J Syst Sci Complex (2011) 24: 367–380

PROPER REPARAMETRIZATION FOR INHERENTLY IMPROPER UNIRATIONAL VARIETIES*

Liyong SHEN · Engwee CHIONH · Xiao-Shan GAO · Jia LI

DOI: 10.1007/s11424-010-7221-y
Received: 5 November 2007

Abstract In this paper, a class of lattice supports in the lattice space Z^m is found to be inherently improper because any rational parametrization from C^m to C^n defined on such a support is improper. The improper index for such a lattice support is defined to be the gcd of the normalized volumes of all the simplex sub-supports. The structure of an improper support S is analyzed and shrinking transformations are constructed to transform S to a proper one. For a generic rational parametrization RP defined on an improper support S, we prove that its improper index is the improper index of S and give a proper reparametrization algorithm for RP. Finally, properties for rational parametrizations defined on an improper support and with numerical coefficients are also considered.

Key words BKK bound, chow form, improper lattice supports, improper rational parametrizations, reparametrization, support transformation.

1 Introduction

Algebraic curves and surfaces 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 aided design and manufacturing[1]. In general, an algebraic variety admitting a rational parametrization is called unirational. A basic property of a rational parametrization is whether it is proper (one-to-one) or improper (many-to-one). If a rational parametrization RP is not proper, a generic point of the variety corresponds to $\mu > 1$ parameters. The integer μ, denoted as $IX(RP)$, is called the improper index of the rational parametrization[2−5].

Liyong SHEN
School of Mathematical Sciences, Graduate University, Chinese Academy of Sciences, Beijing 100049, *China*.
Engwee CHIONH
School of Computing, National University of Singapore, 117543, *Singapore*.
Xiao-Shan GAO
Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, *China*. Email: xgao@mmrc.iss.ac.cn.
Jia LI
Beijing Electrical Science and Technology Institute, Beijing 100070, *China*.
*This research is supported by the National Key Basic Research Project of China under Grant No. 2011CB302400 and the National Natural Science Foundation of China under Grant No. 10901163.
◇ *This paper was recommended for publication by Editor Ziming LI.*

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[6]. Effective methods to find a proper reparametrization for an improper parametrization of an algebraic curve were proposed in [7–10]. For algebraic surfaces, if the base field is algebraically closed, there always exists a proper reparametrization for an improper parametrization[11]. 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 algebraically closed fields[12].

The problem of finding a proper reparametrization for surfaces and varieties of higher dimensions is open in the general case[13]. There exist several partial results. In [14], a proper reparametrization algorithm was proposed for rational parametrizations which are improper in only one of the parameters. In [10], 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. A proper reparametrization algorithm was given for algebraic ruled surfaces in [15]. A class of inherently improper rational parametrizations was studied in [16].

In this paper, we consider the inherently improper parametric supports in the general case, that is, rational parametric mappings defined on these supports from C^m to C^n for any $m < n$ are always improper. The paper is naturally divided into two parts.

In Sections 3 and 4, we consider properties of improper lattice supports. For a given finite lattice support S in Z^m, we define its improper index $IX(S)$ to be the gcd of the normalized volumes of all the simplex sub-supports. A lattice support is called proper if and only if its support index is one. Lattice reduction algorithms from [17–18] are used to construct a support transformation which can be used to transform an improper lattice support to a proper one. The structure of an improper support S is analyzed. We show that for an improper lattice support S, we can construct a set of linear congruent equations LS such that S is a subset of the solutions of the equations $LS = 0$ and addition of any solutions of $LS = 0$ to S does not change the index of the enlarged support.

In Sections 5 and 6, we consider properties of rational parametrizations defined on a lattice support. For a generic rational parametrization $RP(S)$ defined on a lattice support S, we prove that its improper index equals the improper index of S. This gives an efficient method to compute the improper index of a rational parametrization with elementary tools. We further design an algorithm to find a proper reparametrization for $RP(S)$ 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 a rational parametrization $RP(S, C)$ defined on S with numerical coefficients C, we prove that $IX(S)$ is a factor of $IX(RP(S, C))$. We design an algorithm to find a reparametrization whose improper index is $IX(RP(S, C))/IX(S)$ and prove that for almost all coefficients (coefficients from a non empty open Zariski subset of the coefficient space) the reparametrization is proper. The results in this part are essential generalizations of the results in [16]. For algebraic surfaces in R^3, the implicit variety can be defined with an irreducible polynomial equation $f(x, y, z) = 0$. In the general case, this is not valid anymore. We need to use the Chow form of the implicit variety to overcome the difficulties. Also, the construction of the transformation is more complicated.

The rest of the paper is organized as follows. In Section 1, notations and preliminary results are given. In Section 2, the shrinking transformation for an improper lattice support is constructed. In Section 3, the structure of improper lattice supports is analyzed. In Section 4, generic rational parametrizations are considered. In Section 5, rational parametrizations with numerical coefficients are studied. Section 6 concludes the paper with a summary.

2 Preliminaries

In this section, we introduce the lattice support and define the improper index for a lattice support.

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

A finite set $S \subset Z^m$ is a non-degenerate lattice support if $NV(NP(S)) > 0$. For instance, the lattice supports with total degree less than or equal to d is

$$S = \left\{ p = (p_1, p_2, \cdots, p_m) \in Z^m : 0 \leq p_1, 0 \leq p_2, \cdots, 0 \leq p_m, |p| = \sum_{i=1}^{m} p_i \leq d \right\}.$$

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

Another example is a support with $|S| = m + 1$, which is called simplex support. Let $S = \{p_j \in Z^m : p_j = (p_{j,1}, p_{j,2}, \cdots, p_{j,m}), j = 1, 2, \cdots, m+1\}$ be a simplex support. Then

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

Any set $S' \subseteq S$ is a lattice sub-support of S if S' is also a lattice support. In particular, a sub-support S' is simplex if $|S'| = m + 1$. Simplex sub-supports are important in the study of improper supports.

We define the improper index of a support S to be

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

S is called proper if $IX(S) = 1$ and improper if $IX(S) > 1$.

To simplify our discussion, we assume the lattice support S contains the origin. Furthermore, we assume the lattice support is non-degenerate, that is, $IX(S) > 0$.

Let $T : R^m \to R^m$ be an invertible affine transformation with

$$T(p_1, p_2, \cdots, p_m) = (a_{1,0} + a_{1,1}p_1 + \cdots + a_{1,m}p_m, \cdots, a_{m,0} + a_{m,1}p_1 + \cdots + a_{m,m}p_m). \tag{2}$$

Here transformation T is a support transformation with respect to a lattice support S if $T(S)$ is also a lattice support; it holds that, $T(S) \subseteq Z^m$ and T is non-singular. The absolute value of the determinant of the Jacobian matrix of T is written as

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

Given a support transformation T for a support S, it is well-known that

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

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. In the next section, we will show that improper supports can be shrunk by support transformations.

3 Constructing a Proper Support from an Improper One

In this section, we will construct a support transformation to transform an improper lattice support to a proper one.

Let $p_0 \in Z^m$. For any set of $m+1$ lattice points $S = \{p_1, p_2, \cdots, p_{m+1}\}$, $NV(NP(S))$ is a linear combination of $NV(NP(p_0 \cup S \setminus \{p_j\}))$, $j = 1, 2, \cdots, m+1$. Thus, instead of computing the gcd of all simplex sub-supports, we only need to compute the gcds of simplex sub-supports anchored at some chosen point p_0. This observation leads to the following result.

Lemma 1 *Let S be a lattice support and $p_0 \in S$. We have*

$$IX(S) = \gcd\{NV(NP(S'')) : p_0 \in S'' \subseteq S,\ |S''| = m+1\}.$$

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

The following result shows how to construct a shrunken support for an improper support.

Theorem 1 *Let S be a lattice support containing the origin. Then there exists a support transformation T for S such that $IX(S)J(T) = 1$ and $T(S)$ is a proper lattice support.*

Proof We first introduce the following notations.

For a lattice point $p = (p_1, p_2, \cdots, p_m) \in Z^m$, the k-th projection of p is $p^{(k)} = (p_{m+1-k}, \cdots, p_m) \in Z^k$. We write $0^{(k)} = (0, 0, \cdots, 0) \in Z^k$.

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

$$A_\sigma^{(k)} = abs \begin{vmatrix} 0^{(k)} & 1 \\ p_{\sigma_1}^{(k)} & 1 \\ \vdots & \vdots \\ p_{\sigma_k}^{(k)} & 1 \end{vmatrix}, \tag{3}$$

where σ chooses k points $p_{\sigma_1}, p_{\sigma_2} \cdots, p_{\sigma_k}$ from S.

We define $g_k = \gcd_\sigma\{A_\sigma^{(k)}\},\ k = 1, 2, \cdots, m$. By Laplace expansion along the first column we see that $g_k | g_{k+1}$. Since the $IX(S) \neq 0$, g_k cannot be zero.

We now set the support transformation T as

$$\begin{aligned} &T(p_1, p_2, \cdots, p_m) \\ &= \left(\frac{g_{m-1}p_1 + \beta_{1,2}p_2 + \cdots + \beta_{1,m}p_m}{g_m}, \cdots, \frac{g_1 p_{m-1} + \beta_{m-1,m}p_m}{g_2}, \frac{p_m}{g_1} \right), \end{aligned} \tag{4}$$

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

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

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

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

By Laplace expansion along the last row, we have

$$A_{\sigma'}^{(k+1)} = A_{\sigma}^{(k)} p_{m-k} + B_{\sigma,m-k+1} p_{m-k+1} + \cdots + B_{\sigma,m} p_m, \tag{5}$$

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

Since $g_k = \gcd_\sigma\{A_\sigma^{(k)}\}$, there exist integers α_σ such that $\sum\limits_\sigma \alpha_\sigma A_\sigma^{(k)} = g_k$. But $g_{k+1} | A_{\sigma'}^{(k+1)}$ for any σ, by (5), we have

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

is an integer, where $\beta_{m-k,j} = \sum\limits_\sigma \alpha_\sigma B_{\sigma,j}$. The construction of T ensures that it is a support transformation for S. And one can find that

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

By Lemma 1 and the above construction, then we have $g_m = IX(S)$, therefore $IX(S)J(T) = 1$.

Furthermore, we have

$$\begin{aligned} IX(T(S)) &= \gcd\{NV(NP((S'')) : 0 \in S'' \subseteq T(S), |S''| = m+1\} \\ &= \gcd\{NV(NP((T(S')) : 0 \in S' \subseteq S, |S'| = m+1\} \\ &= J(T) \gcd\{NV(NP((S')) : 0 \in S' \subseteq S, |S'| = m+1\} \\ &= IX(S)J(T) = 1. \end{aligned}$$

Thus, $T(S)$ is a proper lattice support. ∎

Example 1 Let $S = \{(0,0,0), (1,1,0), (0,2,0), (0,1,2)\}$ (see Figure 1(a)), which is a simplex support. We easily find $IX(S) = NV(NP(S)) = 4$.

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

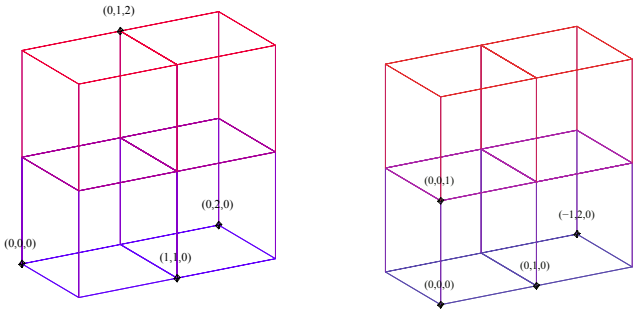
$$T(p_1, p_2, p_3) = \left(\frac{2p_1 - 2p_2 + p_3}{4}, \frac{2p_2 - p_3}{2}, \frac{p_3}{2} \right).$$

Then $T(S) = \{(0,0,0), (0,1,0), (-1,2,0), (0,0,1)\}$ and $NV(NP(T(S))) = 1$ (see Figure 1(b)).

4 Structure of Improper Lattice Support

In this section, we study the structure of an improper lattice support. This leads to a more efficient algorithm to find a proper lattice support from an improper one.

We now consider the lattice $\mathcal{S} = \text{span}(S) = \{\sum\limits_i r_i p_i : r_i \in Z, p_i \in S\}$ generated by the lattice support S as a free Z-module. Then $\mathcal{S}$ has a basis as $\{s_1, s_2, \cdots, s_m\} \in Z^m$ and determinant of



(a) improper support (b) proper support

Figure 1 support transformation

the lattice is defined by $d(\mathcal{S}) = abs(\det(s_1, s_2, \cdots, s_m))$, which does not depend on the choice of its basis[18−19].

From a full rank generating set $S \subset Z^m$, 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[17−18]. The vectors of LLL-reduced basis will be much shorter in Euclidean length and the running time is at most $\mathcal{O}(m+|S|)^4 \log \Theta, \|p\| \leq \Theta$.

Now, we can obtain the transformation of S by two steps. The first step is to find a basis of S and the second step is to construct the shrinking transformation T as in Section 2 with the basis.

Theorem 2 *Let S be a lattice support, $\mathcal{S}$ the lattice generated by S, and $B = \{s_1, s_2, \cdots, s_m\}$ a basis of $\mathcal{S}$, T_B the transformation obtained as in (4) from B. Then T_B is a support transformation for S and $T_B(S)$ is a proper lattice support.*

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

$$d(\mathcal{S}) = abs \begin{vmatrix} s_1 \\ s_2 \\ \vdots \\ s_m \end{vmatrix} = abs \begin{vmatrix} \sum_{j=1}^{|S|} \alpha_{1,j} p_j \\ \sum_{j=1}^{|S|} \alpha_{2,j} p_j \\ \vdots \\ \sum_{j=1}^{|S|} \alpha_{m,j} p_j \end{vmatrix} = \sum \beta_k NV(NP(S')),$$

where $p_j \in S, 0 \in S' \subset S, |S'| = m+1$, and $\alpha_{i,j}, \beta_k$ are integers. It means that $IX(S)|d(\mathcal{S})$. On the other hand, $\{s_1, s_2, \cdots, s_m\}$ is also a basis of S, and so we have $d(\mathcal{S})|IX(S)$. Hence, $IX(S) = d(\mathcal{S})$.

For $p \in S$, $p = \sum_{j=1}^m \alpha_j s_j$, then $T_B(p) = \sum_{j=1}^m \alpha_j T_B(s_j) \in Z^m$, which means T_B is a support transformation for S. By Theorem 1, $J(T_B) = 1/NV(NP(\{B, 0\})) = 1/d(\mathcal{S}) = 1/IX(S)$. We have $IX(T_B(S)) = 1$. ∎

The above theorem leads to a new transformation algorithm. The complexity of generating B is polynomial in $|S|$. Since $|B| = m$, if $|S|$ is much larger than m, then the new algorithm is of great advantage over the algorithm proposed in Section 2. On the other hand, if $|S|$ and m are almost the same, then we can still use the algorithm in Section 2, because that algorithm is much simpler.

The following result describes the structure of a lattice support.

Theorem 3 *Let S be a lattice support, $\mathcal{S}$ the lattice spanned by S, $\{s_1, s_2, \cdots, s_m\}$ a basis of the lattice $\mathcal{S}$. Then there exist integers $a_{i,j}$ such that $\mathcal{S} = \{(x_1, x_2, \cdots, x_m) : \sum_{j=1}^m a_{i,j} x_j =$*

0 mod $d(\mathcal{S}), 1 \le i \le m\}$.

Proof Considering the hyperplanes determined by the origin and $m-1$ points from $\{s_1, s_2, \cdots, s_m\}, s_i = (s_{i,1}, s_{i,2}, \cdots, s_{i,m})$, 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 $\mathcal{L} = \{(x_1, x_2, \cdots, x_m) \in Z^m : \sum_{j=1}^{m} s^*_{i,j} x_j = Zd(\mathcal{S}), 1 \le i \le m\}$ is a lattice. Since $\{s_1, s_2, \cdots, s_m\} \subset \mathcal{L}$, we have $\mathcal{S} \subset \mathcal{L}$ and $d(\mathcal{L}) | d(\mathcal{S})$.

Let $\{l_1, l_2, \cdots, l_m\}$ 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 so 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 Theorem 3. ∎

As a consequence, we can produce new lattice supports with a given improper index.

Corollary 1 *Let S be a lattice support. If we add more lattice points satisfying the linear congruent equations given in Theorem* 3 *to S, the improper index of the new lattice support is the same as that of S.*

In practice, we could design an improper design lattice support with its improper index divisible by a given number with the follow proposition.

Proposition 1 *Let $\mathcal{S} = \{(x_1, x_2, \cdots, x_m) \in Z^m : \sum_{i=1}^{m} a_i x_i = 0 \bmod p\}$ be a lattice with $d(\mathcal{S}) = p/\gcd(a_1, a_2, \cdots, a_m, p)$, where a_i, p are integers. For any lattice 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 2 in [20]. And similar to the proof of Theorem 2, we can get second part. ∎

Example 2 We construct an improper lattice support as follows. Let $m = 3$, $a_1 = 2, a_2 = 2, a_3 = 3$ and $p = 4$. Consider the lattice support $S \subset \{(p_1, p_2, p_3) | 2p_1 + 2p_2 + 3p_3 = 0 \bmod 4\}$, by Proposition 1, we have $4 | IX(S)$. Construct a simplex lattice support as $S = \{(0,0,0), (1,1,0), (0,2,0), (0,1,2)\}$. We have $IX(S) = NV(NP(S)) = 4$, following Proposition 1.

5 Generic Rational Parametrization on Improper Supports

In this section, we study rational parametrizations on lattice supports with generic coefficients.

5.1 Rational Parametrizations on Lattice Supports

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

$$(X_1(t), X_2(t), \cdots, X_n(t)) = \left(\frac{x_1(t)}{x_0(t)}, \cdots, \frac{x_n(t)}{x_0(t)}\right) = \frac{\sum\limits_{p\in S}(x_{1,p}, x_{2,p}, \cdots, x_{n,p})t^p}{\sum\limits_{p\in S} x_{0,p}t^p}, \tag{6}$$

where $0 \neq (x_{0,p}, x_{1,p}, \cdots, x_{n,p}) \in K^{n+1}$ are coefficients from some field $K \subseteq C$; and $t = (t_1, t_2, \cdots, t_m)$, $p = (p_1, p_2, \cdots, p_m)$, $t^p = (t_1^{p_1}, t_2^{p_2}, \cdots, t_m^{p_m})$.

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

Lemma 2 *Let S be a nonnegative lattice support. The rational parametrization $RP(S)$ on S has a bi-rational reparametrization on a lattice support S' such that S' contains the origin and is nonnegative.*

Proof Suppose $0 \notin S$. Consider the monomials t^p, $p \in S$, of least total degree $|p| = d$. 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:

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

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

$$t_1 = s_1, \quad t_2 = s_1 s_2, \quad \cdots, \quad t_m = s_1 s_m. \tag{7}$$

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 nonnegative. ∎

A rational parametrization $RP(S)$ on a lattice support S is non-degenerate if it 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 C. This loses no generality as we can always check if a rational parametrization is non-degenerate[2,9].

The following lemma states that a support transformation reparamet rizes a rational paramet -rization.

Lemma 3 *A support transformation T of a lattice support S induces a reparametrization of the original unirational variety on the lattice support $T(S)$. Furthermore, the induced reparametrization preserves the dimension of the variety since $J(T) > 0$.*

Proof Let T given by (2) be a support transformation with respect to the lattice support S. Let

$$t_1 = s_1^{a_{1,1}} s_2^{a_{2,1}} \cdots s_m^{a_{m,1}}, \ \cdots, \ t_m = s_1^{a_{1,m}} s_2^{a_{2,m}} \cdots s_m^{a_{m,m}}. \tag{8}$$

By making t a function of s, we obtain a reparametrization $RP(t(s))$ from the parametrization $RP(t)$.

Next, we show that the support of $RP(t(s))$ is $T(S)$. A direct calculation shows that the transformation changes the monomial t^p to $s^{T(p)-(a_{1,0},a_{2,0},\cdots,a_{m,0})}$. Since the parametrization is rational we may regard the transformed monomials as $s^{T(p)}$. Thus, the parametric equation $\sum_{p\in S} x_{i,p}t^p$ becomes the parametric equation $\sum_{T(p)\in T(S)} x_{i,p}s^{T(p)}$, that is, the support of $RP(t(s))$ is $T(S)$.

The transformation (8) is invertible since $J(T) > 0$, thus, the reparametrization does not change the dimension of the variety. ∎

5.2 Improper Indices of Generic Rational Parametrization

Consider a generic rational parametrization $RP(S)$ defined in (6) with generic coefficients $x_{i,p}$, $i = 0, 1, \cdots, n$, $p \in S$. This is equivalent to treating the coefficients as indeterminates. The actual algebraic degree of the implicit variety defined by (6) is denoted by $AD(RP(S))$, which is the number of generic intersection points between the implicit variety and a generic affine space of dimension $n - m$[4].

Similar to the definition of $AD(RP(S))$, we define the apparent algebraic degree of a generic rational parametrization $RP(S)$ as the number of intersection points of $RP(S)$ and a generic dimension $n - m$ affine space determined by m generic hyperplanes:

$$\begin{cases} u_{10} + u_{11}X_1 + u_{12}X_2 + \cdots + u_{1n}X_n = 0, \\ \qquad\qquad \vdots \\ u_{m0} + u_{m1}X_1 + u_{m2}X_2 + \cdots + u_{mn}X_n = 0. \end{cases} \tag{9}$$

Lemma 4 *The apparent algebraic degree of a generic rational parametrization (6) is* $NV(NP(S))$.

Proof Consider the solutions of the polynomial equations obtained by substituting (6) into (9) and multiplying $x_0(t)$:

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

The intersection points of (9) and (6) are the solutions of (10) by removing the solutions

$$\begin{cases} u_{11}x_1(t) + u_{12}x_2(t) + \cdots + u_{1n}x_n(t) = 0, \\ \qquad\qquad \vdots \\ u_{m1}x_1(t) + u_{m2}x_2(t) + \cdots + u_{mn}x_n(t) = 0, \\ x_0(t) = 0. \end{cases} \tag{11}$$

Since (11) has $m + 1$ equations with m variables, (11) has common solutions if and only if its non-identical zero resultant is zero (Theorem 2.3 on page 86 of [21]), which is impossible because the equations in (11) have generic coefficients and generic constant items without relating to the variables. So the intersection points of (9) and (6) are exactly the solutions of (10) for a generic rational parametrization.

According to a modified version of Bernstein's Theorem[22], 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. ∎

By Lemma 4, 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 a generic rational parametrization $RP(S)$ to be

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

For a generic parametrization (6) on S, the improper index $IX(RP(S))$ gives the number of parameter points $(t_1, t_2, \cdots, t_m)$ corresponding to a generic point $(X_1, X_2, \cdots, X_n)$ of the unirational variety defined by $RP(S)$. We state this fundamental property as a lemma.

Lemma 5 *For a generic rational parametrization $RP(S)$ on a lattice support S, there are $IX(RP(S))$ parametric points corresponding to a generic variety point.*

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

Lemma 6 *If there is a support transformation T for a lattice support S with $J(T) < 1$, then $RP(S)$ is improper and*

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

Proof By Lemma 3, the induced parametrization $RP(T(S))$ on the support $T(S)$ is a reparametrization of $RP(S)$ on the support S. Thus, $AD(RP(T(S))) = AD(RP(S))$ and

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

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

Example 3 $m = 3$, $n = 4$, $S = \{ (0,0,0), (2,0,0), (0,2,0), (0,0,2), (0,2,2), (2,0,2), (2,2,0), (1,1,1), (2,2,2)\}$ (Figure 2).

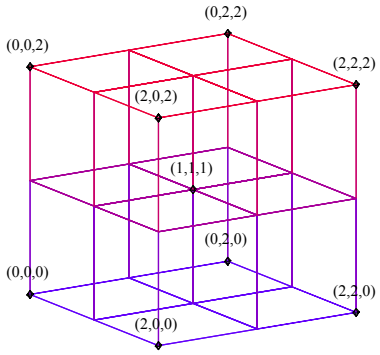


Figure 2 A lattice support of $m = 3$

By using random coefficients or otherwise, we find $AD(RP(S)) = 12$. Thus, $IX(RP(S)) = \frac{3! \times 2^3}{12} = 4$. 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 $(X_1, X_2, \cdots, X_4)$.

Lemma 7 *Let S be a simplex support, that is, $|S| = m + 1$. Then $IX(RP(S)) = NV(NP(S))$*

Proof It is easily verified that a generic rational parametrization on S gives a hyperplane, thus $AD(S) = 1$ and $IX(RP(S)) = NV(NP(S))$. ∎

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

5.3 Generic Rational Parametrization on Improper Supports

In this subsection, we prove the main result for an inherently lattice support S and the its corresponding generic rational parametrization:

$$IX(RP(S)) = IX(S).$$

The result allows us to find the improper index of a generic rational parametrization without having to compute the non-trivial algebraic degree.

First, we give a lemma about the improper index of the generic parametrization on a support and its sub-supports.

Lemma 8 *Let S be a lattice support. If $S' \subseteq S$ is a sub-support, $IX(RP(S))|IX(RP(S'))$.*

Proof To find the improper index $IX(RP(S))$ of generic rational parametrization (6), we consider $m+1$ generic hyperplanes:

$$\begin{cases} u_{00} + u_{01}X_1 + u_{02}X_2 + \cdots + u_{0n}X_n = 0, \\ u_{10} + u_{11}X_1 + u_{12}X_2 + \cdots + u_{1n}X_n = 0, \\ \qquad\qquad \vdots \\ u_{m0} + u_{m1}X_1 + u_{m2}X_2 + \cdots + u_{mn}X_n = 0. \end{cases} \tag{12}$$

The intersections of the hyperplanes and (6) are the solutions of

$$\begin{cases} u_{00}x_0(t) + u_{01}x_1(t) + u_{02}x_2(t) + \cdots + u_{0n}x_n(t) = 0, \\ u_{10}x_0(t) + u_{11}x_1(t) + u_{12}x_2(t) + \cdots + u_{1n}x_n(t) = 0, \\ \qquad\qquad \vdots \\ u_{m0}x_0(t) + u_{m1}x_1(t) + u_{m2}x_2(t) + \cdots + u_{mn}x_n(t) = 0, \end{cases} \tag{13}$$

where $x_0, x_1, \cdots, x_n$ are the parametric polynomials defined in (6). By classical elimination theory, the resultant $F(u_0, u_1, \cdots, u_m)$, $u_i = (u_{i,0}, u_{i,1}, \cdots, u_{i,n})$, of (13) with respect to $t_1, t_2, \cdots, t_m$ exists; it is known as the Chow form of (6)[4,23]. By the properties of resultants, the resultant F is homogeneous in each $u_{i,j}$ with the apparent algebraic degree of (6), which is the number of intersections of (6) and the other m hyperplanes involving u_k, $k \neq i$. Since the improper index $IX(RP(S)) = \mu$ is the multiplicity of each intersection point of (6) and any m hyperplanes of (12), we can write $F = f^{\mu}$ for some polynomial $f(u_0, u_1, \cdots, u_m)$.

Consider a sub-support $S' \subseteq S$. The sub-support S' can be obtained from S by setting indeterminate coefficients $x_{0,p}$, $x_{1,p}$, $\cdots$, $x_{n,p}$ to zero for each $p \in S \setminus S'$. 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 $f_l^{\mu_l}$ 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 $f_{l+1}^{\mu_l\nu_{l+1}}$. 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 $IX(RP(S')) = \mu\nu_1\cdots\nu_L$ and thus $IX(RP(S))|IX(RP(S'))$.

The proof is completed. ∎

Now, we are ready to prove the main result.

Theorem 4 *Let S be a lattice support. We have $IX(RP(S)) = IX(S)$.*

Proof Considering the transformation T of S in (4), we have

$$IX(T(S)) = \gcd\{NV(NP((S'')) : S'' \subseteq T(S), |S''| = m+1\} = 1.$$

By Lemma 7, we have $IX(RP(S'')) = NV(NP(S''))$ since $S'' \subseteq T(S)$ is a simplex sub-support. By Lemma 8, $IX(RP(T(S)))|IX(RP(S''))$ for all $S'' \subseteq T(S)$, so $IX(RP(T(S)))|IX(T(S))$. We now get $IX(RP(T(S))) = 1$. But by Lemma 6, $IX(RP(T(S))) = IX(RP(S))J(T)$. Thus we have $IX(RP(S)) = 1/J(T) = IX(S)$. ∎

This theorem tells that the properness of a generic rational parametrization on a support is equal to the properness of the support. And we can obtain the following theorem.

Theorem 6 *For a lattice support S, there exists a support transformation T such that $IX(RP(S))J(T) = 1$ and $RP(T(S))$ is proper. Furthermore, there exists a proper reparametrization induced by the support transformation.*

Proof According to Theorem 1, there exists a support transformation T such that $T(S)$ is proper. Then by Theorem 5, $IX(RP(S))J(T) = 1$ and $RP(T(S))$ is proper. Furthermore, by Lemma 3, transformation T induces a reparametrization. Since a rational parametrization is invariant under integer translation of $T(S)$ and and the reparametrization in Lemma 2 is bi-rational, we can get a composite proper reparametrization for $RP(S)$ on S to $RR(S')$ on S', where $RR(S')$ is proper, S' is nonnegative and contains the origin. ∎

Note that if $S' \subseteq S$ is a parametric sub-support then $IX(S)|IX(S')$. The following corollaries are immediate consequences of Theorem 5.

Corollary 2 *Let S_1,S_2, $\cdots$, S_N be sub-supports of a lattice support S. If* $\gcd(IX(S_1)$,$IX(S_2)$, $\cdots$, $IX(S_N)) = 1$, *then a generic rational parametrization $RP(S)$ is proper.*

6 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.

In this section, we consider a rational parametrization $RP(S)$ defined on a lattice support S and with numerical coefficients C. Let $IX(RP(S), C)$ be the improper index of $RP(S)$.

Theorem 7 *Let S be a lattice support, and T the transformation* (4). *Then $IX(RP(S), C) = IX(RP(T(S)), T(C))\ IX(RP(S))$, where $T(C)$ is the set of coefficients of the reparametrization by the transformation T. Consequently, if $IX(RP(S)) > 1$ then $IX(RP(S), C) > 1$.*

Proof By (8), the reparametrization introduced by T in (4) is

$$\begin{aligned} t_1 &= s_1^{\frac{g_{m-1}}{g_m}}, \\ t_2 &= s_1^{\frac{\beta_{1,2}}{g_m}} s_2^{\frac{g_{m-2}}{g_{m-1}}}, \\ &\vdots \\ t_m &= s_1^{\frac{\beta_{1,m}}{g_m}} s_2^{\frac{\beta_{2,m}}{g_{m-1}}} \cdots s_m^{\frac{1}{g_1}}. \end{aligned} \tag{14}$$

The inverse of (14) can be represented as

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

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

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 $RP(S)$. 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 $IX(RP(T(S)), T(C))$ parameter values $(s_1, s_2, \cdots, s_m)$. We may assume $s_1, s_2, \cdots, s_m \neq 0$ as this condition fails only on some lower dimensional subvariety of V. By (15), a parameter point $(s_1, s_2, \cdots, s_m)$ with $s_1, s_2, \cdots, s_m \neq 0$ leads to $\frac{g_m}{g_{m-1}} \cdots \frac{g_2}{g_1} g_1 = g_m$ parameter points $(t_1, t_2, \cdots, t_m)$. This completes the proof since $g_m = IX(RP(S))$. ∎

Theorem 8 *Let S be a proper lattice support; that is, $IX(RP(S)) = 1$. For coefficients C of* (6) *taken from a Zariski open set in the coefficient space $K^{(n+1)|S|}$, rational parametrization* (6) *is proper; that is, $IX(RP(S), C) = 1$.*

Proof By $IX(RP(S)) = 1$ and Lemma 5, the rational parametrization (6) with indeterminate coefficients is proper. By the proof of Lemma 8, the Chow form F of (6) involves $u_0 = (u_{00}, u_{01}, \cdots, u_{0n}), u_1, u_2, \cdots, u_m$. 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 $\mu = IX(RP(S), C) > 1$, the Chow form of (6) with coefficients C becomes F_C^μ. Since the specialized Chow form F_C^μ 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 $u_{01}, u_{02}, \cdots, u_{0n}$; $u_1, u_2, \cdots, u_m$. Then the coefficients of $D_{u_{00}}$ as polynomials in $u_{01}, u_{02}, \cdots, u_{0n}$; $u_1, u_2, \cdots, u_m$ should be zero. Let D be such a coefficient which is a polynomial in $x_{0,p}, x_{1,p}, \cdots, x_{n,p}$. From the above argument, we see that for a set C of numerical values of the coefficients of (6), if $D(C) \neq 0$, (6) must be proper. The required Zariski open set can be taken as $K^{(n+1)|S|} \setminus Zero(D)$. ∎

Since a Zariski open set is the whole coefficient space minus a set with lower dimensions, Theorem 8 means that for almost all numerical coefficients, transformation T in Theorem 1 gives a proper reparametrization. We state this result as a corollary.

Corollary 3 *Let S be an improper lattice support. For coefficients C of* (6) *taken from a Zariski open set in the coefficients space, the rational parametrization obtained with the transformation* (4) *is proper.*

Example 4 We give a support S with $IX(RP(S)) = 2$, $IX(RP(S), C) = 8$, $IX(RP(T(S)), T(C)) = 4$. Let $m = 2$, $S = \{1, t_1^2, t_1t_2, t_2^2, t_1^2t_2^2\}$ 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 $IX(RP(S), C) = 1$ need more subtle discussion, which is beyond the scope of this paper.

7 Conclusion

We identify a class of lattice supports in Z^m, the properness and the structure of support are considered. For improper supports, shrinking transformations are constructed. Considering the parametrization problem on the lattice supports, we prove that the rational parametric equations defined on them are always improper. And the proper reparametrization on the lattice supports can be induced by shrinking transformations. The main results of the paper are as follows.

We show that improper lattice supports can be described with a set of linear congruent

equations. And we construct shrinking support transformations for the improper supports. Based on theories of lattices, we give an algorithm of transformation with better complexities.

If the coefficients of a rational parametrization are generic or indeterminates, then the improper index of S is $IX(RP(S)) = IX(S)$. Furthermore, 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 $IX(RP(S))$. Furthermore, almost all rational specialized parametrizations on a lattice support S with $IX(RP(S)) = 1$ are proper.

References

[1] G. Farin, J. Hoschek, and M. S. Kim, *Handbook of CAGD*, Elsevier, North Holland, 2002.

[2] E. W. Chionh and R. N. Goldman, Degree, multiplicity and inversion formulas for rational surfaces using U-resultants, *Computer Aided Geometric Design*, 1992, **9**(2): 93–108.

[3] O. Zariski, *Algebraic Surfaces*, Springer, Berlin, 1995.

[4] Van der Waerden, *B. L. Einfürung in Die Algebaischen Geometrie*, Springer-Verlag, Berlin, 1973.

[5] L. Y. Shen and C. M. Yuan, Implicitization using univariate resultants, *Journal of Systems Science & Complexity*, 2010, **23**(4): 804–814.

[6] R. J. Walker, *Algebraic Curves*, Princeton University Press, New Jersey, 1950.

[7] T. W. Sederberg, Improperly parameterized rational curves, *Computer Aided Geometric Design*, 1986, **3**(1): 67–75.

[8] S. Abhyankar and C. Bajaj, Automatic Parameterization of Rational Curves and Surfaces III: Algebraic Plane Curves, *Computer Aided Geometric Design*, 1988, **5**(4): 309–321.

[9] X. S. Gao and S. C. Chou, Implicitization of rational parametric equations, *Journal of Symbolic Computation*, 1992, **14**(5): 459–470.

[10] S. Perez-Diaz, On the problem of proper reparametrization for rational curves and surfaces, *Computer Aided Geometric Desig*, 2006, **23**(4): 307–323.

[11] G. Castelnuvo, Sulla rationalita della involuzioni pinae, *Mathematische Annalen*, 1894, **44**: 125–155.

[12] M. Artin and D. Mumford, Some elementary examples of unirational varieties which are non-rational, *Proc. London Math. Soc.*, 1972, **25**(3): 75–95.

[13] A. Schinzel, *Polynomials with Special Regard to Reducibilit*, Cambridge University Press, Cambridge, 2000.

[14] J. Li and X. S. Gao, The proper reparametrization of a special class of rational parametric equations, *Jouranl of Systems Science & Complexity*, 2006, **19**(3): 331–339.

[15] J. Li, L. Y. Shen, and X. S. Gao, Proper reparametrization of rational ruled surface, *Journal of Computer Science and Technology*, 2008, **23**(2): 290–297.

[16] E. W. Chionh, X. S. Gao, and L. Y. Shen, Inherently improper surface parametric supports, *Computer Aided Geometric Design*, 2006, **23**(8): 629–639.

[17] M. Pohst, A modification of the LLL reduction algorithm, *Journal of Symbolic Computation*, 1987, **4**(1): 123–127.

[18] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, New York, 1996.

[19] A. K. Lenstra, H. W. Lenstra, and L. Lovász, Factoring polynomials with rational coefficients, *Mathematische Annalen*, 1982, **261**: 515–534.

[20] P. Q. Nguyen, Can we trust cryptographic software? *Proceedings of Eurocrypt'04,* C. Cachin and J. Camenisch (eds.), LNCS, 2004, **3027**: 555–570.

[21] D. Cox, J. Little, and D. O'Shea, *Using Algebraic Geometry*, Springer-Verlag, New York, 1998.

[22] T. Y. Li and X. S. Wang, The BKK root count in C^n, *Mathematics of Computation*, 1996, **65**(216): 1477–1484.

[23] W. T. Wu, *Mathematics Mechanization*, Scinece/Kluwer Press, Beijing, 2001.