. Conversely, if a sub-support of a parametric support is proper, then the support is also proper.*

**Corollary 2** *Let  $S_1, \dots, S_N$  be sub-supports of a parametric support  $S$ . If  $\gcd(IX(S_1), \dots, IX(S_N)) = 1$ , then  $S$  is a proper parametric support.*

### 3.2 Constructing $m$ -Dimensional Support Transformations

Let  $S$  be a parametric support containing the origin. The following construction shows that there is a support transformation  $T$  such that  $IX(S)J(T) = 1$ . First we introduce the notations.

- For a lattice point  $\mathbf{p} = (p_1, \dots, p_m) \in \mathbf{Z}^m$ , the  $k$ -th projection of  $\mathbf{p}$  is  $\mathbf{p}^{(k)} = (p_{m+1-k}, \dots, p_m) \in \mathbf{Z}^k$ . We write  $0^{(k)} = (0, \dots, 0) \in \mathbf{Z}^k$ .
- The normalized volume of the  $k$ -th projections of  $k$  lattice points of  $S$  and the  $k$ -th projection of the origin is a  $(k+1) \times (k+1)$  determinant

$$A_{\sigma}^{(k)} = abs \begin{vmatrix} 0^{(k)} & 1 \\ \mathbf{p}_{\sigma_1}^{(k)} & 1 \\ \vdots & \vdots \\ \mathbf{p}_{\sigma_k}^{(k)} & 1 \end{vmatrix} \quad (11)$$

where  $\sigma$  chooses  $k$  points  $\mathbf{p}_{\sigma_1}, \dots, \mathbf{p}_{\sigma_k}$  from  $S$ .

- We define  $g_k = \gcd_\sigma \{A_\sigma^{(k)}\}$ ,  $k = 1, \dots, m$ . By Laplace expansion along the first column we see that  $g_k | g_{k+1}$ .

We set the support transformation  $T$  as

$$T(p_1, \dots, p_m) = \left( \frac{g_{m-1}p_1 + \beta_{1,2}p_2 + \dots + \beta_{1,m}p_m}{g_m}, \dots, \frac{g_1p_{m-1} + \beta_{m-1,m}p_m}{g_2}, \frac{p_m}{g_1} \right) \quad (12)$$

where  $\beta_{i,j}$  are integers to be found such that  $T(S) \subset \mathbf{Z}^m$ .

When  $k = 1$ ,  $A_\sigma^{(1)} = abs \begin{vmatrix} 0 & 1 \\ \mathbf{p}_\sigma^{(1)} & 1 \end{vmatrix} = |\mathbf{p}_\sigma^{(1)}| = |p_{\sigma,m}|$ . Thus  $g_1 = \gcd_\sigma \{|p_{\sigma,m}|\}$  and we have  $g_1 | p_{\sigma,m}$  for all  $\mathbf{p}_\sigma \in S$ .

For each  $A_\sigma^{(k)}$  involved in computing  $g_k$ , enlarge it to become  $A_{\sigma'}^{(k+1)}$  where  $\sigma'$  chooses the same  $k$  points chosen by  $\sigma$  together with a general point  $\mathbf{p} \in S$ . We thus have

$$A_{\sigma'}^{(k+1)} = abs \begin{vmatrix} 0^{(k+1)} & 1 \\ \mathbf{p}_{\sigma_1}^{(k+1)} & 1 \\ \vdots & \vdots \\ \mathbf{p}_{\sigma_k}^{(k+1)} & 1 \\ \mathbf{p}^{(k+1)} & 1 \end{vmatrix}.$$

By Laplace expansion along the last row, we have

$$A_{\sigma'}^{(k+1)} = A_\sigma^{(k)} p_{m-k} + B_{\sigma, m-k+1} p_{m-k+1} + \dots + B_{\sigma, m} p_m \quad (13)$$

where  $B_{\sigma, m-k+1}, \dots, B_{\sigma, m}$  are minor determinants of  $A_{\sigma'}^{(k+1)}$ .

Since  $g_k = \gcd_\sigma \{A_\sigma^{(k)}\}$ , there exist integers  $\alpha_\sigma$  such that  $\sum_\sigma \alpha_\sigma A_\sigma^{(k)} = g_k$ . But  $g_{k+1} | A_{\sigma'}^{(k+1)}$  for any  $\sigma$ , by (13), we have

$$\frac{\sum_\sigma \alpha_\sigma A_{\sigma'}^{(k+1)}}{g_{k+1}} = \frac{g_k p_{m-k} + \beta_{m-k, m-k+1} p_{m-k+1} + \dots + \beta_{m-k, m} p_m}{g_{k+1}}$$

is an integer, where  $\beta_{m-k, j} = \sum_\sigma \alpha_\sigma B_{\sigma, j}$ .

From the above computation, we obtain the following lemma.

**Proposition 7** *The transformation (12) is a support transformation for  $S$  and  $J(T) = 1/g_m$ .*

Proof

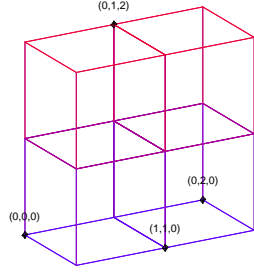
The construction of  $T$  ensures that it is a support transformation for  $S$ . Furthermore, one finds that

$$J(T) = \text{abs} \begin{vmatrix} g_{m-1} & \beta_{1,2} & \dots & \beta_{1,m} \\ g_m & g_m & & g_m \\ 0 & g_{m-2} & \dots & \beta_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \frac{1}{g_1} \end{vmatrix} = \frac{1}{g_m}.$$

□

### 3.2.1 Example: Constructing a 3-dimensional Support Transformation

Let  $S = \{(0, 0, 0), (1, 1, 0), (0, 2, 0), (0, 1, 2)\}$  (see Figure 3(a)). We easily find  $NV(NP(S)) = 4$ .



(a) improper support      (b) proper support

Fig. 3. support transformation

By (12), we find  $g_1 = 2, g_2 = 2, g_m = g_3 = 4$ , and the transformation is:

$$T(p_1, p_2, p_3) = \left( \frac{2p_1 - 2p_2 + p_3}{4}, \frac{2p_2 - p_3}{2}, \frac{p_3}{2} \right)$$

Then  $T(S) = \{(0, 0, 0), (0, 1, 0), (-1, 2, 0), (0, 0, 1)\}$  and  $NV(NP(T(S))) = 1$ . Later we will show that  $NV(NP(T(S))) = 1$  always holds for  $T$  given by (12).  $T(S)$  can be translated to  $S' = T(S) \oplus (1, 0, 0) = \{(1, 0, 0), (1, 1, 0), (0, 2, 0), (1, 0, 1)\}$ . By Proposition 1, we can transform  $S'$  to  $S'' = \{(0, 0, 0), (1, 1, 0), (1, 2, 0), (1, 0, 1)\}$  (see Figure 3(b)). Then  $S''$  is a non-negative parametric support containing the origin and  $NV(NP(S'')) = 1$ .

Let  $\mathbf{p}_0 \in \mathbf{Z}^m$ . For any set of  $m + 1$  lattice points  $P = \{\mathbf{p}_1, \dots, \mathbf{p}_{m+1}\}$ ,  $NV(P)$  is a linear combination of  $NV(\mathbf{p}_0 \cup P \setminus \{\mathbf{p}_j\})$ ,  $j = 1, \dots, m + 1$ . Thus instead of

computing the gcd of all simplex sub-supports we need only compute the gcds of simplex sub-supports anchored at some chosen point  $\mathbf{p}_0$ . This observation leads to the following result.

**Proposition 8** *Let  $S$  be a parametric support and  $\mathbf{p}_0 \in S$ . We have*

$$\begin{aligned} & \gcd\{NV(NP(S')) : S' \subseteq S, |S'| = m + 1\} = \\ & \gcd\{NV(NP(S'')) : \mathbf{p}_0 \in S'' \subseteq S, |S''| = m + 1\}. \end{aligned}$$

Now we are ready to prove the main result.

**Theorem 1** *Let  $S$  be a parametric support. We have*

$$IX(S) = \gcd\{NV(NP(S')) : S' \subseteq S, |S'| = m + 1\}. \quad (14)$$

Proof

Since  $IX(S)$  and  $NV(NP(S'))$ ,  $S' \subseteq S$ , are invariant under any translation, we may assume  $S$  contain the origin as required by the construction of  $T$  given by (12).

Since  $T$  defined in (12) is invertible, we have

$$\begin{aligned} & \gcd\{NV(NP(S'')) : S'' \subseteq T(S), |S''| = m + 1\} \\ & = \gcd\{NV(NP(T(S'))) : S' \subseteq S, |S'| = m + 1\} \\ & = J(T) \gcd\{NV(NP(S')) : S' \subseteq S, |S'| = m + 1\} \\ & = \frac{\gcd\{NV(NP(S')) : S' \subseteq S, |S'| = m + 1\}}{g_m} \\ & = 1. \end{aligned}$$

The last equality uses Proposition 8 with the origin as the anchor. By Example 2.3.3,  $IX(S'') = NV(NP(S''))$  when  $S'' \subseteq T(S)$  is a simplex sub-support. By Proposition 6, we conclude  $IX(T(S)) = 1$ . But by Proposition 5,  $IX(T(S)) = IX(S)J(T)$ . Thus we have  $IX(S) = g_m$ .  $\square$

The theorem may also be phrased in the following form:

**Corollary 3** *For a parametric support  $S$ , there exists a support transformation  $T$  such that  $IX(S)J(T) = 1$  and  $T(S)$  is proper.*

**Corollary 4** *Let  $S$  be a parametric support and  $\mathbf{p}_0 \in S$ . We have*

$$IX(S) = \gcd\{NV(NP(S')) : S' \subseteq S, |S'| = m + 1, \mathbf{p}_0 \in S'\}.$$

Note that Corollary 4 provides an algorithm to compute  $IX(S)$  by computing the gcd of  $\binom{|S|-1}{m}$  integers.

#### 4 Arbitrary Parametrizations on Improper Supports

All the preceding results hold for a rational parametrization with generic coefficients. We now investigate the situation when the coefficients are specialized to some values in the coefficient field.

For a set of coefficients  $C$  of (1) taken from the coefficient field  $\mathbf{K}$ , we use  $IX(S, C)$  to denote the *improper index* of the rational parametrization.

**Theorem 2** *Let  $IX(S, C)$  be the improper index of a parametrization with coefficients  $C$  on a parametric support  $S$ , and  $T$  the transformation (12). Then  $IX(S, C) = IX(T(S), T(C)) IX(S)$ , where  $T(C)$  is the set of coefficients of the reparametrization by the transformation  $T$ . Consequently, if  $IX(S) > 1$  then  $IX(S, C) > 1$ .*

Proof

By (4), the reparametrization introduced by  $T$  in (12) is

$$\begin{aligned} t_1 &= s_1^{\frac{g_{m-1}}{g_m}}, \\ t_2 &= s_1^{\frac{\beta_{1,2}}{g_m}} s_2^{\frac{g_{m-2}}{g_{m-1}}}, \\ &\vdots \\ t_m &= s_1^{\frac{\beta_{1,m}}{g_m}} s_2^{\frac{\beta_{2,m}}{g_{m-1}}} \cdots s_m^{\frac{g_1}{g_m}}. \end{aligned} \tag{15}$$

The inverse of (15) can be represented as

$$\begin{aligned} s_1 &= t_1^{\frac{g_m}{g_{m-1}}}, \\ s_2 &= t_1^{\gamma_{1,2}} t_2^{\frac{g_{m-1}}{g_{m-2}}}, \\ &\vdots \\ s_m &= t_1^{\gamma_{1,m}} t_2^{\gamma_{2,m}} \cdots t_m^{g_1}, \end{aligned} \tag{16}$$

where  $\gamma_{j,k}$  are some rational numbers not important in the derivation.

Recall Proposition 4, the improper index of a rational parametrization is the number of parameter values corresponding to a generic point of the unirational

variety  $V$  defined by the parametrization  $RP(C)$ . Since transformation  $T$  leads to a reparametrization, the transformed parametrization  $RP(T(S))$  defines the same variety  $V$ . By definition, a generic point of  $V$  under the reparametrization corresponds to  $IX(T(S), T(C))$  parameter values  $(s_1, \dots, s_m)$ . We may assume  $s_1 s_2 \dots s_m \neq 0$  as this condition fails only on some lower dimensional subvariety of  $V$ . By (16), a parameter point  $(s_1, \dots, s_m)$  with  $s_1 s_2 \dots s_m \neq 0$  leads to  $\frac{g_m}{g_{m-1}} \dots \frac{g_2}{g_1} g_1 = g_m$  parameter points  $(t_1, \dots, t_m)$ . This completes the proof since  $g_m = IX(S)$ .  $\square$

**Theorem 3** *Let  $S$  be a proper parametric support; that is,  $IX(S) = 1$ . For coefficients  $C$  of (1) taken from a Zariski open set in the coefficient space  $\mathbf{K}^{(n+1)|S|}$ , rational parametrization (1) is proper; that is,  $IX(S, C) = 1$ .*

Proof

When (1) has base points, the following homogenous equations in  $\bar{\mathbf{t}} = (t_0, \mathbf{t})$ , have nonzero solutions

$$\sum_{\mathbf{p} \in S} x_{0,\mathbf{p}} t_0^{d-|\mathbf{p}|} \mathbf{t}^{\mathbf{p}} = 0, \dots, \sum_{\mathbf{p} \in S} x_{n,\mathbf{p}} t_0^{d-|\mathbf{p}|} \mathbf{t}^{\mathbf{p}} = 0 \quad (17)$$

where  $d = \max\{|\mathbf{p}| : \mathbf{p} \in S\}$ . Take the sparse resultant  $R$  (Cox et al., 1998) of any  $m + 1$  of the  $n + 1$  equations. If  $R(C) \neq 0$  for a set of numerical coefficients  $C$ , equations (17) with coefficients  $C$  have no non-zero solutions. In other words, if  $C$  is taken from the Zariski open set  $\mathbf{K}^{(n+1)|S|} \setminus Zero(R)$  then (1) has no base points. Thus there is no loss of generality by assuming the parametrization on  $S$  has no base points.

By  $IX(S) = 1$  and Proposition 4, the rational parametrization (1) with indeterminate coefficients is proper. By the proof of Proposition 6, the Chow form  $F$  of (1) involves  $\mathbf{u}_0 = (u_{00}, u_{01}, \dots, u_{0n}), \mathbf{u}_1, \dots, \mathbf{u}_m$ . Let  $D_{u_{00}}$  be the discriminants of  $F$  as a univariate polynomial in  $u_{00}$ , which is not identical zero. When the indeterminate coefficients are specialized to  $C$  such that the improper index is  $\mu = IX(S, C) > 1$ , the Chow form of (1) with coefficients  $C$  becomes  $F_C^\mu$ . Since the specialized Chow form  $F_C^\mu$  is no longer square-free, then the discriminant  $D_{u_{00}}$  vanishes when it is also specialized to  $C$ . But  $D_{u_{00}}$  is a non-zero polynomial in  $u_{01}, \dots, u_{0n}; \mathbf{u}_1, \dots, \mathbf{u}_m$ . Then the coefficients of  $D_{u_{00}}$  as polynomials in  $u_{01}, \dots, u_{0n}; \mathbf{u}_1, \dots, \mathbf{u}_m$  should be zero. Let  $D$  be such a coefficient which is a polynomial in  $x_{0,\mathbf{p}}, \dots, x_{n,\mathbf{p}}$ . From the above argument, we see that for a set  $C$  of numerical values of the coefficients of (1), if  $R(C)D(C) \neq 0$ , (1) must be proper. The required Zariski open set can be taken as  $\mathbf{K}^{(n+1)|S|} \setminus Zero(RD)$ .  $\square$

Since a Zariski open set is the whole coefficient space minus a set with lower dimensions, Theorem 3 means that for almost all numerical coefficients, trans-

formation  $T$  in Theorem 1 gives a proper reparametrization. We state this result as a corollary.

**Corollary 5** *Let  $S$  be an improper parametric support. For coefficients  $C$  of (1) taken from a Zariski open set in the coefficients space, the rational parametrization obtained with the transformation (12) is proper.*

4.1 *Example:  $IX(S) = 2, IX(S, C) = 8, IX(T(S), T(C)) = 4$*

Let  $m = 2, S = \{1, t_1^2, t_1 t_2, t_2^2, t_1^2 t_2^2\}$  in Example 2.3.1 and  $n = 4$ . Random integer values are generated to construct three different polynomials in  $t_1, t_2$  and arbitrarily take them to be  $x_0(t_1, t_2), x_1(t_1, t_2), x_2(t_1, t_2)$ . We then set  $x_3(t_1, t_2) = x_1(t_1, t_2), x_4(t_1, t_2) = x_2(t_1, t_2)$ . Computing the Chow form using the Dixon resultant, we find both before and after the parametrizations to be improper, but the reparametrization has only half of the original improper index.

To find the exact conditions for the coefficients  $C$  such that the  $IX(S, C) = 1$  need more subtle discussion, which is beyond the scope of this paper.

## 5 Improper Parametric Support and Lattice

Since the structure of the support decides the index of its parametrization, we will take a look at the structure of the inherent parametric support.

We now consider the lattice  $\mathcal{S} = \text{span}(S) = \{\sum_i r_i \mathbf{p}_i : r_i \in \mathbf{Z}, \mathbf{p}_i \in S\}$  generated by the parametric support  $S$  as a free  $\mathbf{Z}$ -module. Then  $\mathcal{S}$  has a basis as  $\{\mathbf{s}_1, \dots, \mathbf{s}_m\} \in \mathbf{Z}^m$  and *determinant of the lattice* is defined by  $d(\mathcal{S}) = \text{abs}(\det(\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_m))$ , which does not depend on the choice of the basis (Lenstra et al, 1982; Cohen, 1996).

From a full rank generating set  $S \subset \mathbf{Z}^m$ , we can get a basis by computing the its *Hermite normal form*. Since the Hermite normal form often involves large numbers, we can obtain an LLL-reduced basis by the MLLL algorithm (Pohst, 1987; Cohen, 1996). The vectors of LLL-reduced basis will be much shorter in Euclidean length and the running time is at most  $\mathcal{O}(m + |S|)^4 \log B, \|\mathbf{p}\| \leq B$ .

Now we can obtain the reparametrization of  $S$  by two steps. The first step is to find a basis of  $S$  and the second step is to construct the shrink transformation  $T$  as in subsection 3.2 with the basis.

**Theorem 4** *Let  $S$  be a parametric support,  $\mathcal{S}$  the lattice generated by  $S$ , and*

$B = \{\mathbf{s}_1, \dots, \mathbf{s}_m\}$  a basis of  $\mathcal{S}$ ,  $T_B$  the transformation obtained as in (12) from  $B$ . Then  $T_B$  is a support transformation for  $S$  and  $T_B(S)$  is a proper parametric support.

Proof

Since  $S$  is the generating set of  $\mathcal{S}$ , we have

$$d(\mathcal{S}) = \begin{vmatrix} \mathbf{s}_1 \\ \vdots \\ \mathbf{s}_m \end{vmatrix} = \begin{vmatrix} \sum_{j=1}^{|S|} \alpha_{1,j} \mathbf{p}_j \\ \vdots \\ \sum_{j=1}^{|S|} \alpha_{m,j} \mathbf{p}_j \end{vmatrix} = \sum \beta_k NV(NP(S'))$$

where  $\mathbf{p}_j \in S, 0 \in S' \subset S, |S'| = m + 1$ , and  $\alpha_{i,j}, \beta_k$  are integers. It means that  $IX(S) | d(\mathcal{S})$ . On the other hand,  $\{\mathbf{s}_1, \dots, \mathbf{s}_m\}$  is also a basis of  $S$ , and so we have  $d(\mathcal{S}) | IX(S)$ . Then  $IX(S) = d(\mathcal{S})$

By Proposition 7,  $J(T_B) = 1/NV(NP(\{B, 0\})) = 1/d(\mathcal{S}) = 1/IX(S)$ . Now we show  $T_B$  is an integer transformation on  $S$ . Actually, for  $\mathbf{p} \in S$ , thus  $\mathbf{p} = \sum_{j=1}^m \alpha_j \mathbf{s}_j$  and  $T_B(\mathbf{p}) = \sum_{j=1}^m \alpha_j T_B(\mathbf{s}_j) \in \mathbf{Z}^m$ .  $\square$

The above theorem leads to a new reparametrization algorithm: for a parametric support  $S$ , we first generate a basis  $B$  of  $\mathcal{S}$ , and then construct  $T_B$  as the support transformation of  $S$ . The complexity of generating  $B$  is polynomial in  $|S|$  (Lenstra et al, 1982; Cohen, 1996). Since  $|B| = m$ , if  $|S|$  is much larger than  $m$ , then the new algorithm is of great advantage over the algorithm proposed in Section 3. On the other hand, if  $|S|$  and  $m$  are almost the same, then we can still use the algorithm in Section 3, because that algorithm is much simpler.

The following proposition gives useful information on the structure of a parametric support.

**Theorem 5** *Let  $S$  be a parametric support,  $\mathcal{S}$  the lattice spanned by  $S$ , and  $\{\mathbf{s}_1, \dots, \mathbf{s}_m\}$  a basis of the lattice  $\mathcal{S}$ . Then there exist integers  $a_{i,j}$  s.t.  $\mathcal{S} = \{(x_1, \dots, x_m) : \sum_{j=1}^m a_{i,j} x_j = 0 \pmod{d(\mathcal{S})}, 1 \leq i \leq m\}$ .*

Proof

Considering the hyperplanes determined by the origin and  $m - 1$  points from  $\{\mathbf{s}_1, \dots, \mathbf{s}_m\}$ ,  $\mathbf{s}_i = (s_{i,1}, \dots, s_{i,m})$ , we get  $m$  hyperplanes  $\sum_{j=1}^m s_{i,j}^* x_j = 0$ , where

$s_{i,j}^*$  are algebraic co-minors of  $s_{i,j}$  in the determinant

$$\begin{vmatrix} s_{1,1} & \cdots & s_{1,m} \\ \vdots & \ddots & \vdots \\ s_{m,1} & \cdots & s_{m,m} \end{vmatrix}$$

and not all are zero because any  $m - 1$  points of the basis are linearly independent.

It is clear that  $\mathcal{L} = \{(x_1, \dots, x_m) \in \mathbf{Z}^m : \sum_{j=1}^m s_{i,j}^* x_j = \mathbf{Z}d(\mathcal{S}), 1 \leq i \leq m\}$  is a lattice. Since  $\{\mathbf{s}_1, \dots, \mathbf{s}_m\} \subset \mathcal{L}$ , we have  $\mathcal{S} \subset \mathcal{L}$  and  $d(\mathcal{L})|d(\mathcal{S})$ .

Let  $\{\mathbf{l}_1, \dots, \mathbf{l}_m\}$  be a basis of  $\mathcal{L}$ , then

$$\begin{pmatrix} s_{1,1}^* & \cdots & s_{1,m}^* \\ \vdots & \ddots & \vdots \\ s_{m,1}^* & \cdots & s_{m,m}^* \end{pmatrix} \begin{pmatrix} l_{1,1} & \cdots & l_{m,1} \\ \vdots & \ddots & \vdots \\ l_{1,m} & \cdots & l_{m,m} \end{pmatrix} = d(\mathcal{S}) \begin{pmatrix} k_{1,1} & \cdots & k_{1,m} \\ \vdots & \ddots & \vdots \\ k_{m,1} & \cdots & k_{m,m} \end{pmatrix}$$

But

$$abs \begin{vmatrix} s_{1,1}^* & \cdots & s_{1,m}^* \\ \vdots & \ddots & \vdots \\ s_{m,1}^* & \cdots & s_{m,m}^* \end{vmatrix} = d(\mathcal{S})^{m-1}, \quad abs \left| d(\mathcal{S}) \begin{pmatrix} k_{1,1} & \cdots & k_{1,m} \\ \vdots & \ddots & \vdots \\ k_{m,1} & \cdots & k_{m,m} \end{pmatrix} \right| = |\det(k_{i,j})|d(\mathcal{S})^m$$

Thus  $d(\mathcal{S})|d(\mathcal{L})$  and we have  $d(\mathcal{S}) = d(\mathcal{L})$ , then  $\mathcal{L} = \mathcal{S}$ . To simplify the representation, we can write  $\mathcal{L}$  in modular form which is exact the form in the proposition.  $\square$

As a consequence, we could produce new parametric supports with a given improper index.

**Corollary 6** *Let  $S$  be a parametric support. If we add more lattice points satisfying the linear congruent equations given in Theorem 5 to  $S$ , the improper index of the new parametric support is the same as that of  $S$ .*

In practice, we could design parametric supports with a given improper index with the follow proposition.

**Proposition 9**  $\mathcal{S} = \{(x_1, \dots, x_m) \in \mathbf{Z}^m : \sum_{i=1}^m a_i x_i = 0 \pmod{p}\}$  is a lattice with  $d(\mathcal{S}) = p / \gcd(a_1, \dots, a_m, p)$ , where  $a_i, p$  are integers. For any parametric support  $S \subset \mathcal{S}$  we have  $d(\mathcal{S})|IX(S)$ .

Proof

The first part of the proposition can be directly generalized from Lemma 1 in (Nguyen, 2004). And similar to the proof of Theorem 4, we can get second part.  $\square$

By the above proposition, we can design an improper parametric support  $S$  with its improper index divisible by an integer.

### 5.1 Example: Constructing an improper parametric support

Let  $m = 3$ ,  $a_1 = 2$ ,  $a_2 = 2$ ,  $a_3 = 3$  and  $p = 4$ . Consider the parametric support  $S \subset \{(p_1, p_2, p_3) | 2p_1 + 2p_2 + 3p_3 = 0 \pmod{4}\}$ , by Proposition 9, we have  $4 | IX(S)$ . Construct a simplex parametric support as  $S = \{(0, 0, 0), (1, 1, 0), (0, 2, 0), (0, 1, 2)\}$ . By Theorem 1, we have  $IX(S) = NV(NP(S)) = 4$ , following Proposition 9.

## 6 Conclusion

We consider the proper reparametrization problem by identifying a class of parametric supports in  $\mathbf{Z}^m$  such that rational parametric equations defined on them are always improper. We therefore name them as inherently improper parametric supports. The main results of the paper are as follows:

- If the coefficients of a rational parametrization are generic or indeterminates, then the improper index of  $S$  is

$$IX(S) = \gcd\{NV(NP(S')) : S' \subseteq S, |S'| = m + 1\}$$

and we can find a proper reparametrization by constructing a support transformation.

- If the coefficients of the rational parametrization are numerical values, we can re-parameterize the parametrization such that the improper index of the new parametrization is reduced by a factor of  $IX(S)$ . Furthermore, almost all rational specialized parametrizations on a parametric support  $S$  with  $IX(S) = 1$  are proper.
- We show that improper parametric supports can be described with a set of linear congruent equations. Based on theories of lattices, we give an algorithm of reparametrization with better complexities.

## References

- Artin, M. and Mumford, D. Some elementary examples of unirational varieties which are non-rational, *Proc. London Math. Soc.*, 3, 25, 75–95, 1972.
- Castelnuovo, G. Sulla rationalita della involuzioni pinae, *Mathematische Annalen*, 44, 125–155, 1894.
- Chionh, E.W., Gao, X.S., Shen, L.Y. Inherently improper surface parametric supports, *Computer Aided Geometric Design*, 23, 629–639, 2006.
- Chionh, E.W., Goldman R.N. Degree, multiplicity and inversion formulas for rational surfaces using u-resultants, *Computer Aided Geometric Design*, 9:93–108, 1992.
- Cohen, H. A course in computational algebraic number theory, *Springer-Verlag*, 3rd, New York, 1996.
- Cox, D., Little, J., O’Shea, D. Using algebraic geometry, *Springer-Verlag*, New York, 1998.
- Diaz, S.P. On the problem of proper reparametrization for rational curves and surfaces, *Computer Aided Geometric Design*, 23, 307–323, 2006.
- Farin, G., Hoschek, J., and Kim, M.S. (eds.). Handbook of CAGD, *Elsevier*, 2002.
- Gao, X.S., Chou, S.C. Implicitization of rational parametric equations, *Journal of Symbolic Computation*, 14, 459–470, 1992.
- Gutierrez, J., Sevilla, D. Computation of unirational fields, *Journal of Symbolic Computation*, 1222–1244, 2006.
- Lenstra, A.K., Lenstra, H.W., Lovász, L. Factoring polynomials with rational coefficients, *Mathematische Annalen*, 261, 515–534, 1982.
- Li, J., Gao, X.S. The proper reparametrization of a special class of rational parametric equations, *J. of Sys. Sci. and Complexity*, 19, 331–339, 2006.
- Li, T.Y., Wang, X.S. The BKK root count in  $C^n$ , *Mathematics of computation* 65, No.216, 1477–1484, 1996.
- Nguyen, P. Q. Can we trust cryptographic software? *Proceedings of Eurocrypt ’04*, C. Cachin and J. Camenisch (eds.), LNCS 3027, 555–570, 2004.
- Pohst, M. A modification of the LLL reduction algorithm, *Journal of Symbolic Computation*, 4, 123–127, 1987.
- Schinzel, A. Polynomials with special regard to reducibility, *Cambridge University Press*, 2000.
- Sederberg, T.W. Improperly parametrized rational curves, *Computer Aided Geometric Design*, 3, 67–75, 1986.
- Sommerville, D.M.Y. Analytical geometry of three dimensions, *Cambridge University Press*, 1959.
- Van der Waerden, B.L. Einführung in die algebaischen geometrie, *Springer-Verlag*, Berlin, 1973.
- Walker, R.J. Algebraic curves, *Princeton University Press*, New Jersey, 1950.
- Wu, W.T. Mathematics mechanization, *Scinece/Kluwer Press*, Beijing, 2001.
- Zariski O. Algebraic Surfaces. Springer, Berlin, 2nd supplemented edition.