Implicitizing Rational Curves by the Method of Moving Algebraic Curves

TOM SEDERBERG†, RON GOLDMAN‡ AND HANG DU§

†Department of Civil Engineering, Brigham Young University, Provo, UT 84602, U.S.A.
‡Department of Computer Science, Rice University, Houston, TX 77251, U.S.A.
§Department of Computer Science, Kuwait University, Safat 13060, Kuwait

(Received 8 January 1996)

A function \( F(x, y, t) \) that assigns to each parameter \( t \) an algebraic curve \( F(x, y, t) = 0 \) is called a moving curve. A moving curve \( F(x, y, t) \) is said to follow a rational curve \( x = x(t)/w(t), y = y(t)/w(t) \) if \( F(x(t)/w(t), y(t)/w(t), t) \) is identically zero.

A new technique for finding the implicit equation of a rational curve based on the notion of moving conics that follow the curve is investigated. For rational curves of degree \( 2n \) with no base points the method of moving conics generates the implicit equation as the determinant of an \( n \times n \) matrix, where each entry is a quadratic polynomial in \( x \) and \( y \), whereas standard resultant methods generate the implicit equation as the determinant of a \( 2n \times 2n \) matrix where each entry is a linear polynomial in \( x \) and \( y \). Thus implicitization using moving conics yields more compact representations for the implicit equation than standard resultant techniques, and these compressed expressions may lead to faster evaluation algorithms. Moreover whereas resultants fail in the presence of base points, the method of moving conics actually simplifies, because when base points are present some of the moving conics reduce to moving lines.

© 1997 Academic Press Limited

1. Introduction

In computer-aided geometric design there are two standard ways to represent planar curves: the rational form and the algebraic form. Both representations are valuable for geometric modeling. Parametric equations are convenient for generating points along a curve and therefore useful in rendering algorithms. Implicit equations are suitable for determining if a point lies on, inside, or outside a curve. When both representations are accessible, simple procedures are available for intersecting planar curves.

The rational and algebraic forms are related by the following well-known theorem from algebraic geometry.

**Theorem 1.1.** Every properly parametrized degree \( n \) rational curve with no base points can be represented by a unique, irreducible, implicit, degree \( n \) polynomial equation (Goldman et al., 1984; De Montaudouin and Tiller, 1984; Sederberg et al., 1984).
Finding this unique irreducible polynomial \( F(x, y) \) given the rational expressions \( x = x(t)/w(t) \) and \( y = y(t)/w(t) \) is called implicitization. In this paper, we shall be concerned with developing new implicitization techniques for properly parametrized rational curves. If a degree \( n \) rational curve is not properly parametrized—that is, if every point on the rational curve corresponds to \( p > 1 \) parameter values—then the curve can be represented by a unique, irreducible, implicit, polynomial equation of degree \( n/p \). To avoid discussing these special cases, we shall assume without further comment that throughout this paper all rational curves are properly parametrized.

Standard implicitization techniques are based on resultants (Macaulay, 1916; Van Der Waerden, 1950). Although resultants can be applied to find the implicit equation of a rational curve, implicitization methods based on resultants lead to determinants of rather large matrices. We would like to find a more compact representation for the implicit equation.

A more serious concern is that implicitization techniques based on resultants either become much more complicated or fail altogether in the presence of base points. A base point is a common root of the polynomials \( x(t), y(t), w(t) \). For rational curves a base point means that the polynomials \( x(t), y(t), w(t) \) have a common factor. We can eliminate such base points by canceling these common factors. For rational surfaces, however, base points cannot generally be removed. But base points simplify the implicit equation of a rational surface by lowering its degree (Chionh and Goldman, 1992a). We would like an implicitization method that also simplifies in the presence of base points. Unfortunately, resultants vanish in the presence of base points. The resultant can be recovered by carefully perturbing the parametric equations, but such perturbations generally introduce extraneous factors in the implicit equation which then need to be painstakingly removed (Canny, 1988; Chionh and Goldman, 1992a; Manocha and Canny, 1992). One of our main goals in trying to find new implicitization methods for rational curves is to develop simpler techniques that will be applicable to rational surfaces even in the presence of base points.

Here we investigate an observation first made by Sederberg et al. (1994) that parameterized algebraic curves and surfaces can be used to develop efficient implicitization methods for rational curves and surfaces. Empirical studies by Sederberg and Chen (1995) show that these methods work well on rational surfaces with base points. In this paper we shall concentrate on developing a rigorous theory for this novel approach to implicitizing rational curves. We reserve work on implicitizing rational surfaces for a future paper.

2. Resultants

Since we shall have occasion to use both the Sylvester and Bezout resultants, we briefly review their construction here. For further details and proofs see Goldman et al. (1984), Macaulay (1916), De Montaudouin and Tiller (1984), Van Der Waerden (1950).

Consider two degree \( n \) polynomials

\[
\begin{align*}
f(t) &= a_n t^n + \cdots + a_1 t + a_0 \\
g(t) &= b_n t^n + \cdots + b_1 t + b_0.
\end{align*}
\]

To form the Sylvester resultant of \( f(t) \) and \( g(t) \), we introduce the \( 2n \) polynomials

\[
\begin{align*}
t^k f(t) &= a_n t^{n+k} + \cdots + a_1 t^{k+1} + a_0 t^k \\
t^k g(t) &= b_n t^{n+k} + \cdots + b_1 t^{k+1} + b_0 t^k.
\end{align*}
\]
$k = 0, \ldots, n - 1$. The Sylvester resultant of $f(t)$ and $g(t)$ is the determinant of the coefficients of the polynomials $f, g, \ldots, t^{n-1}f, t^{n-1}g$.

**Theorem 2.1.** The polynomials $f(t)$, $g(t)$ have a common root if and only if the Sylvester resultant is zero (Macaulay, 1916; Van Der Waerden, 1950).

The construction of the Bezout resultant is a bit more complicated, but the end product is a more compact matrix. Let

- $f_k(t) = a_nt^k + \cdots + a_{n-k}$
- $g_k(t) = b_nt^k + \cdots + b_{n-k}$
- $p_{k+1}(t) = g_k(t)f(t) - f_k(t)g(t)$  $k = 0, \ldots, n - 1$.

Since

- $f(t) = f_k(t)t^{n-k} + a_{n-k-1}t^{n-k-1} + \cdots + a_1t + a_0$
- $g(t) = g_k(t)t^{n-k} + b_{n-k-1}t^{n-k-1} + \cdots + b_1t + b_0$

it follows that $p_1(t), \ldots, p_n(t)$ are polynomials of degree $n - 1$ in $t$. The Bezout resultant of $f(t)$ and $g(t)$ is the determinant of the coefficients of $p_1(t), \ldots, p_n(t)$. Thus while the Sylvester resultant is the determinant of a $2n \times 2n$ matrix, the Bezout resultant is the determinant of an $n \times n$ matrix. But notice that whereas the entries of the Sylvester matrix are linear in the coefficients of $f(t)$ and $g(t)$, the coefficients for the Bezout matrix are quadratic in the coefficients of $f(t)$ and $g(t)$. Explicit formulas for the entries of the Bezout resultant are given in Goldman et al. (1984).

**Theorem 2.2.** The polynomials $f(t)$, $g(t)$ have a common root if and only if the Bezout resultant is zero (Goldman et al., 1984; De Montaudouin and Tiller, 1984).

To show that the Sylvester and Bezout resultants are equivalent up to sign, we can form a collection of hybrid Sylvester–Bezout resultants $R_k$ consisting of matrices of order $(n+k) \times (n+k)$, $k = 0, \ldots, n$, composed partially of columns from the Bezout matrix and partially of columns from the Sylvester matrix. Explicitly the matrices $R_k$ are defined by setting

$R_k = \{p_{k+1}(t) \cdots p_n(t) f(t) g(t) \cdots t^{k-1}f(t) t^{k-1}g(t)\}$  $k = 0, \ldots, n$

where the entries in the column denoted by a polynomial are the coefficients of that polynomial. In particular, notice that:

i. $R_0$ is the Bezout matrix;
ii. $R_{k+1}$ is formed from $R_k$ by annexing a zero to the bottom of each column, deleting the first column, and adjoining as the last two columns the coefficients of the polynomials $t^k f(t)$ and $t^k g(t)$;
iii. $R_n$ is the Sylvester matrix.

**Proposition 2.3.**

\[ \det(R_k) = \pm \det(R_0) \quad k = 0, \ldots, n. \]
Proof. It is enough to show that $\det(R_{k+1}) = \pm \det(R_k)$, $k = 0, \ldots, n - 1$. But by construction

$$R_k = \{p_{k+1}(t) \ldots p_n(t) f(t) g(t) \ldots t^{k-1} f(t) t^{k-1} g(t)\}$$

$$R_{k+1} = \{p_{k+2}(t) \ldots p_n(t) f(t) g(t) \ldots t^k f(t) t^k g(t)\}.$$

Moreover

$$p_{k+1}(t) = g_k(t)f(t) - f_k(t)g(t)$$

$$= (b_0 t^k + \cdots + b_{n-k}) f(t) - (a_n t^k + \cdots + a_{n-k}) g(t)$$

$$= b_n t^k f(t) + \cdots + b_{n-k} f(t) - a_n t^k g(t) - \cdots - a_{n-k} g(t).$$

Thus we can form the column $p_{k+1}(t)$ by taking linear combinations of the last 2$k + 2$ columns of $R_{k+1}$. This observation allows us to use elementary column operations to replace the last column of $R_{k+1}$ by the coefficients of $p_{k+1}(t)$. This procedure changes the determinant of $R_{k+1}$ by the multiple of the last column, that is, by a factor of $a_n$. Rearranging columns, we obtain

$$a_n \det(R_{k+1}) = \pm \det(p_{k+1}(t) \ldots p_n(t) f(t) g(t) \ldots t^{k-1} f(t) t^{k-1} g(t) t^k f(t)).$$

But the last row of the matrix on the right-hand side is $(0 \ldots 0 a_n)$. Expanding this determinant by cofactors of the last row yields

$$\det(p_{k+1}(t) \ldots p_n(t) f(t) g(t) \ldots t^{k-1} f(t) t^{k-1} g(t) t^k f(t)) = \pm a_n \det(R_k).$$

Consequently

$$\det(R_{k+1}) = \pm \det(R_k) \quad k = 0, \ldots, n - 1.$$

□

Corollary 2.4.

$$\det(\text{Bezout Resultant}) = \pm \det(\text{Sylvester Resultant}).$$

Corollary 2.5. The polynomials $f(t), g(t)$ have a common root if and only if $\det(R_k) = 0$ for any $k = 0, \ldots, n$.

We shall have occasion to use these hybrid Sylvester–Bezout resultants $R_k$ later in Section 5, during our discussion of implicitization methods for rational curves with base points.

3. Bezout’s Resultant and Moving Lines

To motivate our approach to implicitization, we begin by briefly reviewing Bezout’s method for finding the implicit equation of a rational curve. Let

$$x(t) = a_n t^n + \cdots + a_1 t + a_0$$

$$y(t) = b_n t^n + \cdots + b_1 t + b_0$$

$$w(t) = d_n t^n + \cdots + d_1 t + d_0.$$

Given a rational curve $x = x(t)/w(t)$, $y = y(t)/w(t)$, we can, by cross multiplying, form two polynomials of degree $n$ in $t$ with coefficients that are linear in $x$ and $y$: 

$$xw(t) - x(t) = (xd_n - a_n) t^n + \cdots + (xd_1 - a_1) t + (xd_0 - a_0) \quad (3.1)$$
As in Section 2, from these two polynomials of degree $n$ in $t$, we generate $n$ polynomials of degree $n - 1$ in $t$ by letting

\begin{align*}
    f_k(t) &= (xd_n - a_n)t^k + \cdots + (xd_{n-k} - a_{n-k}) \\
    g_k(t) &= (yd_n - b_n)t^k + \cdots + (yd_{n-k} - b_{n-k}) \\
    p_{k+1}(t) &= g_k(t)(xw(t) - x(t)) - f_k(t)(yw(t) - y(t)) \quad k = 0, \ldots, n - 1.
\end{align*}

Since

\begin{align*}
    xw(t) - x(t) &= f_k(t)t^{n-k} + (xd_{n-k-1} - a_{n-k-1})t^{n-k-1} + \cdots + (xd_1 - a_1)t + (xd_0 - a_0) \\
    yw(t) - y(t) &= g_k(t)t^{n-k} + (yd_{n-k-1} - b_{n-k-1})t^{n-k-1} + \cdots + (yd_1 - b_1)t + (yd_0 - b_0)
\end{align*}

it follows that $p_1(t), \ldots, p_n(t)$ are polynomials of degree $n - 1$ in $t$. By equation (3.3) the polynomials $p_1(t), \ldots, p_n(t)$ vanish along the curve $x = x(t)/w(t)$, $y = y(t)/w(t)$. Moreover the coefficients of $p_k(t)$ are linear in $x$, $y$ since these coefficients are sums of terms of the form

\[(xd_i - a_i)(yd_j - b_j) - (xd_j - a_j)(yd_i - b_i) = (b_i d_j - b_j d_i)x + (a_j d_i - a_i d_j)y.\]

Thus we can write

\begin{align*}
    p_1(t) &= L_{1,n-1}(x,y)t^{n-1} + \cdots + L_{1,1}(x,y)t + L_{1,0}(x,y) \\
    & \vdots \\
    p_n(t) &= L_{n,n-1}(x,y)t^{n-1} + \cdots + L_{n,1}(x,y)t + L_{n,0}(x,y)
\end{align*}

where the functions $L_{ij}(x,y)$ are linear in $x$, $y$. The determinant of these coefficients $R(x,y) = \det(L_{ij}(x,y))$ is the Bezout resultant of the polynomials $xw(t) - x(t)$ and $yw(t) - y(t)$.

**Theorem 3.1.** When there are no base points, $R(x,y) = 0$ is the implicit equation of the rational curve $x = x(t)/w(t)$, $y = y(t)/w(t)$.

**Proof.** By Theorem 2.2, $R(x,y) = 0$ if and only if the polynomials $xw(t) - x(t)$ and $yw(t) - y(t)$ have a common root. But when there are no base points, the polynomials $xw(t) - x(t)$ and $yw(t) - y(t)$ have a common root if and only if there is a common parameter $t$ such that $x = x(t)/w(t)$ and $y = y(t)/w(t)$, i.e. if and only if the point $(x,y)$ is on the curve. Hence $R(x,y) = 0$ is the implicit equation of the rational curve $x = x(t)/w(t)$, $y = y(t)/w(t)$. $\Box$

What interests us here are not the particular details of this construction, but rather the special form of the polynomials $p_k(t)$, $k = 1, \ldots, n$. We can write each of these polynomials in one of two ways:

\begin{align*}
    L_{n-1}(x,y)t^{n-1} + \cdots + L_1(x,y)t + L_0(x,y) \\
    A(t)x + B(t)y + C(t)
\end{align*}

where $A(t)$, $B(t)$, $C(t)$ are polynomials of degree $n - 1$ in $t$. The second expression is obtained from the first by collecting the coefficients of $x$ and $y$ and recalling that the functions $L_j(x,y)$ are linear in $x$, $y$. For each value of $t$, Expression (3.5) is the
implicit form of a line in the $xy$-plane. We call such a parametrized line, a moving line. We say that a moving line $A(t)x + B(t)y + C(t) = 0$ follows a rational curve $x = x(t)/w(t), y = y(t)/w(t)$ if it vanishes on the curve—that is, if

$$A(t)x(t)/w(t) + B(t)y(t)/w(t) + C(t) = 0$$

or equivalently if

$$A(t)x(t) + B(t)y(t) + C(t)w(t) = 0$$

for all values of $t$. Geometrically a moving line follows a rational curve if the implicit line corresponding to the parameter $t$ passes through the point on the rational curve corresponding to the parameter $t$. By equation (3.3) the polynomials $p_1(t), \ldots, p_n(t)$ in the Bezout resultant represent moving lines that follow the rational curve $x = x(t)/w(t), y = y(t)/w(t)$.

### 4. Moving Lines and Implicit Equations

Bezout’s resultant for a rational curve of degree $n$ is formed from $n$ moving lines that follow the curve. Here we shall reverse engineer the Bezout determinant using the theory of moving lines. Our purpose is to show how to use the method of moving lines to derive the implicit equation of a rational curve without resorting to resultants.

We begin, in Section 4.1, by applying the method of moving lines to rational curves without base points. Our main result is Theorem 4.1, which asserts that the method of moving lines can always generate the implicit equation of a rational curve with no base points. In Section 4.2, we show how to apply Gaussian elimination to generalize the method of moving lines to implicitize rational curves with base points.

#### 4.1. The Method of Moving Lines

Given a rational curve $x = x(t)/w(t), y = y(t)/w(t)$ of degree $n$, we begin by seeking all moving lines

$$L_{n-1}(x, y)t^{n-1} + \cdots + L_1(x, y)t + L_0(x, y) = 0$$

(4.1)

of degree $n - 1$ that follow the curve. Since each coefficient $L_j(x, y)$ is linear in $x, y$, we can rewrite equation (4.1) as

$$(A_{n-1}x + B_{n-1}y + C_{n-1})t^{n-1} + \cdots + (A_1x + B_1y + C_1)t + (A_0x + B_0y + C_0) = 0. \quad (4.2)$$

In equation (4.2), there are $3n$ unknowns $A_k, B_k, C_k, k = 0, \ldots, n-1$. We can generate $2n$ homogeneous linear equations in these $3n$ unknowns by substituting for $x$ and $y$ the rational functions $x(t)/w(t)$ and $y(t)/w(t)$ and multiplying through by $w(t)$. This yields the equation

$$(A_{n-1}x(t) + B_{n-1}y(t) + C_{n-1}w(t))t^{n-1} + \cdots + (A_0x(t) + B_0y(t) + C_0w(t)) = 0 \quad (4.3)$$

where the left-hand side is a polynomial in $t$ of degree $2n - 1$. For equation (4.2) to represent a moving line that follows the rational curve, this polynomial must be identically zero. The vanishing of this polynomial leads to $2n$ homogeneous linear equations in these $3n$ unknowns, which in matrix form can be written as

$$[x \ y \ w \ \ldots \ t^{n-2}x \ t^{n-1}y \ t^{n-1}w] \cdot [A_0 \ B_0 \ C_0 \ \ldots \ A_{n-1} \ B_{n-1} \ C_{n-1}]^T = 0,$$

where the rows of the coefficient matrix $[x \ y \ w \ \ldots \ t^{n-2}x \ t^{n-1}y \ t^{n-1}w]$ are indexed by
the powers of \( t \) and the columns are the coefficients of the polynomials \( t^k x, t^k y, t^k w \),
\( k = 0, \ldots, n - 1 \).

A homogeneous linear system of \( 2n \) equations in \( 3n \) unknowns has at least \( n \) linearly
independent solutions. Let

\[
\begin{align*}
p_1(t) &= L_{1,n-1}(x, y)t^{n-1} + \cdots + L_{1,1}(x, y)t + L_{1,0}(x, y) = 0 \\
\vdots \\
p_n(t) &= L_{n,n-1}(x, y)t^{n-1} + \cdots + L_{n,1}(x, y)t + L_{n,0}(x, y) = 0
\end{align*}
\]

be \( n \) linearly independent solutions, and form the matrix \( R(x, y) = (L_{ij}(x, y)) \). Since
\( L_{ij}(x, y) \) is linear in \( x \) and \( y \), \( \det\{R(x, y)\} \) is a polynomial of degree \( n \) in \( x \) and \( y \). Moreover \( \det\{R(x, y)\} = 0 \) when \( x, y \) is on the rational curve because by equation (4.4) when \( x, y \) is
on the curve, the columns of \( R(x, y) \) are dependent. Thus by Theorem 1.1, \( \det\{R(x, y)\} = 0 \)
is a good candidate for the implicit equation of the rational curve, since \( \det\{R(x, y)\} \) has
the correct degree and vanishes on the curve. The following theorem asserts that as long as
we choose the moving lines \( p_1(t), \ldots, p_n(t) \) to be linearly independent, \( \det\{R(x, y)\} = 0 \)
is indeed the implicit equation of the rational curve, provided that there are no base points.
We call this method of finding the implicit equation of a rational curve, the method of
moving lines.

**Theorem 4.1.** The method of moving lines always generates the correct implicit equation
of a rational curve, provided that the rational curve has no base points.

**Proof.** We shall make use of both the Sylvester and the Bezout resultants. First recall
that the rows of the Bezout resultant for the polynomials \( xw(t) - x(t), yw(t) - y(t) \) are
moving lines of degree \( n - 1 \) that follow the curve. Since by Theorem 3.1 when there
are no base points the determinant of the Bezout matrix is the implicit equation of the
rational curve, we know that these rows must be linearly independent; otherwise this
determinant would be identically zero. To prove that the method of moving lines always
works, we shall show that when there are no base points, there are never more than \( n \)
linearly independent moving lines of degree \( n - 1 \) that follow a degree \( n \) rational curve.
Consider then the system of \( 2n \) homogeneous linear equations in \( 3n \) unknowns which
we need to solve to find the moving lines that follow the curve. In matrix form these
equations are:

\[
[x \ y \ w \ldots t^{n-1}x \ t^{n-1}y \ t^{n-1}w] \cdot [A_0 \ B_0 \ C_0 \ldots A_{n-1} \ B_{n-1} \ C_{n-1}]^T = 0.
\]

Let \( C = [x \ y \ w \ldots t^{n-1}x \ t^{n-1}y \ t^{n-1}w] \) be the coefficient matrix. To prove that there are
never more than \( n \) linearly independent moving lines that follow a degree \( n \) rational curve,
we must show that \( C \) has rank \( 2n \). To do so, let \( x^* (t) = x(t) + xt^{2n}, y^*(t) = y(t) + yt^{2n}, \)
\( w^*(t) = w(t) + t^{2n} \), and let \( S \) denote the \( 3n \times 3n \) matrix
\( S = [x^* \ y^* \ tx^* \ ty^* \ldots t^{n-1}x^* \ t^{n-1}y^* \ w^* \ tw^* \ldots t^{n-1}w^*] \). Note that \( C \) is a submatrix
of \( S \) with its columns rearranged. But \( \det(S) \) is the Sylvester resultant of \( xw(t) - x(t) \) and
\( yw(t) - y(t) \). To prove this assertion, subtract \( x column(t^k w^*) \) from \( column(t^k x^*) \) and
\( y column(t^k w^*) \) from \( column(t^k y^*) \), \( k = 0, \ldots, n - 1 \). This procedure leaves the determi-
nant unchanged, kills off the \( x \)'s and \( y \)'s in the rows below the row indexed by \( t^{2n-1} \),
and produces the matrix
\[
\begin{pmatrix}
\text{Sylvester matrix of } xw(t) - x(t) \text{ and } yw(t) - y(t) & * \\
0 - \text{matrix} & \text{Identity matrix}
\end{pmatrix}
\]
whose determinant is indeed just the Sylvester resultant of \(xw(t) - x(t)\) and \(yw(t) - y(t)\). Since there are no base points, \(xw(t) - x(t)\) and \(yw(t) - y(t)\) do not have common roots for arbitrary values of \(x\) and \(y\). Therefore the Sylvester resultant of \(xw(t) - x(t)\) and \(yw(t) - y(t)\) is not identically zero. Hence \(\det(S) \neq 0\), so the rows of \(S\) are linearly independent. Hence the rows of \(C\) must also be linearly independent, so \(C\) has rank 2\(n\). Since \(C\) has full rank, we conclude that the number of linearly independent solutions of equation (4.2) (i.e. the number of linearly independent moving lines that follow the curve) is exactly \(n\). Thus the rows of the Bezout resultant span the solution space. Hence there is a constant nonsingular matrix \(M\) such that \(R(x, y) = M \times \text{Bezout Matrix}\). Since \(M\) is nonsingular, \(\det(R(x, y)) = 0\) if and only if \(\det(\text{Bezout Matrix}) = 0\). Hence \(\det(R(x, y)) = 0\) is indeed the implicit equation of the rational curve. \(\square\)

### 4.2. The Method of Moving Lines in the Presence of Base Points

By Theorem 4.1 the method of moving lines always succeeds when there are no base points. However if base points are present, then the method must be modified because a degree \(n\) rational curve with \(r\) base points is represented by an algebraic curve of degree \(n - r\). Of course, for rational curves we could remove these base points by canceling common factors in \(x(t), y(t), w(t)\). But removing common factors may not work well in floating point arithmetic. Moreover, our ultimate goal is to understand how to apply these implicitization techniques to rational surfaces, where base points cannot be removed. Therefore we are now going to explore how to utilize the method of moving lines for rational curves with base points without removing common factors.

Suppose then that \(x = x(t)/w(t), y = y(t)/w(t)\) is a degree \(n\) rational curve with \(r\) base points. Then \(x(t), y(t), w(t)\) have a common factor \(c(t)\) of degree \(r\); that is,
\[
ex = c(t)x^*(t) \quad y = c(t)y^*(t) \quad w(t) = c(t)w^*(t).
\]
To apply the method of moving lines, we need to know how many moving lines of degree \(n - 1\) follow this rational curve. A moving line of degree \(n - 1\) follows a degree \(n\) rational curve when the left-hand side of equation (4.3) is identically zero. Canceling out the common factor \(c(t)\), we obtain
\[
(A_{n-1}x^*(t) + B_{n-1}y^*(t) + C_{n-1}w^*(t))t^{n-1} + \cdots + (A_0x^*(t) + B_0y^*(t) + C_0w^*(t)) = 0
\]
where the left-hand side is a polynomial of degree \(2n - r - 1\). The vanishing of this polynomial leads to \(2n - r\) homogeneous linear equations in the \(3n\) unknowns, \(A_k, B_k, C_k, k = 0, \ldots, n - 1\). Now a linear system of \(2n - r\) homogeneous equations in \(3n\) unknowns has at least \(n + r\) linearly independent solutions. Let
\[
p_1(t) = L_{1,n-1}(x, y)t^{n-1} + \cdots + L_{1,1}(x, y)t + L_{1,0}(x, y) = 0
\]
\[
\vdots
\]
\[
p_{n+r}(t) = L_{n+r,n-1}(x, y)t^{n-1} + \cdots + L_{n+r,1}(x, y)t + L_{n+r,0}(x, y) = 0
\]
be \(n + r\) linearly independent solutions, and form the \((n + r) \times n\) matrix \(R(x,y) = (L_{ij}(x,y))\). Our goal is to show how to use the matrix \(R(x,y)\) to recover the implicit equation of the rational curve. The key idea is to apply Gaussian elimination.

Since \(p_k(t)\) follows the rational curve, the line \(p_k(0) = L_{k,0}(x,y)\) must pass through the point \((x(0)/w(0), y(0)/w(0))\). Therefore the lines \(L_{k,0}(x,y), k = 1, \ldots, n + r,\) are concurrent, so any three of these lines are linearly dependent. Thus by Gaussian elimination we can zero out all but the first two elements in the last column of \(R(x,y)\). Since the rows of this new matrix are linear combinations of moving lines that follow the curve, these rows are again moving lines that follow the curve. If we remove the first two rows and last column of this matrix, then the remaining moving lines have the form

\[
\Lambda_k(t) = \Lambda_{k,n-1}(x,y)t^{n-1} + \cdots + \Lambda_{k,1}(x,y)t.
\]

Factoring out \(t\), we obtain an \((n + r - 2) \times (n - 1)\) matrix of \(n + r - 2\) moving lines of degree \(n - 2\) that follow the curve. Repeating this Gaussian elimination \(r\) times, we arrive at \(n - r\) moving lines of degree \(n - r - 1\) that follow that curve.

**Theorem 4.2.** Let \(S(x,y)\) be the \((n - r) \times (n - r)\) matrix generated from \(R(x,y)\) by Gaussian elimination. Then \(\det(S(x,y)) = 0\) is the implicit equation of the rational curve.

**Proof.** By construction, the rows of \(R(x,y)\) are linearly independent. Since \(S(x,y)\) is generated from \(R(x,y)\) by Gaussian elimination, the rows of \(S(x,y)\) must also be linearly independent. Thus the rows of \(S(x,y)\) represent \(n - r\) linearly independent moving lines of degree \(n - r - 1\) that follow the degree \(n - r\) rational curve \(x = x^*/w^*(t), y = y^*/w^*(t)\). But this rational curve has no base points. By Theorem 4.1, the method of moving lines always generates the implicit equation of a rational curve with no base points; that is, the determinant of any set of \(n - r\) linearly independent moving lines of degree \(n - r - 1\) represents the implicit equation of a rational curve of degree \(n - r\) with no base points. Therefore \(\det(S(x,y)) = 0\) must be the implicit equation of the rational curve \(x = x^*(t)/w^*(t), y = y^*(t)/w^*(t)\), and hence too the implicit equation of the original rational curve. \(\Box\)

While Theorems 4.1 and 4.2 are interesting they do not really provide us with a new form for the implicit equation of a rational curve. We do not need to solve lots of equations with lots of unknowns to produce an \(n \times n\) determinant that represents the implicit equation of a degree \(n\) rational curve with no base points. We can simply use the Bezout resultant, where explicit formulas for the entries are known, to find the implicit equation in this form. In fact, as we showed in the proof of Theorem 4.1, the rows of the matrix generated by the method of moving lines are just linear combinations of the rows of the Bezout resultant. Moreover, we do not need Theorem 4.2 to implicitize rational curves with base points. In exact arithmetic, it is much easier simply to remove the base points and again apply the Bezout resultant. In floating point arithmetic, where calculating and canceling common factors may be difficult, we can use the fact that the determinant of the maximal non-zero minor of the Bezout resultant corresponds to the implicit equation of the rational curve (Manocha and Krishnan, 1996). In any event, it is not necessary to solve lots of equations with lots of unknowns to produce an \((n - r) \times (n - r)\) determinant that represents the implicit equation of a degree \(n\) rational curve with \(r\) base points. Nevertheless, that the method of moving lines always works
is very suggestive. In the next section we shall explore a higher order extension of this technique which does generate new, more compact, forms for the implicit equation.

5. Moving Conics and Implicit Equations

Since the method of moving lines is equivalent to the Bezout resultant, this method does not provide us with an essentially new form for the implicit equation of a rational curve. We are now going to use moving conics to implicitize rational curves. This approach does lead to a novel way of representing the implicit equation of a rational curve. We begin, in Section 5.1, by applying the method of moving conics to rational curves without base points. Here our main result is Theorem 5.4, which provides a necessary and sufficient condition for the method of moving conics to implicitize a rational curve with no base points successfully. In Section 5.2, we relate this condition to the singularities of the rational curve. Section 5.3 is devoted to rational curves with base points. Our main result here is Theorem 5.13, which provides a sufficient condition for the method of moving conics to implicitize a rational curve with base points successfully.

To simplify our discussion, we shall assume throughout this section that our rational curves have degree 2

5.1. the method of moving conics

We call a parametrized implicit equation for a line a moving line. Similarly, we call a parametrized implicit equation for a conic section a moving conic. A moving conic of degree n − 1 can be written in two ways:

\[ A(t)x^2 + B(t)xy + C(t)y^2 + D(t)x + E(t)y + F(t) = 0 \]  \hspace{1cm} (5.1)

\[ C_{n-1}(x,y)t^{n-1} + \cdots + C_1(x,y)t + C_0(x,y) = 0. \]  \hspace{1cm} (5.2)

Here \( A(t), B(t), C(t), D(t), E(t), F(t) \) are polynomials of degree \( n-1 \) in \( t \), and the functions \( C_{n-1}(x,y), \ldots, C_1(x,y), C_0(x,y) \) are second degree polynomials in \( x \) and \( y \). Equation (5.2) is obtained from equation (5.1) by collecting the coefficients of the powers of \( t \). As with moving lines, we say that a moving conic \( A(t)x^2 + B(t)xy + C(t)y^2 + D(t)x + E(t)y + F(t) = 0 \) follows a rational curve \( x = x(t)/w(t), \ y = y(t)/w(t) \) if it vanishes on the curve—that is, if

\[ A(t)x^2(t) + B(t)x(t)y(t) + C(t)y^2(t) + D(t)x(t)w(t) + E(t)y(t)w(t) + F(t)w^2(t) = 0. \]

Geometrically a moving conic follows a rational curve if the implicit conic corresponding to the parameter \( t \) passes through the point on the rational curve corresponding to the parameter \( t \).

Since each coefficient \( C_j(x,y) \) is quadratic in \( x, y \), we can rewrite equation (5.2) as

\[ (A_{n-1}x^2 + B_{n-1}xy + C_{n-1}y^2 + D_{n-1}x + E_{n-1}y + F_{n-1})t^{n-1} \]

\[ \vdots \]

\[ + (A_0x^2 + B_0xy + C_0y^2 + D_0x + E_0y + F_0) = 0. \]  \hspace{1cm} (5.3)

To use moving conics to find the implicit equation of a rational curve, we begin by asking how many moving conics of degree \( n-1 \) follow a rational curve of degree \( 2n \)? To answer this question, we proceed just as we did with moving lines.

Equation (5.3) has \( 6n \) unknowns—\( A_k, B_k, C_k, D_k, E_k, F_k, k = 0, \ldots, n-1 \). We can
generate $5n$ homogeneous linear equations in these $6n$ unknowns by substituting for $x$ and $y$ the rational functions $x(t)/w(t)$ and $y(t)/w(t)$ and multiplying through by $w^2(t)$. This yields the equation

\[
(A_{n-1}x^2(t) + B_{n-1}x(t)y(t) + C_{n-1}y^2(t) + D_{n-1}x(t)w(t) + E_{n-1}y(t)w(t) + F_{n-1}w^2(t))t^{n-1} + \cdots + (A_0x^2(t) + B_0x(t)y(t) + C_0y^2(t) + D_0x(t)w(t) + E_0y(t)w(t) + F_0w^2(t)) = 0. 
\] (5.4)

Since $x(t), y(t), w(t)$ are polynomials of degree $2n$ in $t$, the left-hand side is a polynomial in $t$ of degree $5n - 1$. For equation (5.3) to represent a moving conic that follows the rational curve, this polynomial must be identically zero. The vanishing of this polynomial leads to $5n$ homogeneous linear equations in these $6n$ unknowns, which in matrix form can be written as

\[
[x^2 \ y^2 \ xw \ yw \ w^2 \ \cdots \ t^{n-1}xw \ t^{n-1}yw \ t^{n-1}w^2] \cdot [A_0 \ B_0 \ \ldots \ A_{n-1} \ B_{n-1} \ C_{n-1}]^T = 0.
\]

As usual, here the rows of the coefficient matrix are indexed by the powers of $t$ and the columns are the coefficients of the polynomials $t^k x^2, t^k y^2, t^k x w, t^k y w, t^k w^2, k = 0, \ldots, n - 1$.

A homogeneous linear system of $5n$ equations in $6n$ unknowns has at least $n$ linearly independent solutions. Let

\[
q_1(t) = C_{1,n-1}(x,y)t^{n-1} + \cdots + C_{1,1}(x,y)t + C_{1,0}(x,y) = 0 \\
\vdots \\
q_n(t) = C_{n,n-1}(x,y)t^{n-1} + \cdots + C_{n,1}(x,y)t + C_{n,0}(x,y) = 0
\] (5.5)

be $n$ linearly independent solutions, and form the $n \times n$ matrix $C(x,y) = (C_{ij}(x,y))$. Since each coefficient $C_{ij}(x,y)$ is quadratic in $x$ and $y$, $\det(C(x,y))$ is a polynomial of degree $2n$ in $x$ and $y$. Moreover $\det(C(x,y)) = 0$ when $x, y$ is on the rational curve because by equation (5.5) when $x, y$ is on the curve, the columns of $C(x,y)$ are dependent. Thus by Theorem 1.1, $\det(C(x,y)) = 0$ is a good candidate for the implicit equation of the rational curve.

Unlike the method of moving lines, the method of moving conics does not always yield the implicit equation of the rational curve, even if there are no base points, because for some curves $\det(C(x,y))$ is identically zero. We now seek a necessary and sufficient condition for the method of moving conics to generate the implicit equation of a rational curve with no base points. We begin with some technical results.

**Lemma 5.1.** Let $x = x(t)/w(t)$, $y = y(t)/w(t)$ be a rational curve of degree $2n$ with no base points. Then there is a projective transformation

\[
x^*(t) = a_1x(t) + b_1y(t) + c_1w(t) \\
y^*(t) = a_2x(t) + b_2y(t) + c_2w(t) \\
w^*(t) = a_3x(t) + b_3y(t) + c_3w(t)
\]

such that

i. $\text{degree}(x^*(t)) = 2n$,
ii. $x^*(t)$ is one of the functions $x(t), y(t), w(t)$,
iii. \( y^*(t) \neq x^*(t) \) is one of the functions \( x(t), y(t), w(t) \),
iv. \( w^*(t) \) is not the zero polynomial,
v. \( x^*(t) \) and \( w^*(t) \) have no common factors.

**Proof.** Since \( x = x(t)/w(t) \), \( y = y(t)/w(t) \) is a rational curve of degree \( 2n \), at least one of the polynomials \( x(t), y(t), w(t) \) must have degree \( 2n \). Reordering the coordinate functions if necessary, we can assume that \( \deg(x(t)) = 2n \). Moreover it cannot be that \( y(t) \) and \( w(t) \) are both the zero polynomial because then the parametrization would have base points at the roots of \( x(t) \). Reordering the coordinate functions again if necessary, we can assume that \( w(t) \) is not the zero polynomial. In addition, \( y(t) \neq x(t) \) for otherwise the original curve would be a straight line with an improper parametrization, contrary to our prevailing hypothesis. Now if \( x(t) \) and \( w(t) \) have no common roots we are done. Suppose then that \( x(t) \) and \( w(t) \) have some common roots. Since the parametrization has no base points, none of these common roots can be a root of \( y(t) \). Let \( x^*(t) = x(t) \), \( y^*(t) = y(t) \), and \( w^*(t) = ay(t) + bw(t) \). Then there must exist values of \( a \) and \( b \) for which \( x^*(t) \) and \( w^*(t) \) have no common root; otherwise \( x(t), y(t), w(t) \) would have a common root, contradicting the fact that the parametrization has no base point. Hence \( x^*(t), y^*(t), w^*(t) \) satisfy the five required properties. \( \square \)

**Proposition 5.2.** Suppose that \( x = x(t)/w(t), y = y(t)/w(t) \) is a rational curve of degree \( 2n \) with no base points. Let

\[
N = (x^2 \ y^2 \ xy \ wx \ yw \ yw \ x^2 \ t^{n-1}x^2 \ t^{n-1}xy \ t^{n-1}y^2 \ t^{n-1}xy \ t^{n-1}yw \ t^{n-1}w^2)
\]

denote the \( 5n \times 6n \) matrix whose columns are the coefficients of the polynomials \( t^kx^2, t^ky^2, t^kxy, t^kxy, t^kwy, t^kw^2, k = 0, \ldots, n - 1 \), and let

\[
M = (x \ y \ w \ tx \ ty \ tw \ \ldots \ t^{n-1}x \ t^{n-1}y \ t^{n-1}w)
\]

denote the \( 3n \times 3n \) matrix whose columns are the coefficients of the polynomials \( t^kx, t^ky, t^kw, k = 0, \ldots, n - 1 \). Then

\[
\text{rank}(N) \geq 2 \text{rank}(M) - n.
\]

**Proof.** The rank of \( M \) is equal to the number of linearly independent polynomials \( t^kx^2, t^kxy, t^ky^2, t^kxy, t^kwy, t^kw^2, k = 0, \ldots, n - 1 \). Without loss of generality, we can assume that:

i. \( \deg(x(t)) = 2n \),

ii. \( w(t) \) is not the zero polynomial,

iii. \( x(t) \) and \( w(t) \) have no common factors;

otherwise, using Lemma 5.1, we can replace the given rational curve with a projective transformation of the curve that satisfies properties i,ii,iii without changing the rank of \( M \) or \( N \).

Since \( x(t) \) and \( w(t) \) have no common factor, the polynomials \( t^kx, t^kw, k = 0, \ldots, n - 1 \), are linearly independent. For suppose to the contrary that they are linearly dependent. Then there must be constants \( a_k, b_k, k = 0, \ldots, n - 1 \), such that

\[
\sum a_k t^kx(t) + \sum b_k t^kw(t) = 0.
\]
Let $p(t) = \Sigma a_k t^k$ and $q(t) = \Sigma b_k t^k$. Then $\text{degree}(p(t)) = \text{degree}(q(t)) = n - 1$ and 
\[
p(t)x(t) + q(t)w(t) = 0.
\]

Since $x(t)$ and $w(t)$ have no common factors, every factor of $x(t)$ must be a factor of $q(t)$. But $\text{degree}(x(t)) = 2n$ and $\text{degree}(q(t)) = n - 1$. Hence $q(t) = 0$. But now $p(t)x(t)$ must be identically zero. Since $x(t)$ is not the zero polynomial, it follows that $p(t) = 0$. Hence $a_k = b_k = 0$, $k = 0, \ldots, n - 1$, so $t^k x, t^k w$, $k = 0, \ldots, n - 1$, are linearly independent. Thus $\text{rank}(M) \geq 2n$.

Suppose that $\text{rank}(M) = 2n + p$. We already know that the columns of $M$ representing the polynomials $t^k x, t^k w$, $k = 0, \ldots, n - 1$, are linearly independent. Therefore there are $p$ columns of $M$, representing polynomials $t^{k_1} y, \ldots, t^{k_p} y$, such that the polynomials $t^k x, t^k w$, $k = 0, \ldots, n - 1$, and $t^{k_1} y, \ldots, t^{k_p} y$ are linearly independent. We shall show that the $3n + 2p$ columns of $N$ corresponding to the polynomials
\[
t^n x w, t^n w^2, t^n x^2, \quad k = 0, \ldots, n - 1 \quad \text{and} \quad t^{k_1} y w, \ldots, t^{k_p} y w, t^{k_1} x w, \ldots, t^{k_p} x w
\]
are linearly independent. For suppose to the contrary that they are linearly dependent. Then by taking linear combinations of these columns, we can find polynomials $a(t), b(t), c(t), q(t), r(t)$ of degree less than or equal to $n - 1$ such that
\[
(a(t)x(t) + b(t)y(t) + c(t)w(t))w(t) + (q(t)x(t) + r(t)y(t))x(t) = 0. \quad (*)
\]
Since $w(t)$ and $x(t)$ have no common factors, $x(t)$ must divide the coefficient of $w(t)$. Therefore there must be a polynomial $u(t)$ of degree $n - 1$ such that 
\[
a(t)x(t) + b(t)y(t) + c(t)w(t) = u(t)x(t).
\]
But by assumption the columns of $N$ represented by the polynomials $t^k x, t^k w$, $k = 0, \ldots, n - 1$, and $t^{k_1} y, \ldots, t^{k_p} y$ on the left- and right-hand sides of this equation are linearly independent. Hence it must be that $b(t) = c(t) = 0$. Thus by $(*)$
\[
a(t)x(t)w(t) + (q(t)x(t) + r(t)y(t))x(t) = 0.
\]
Since $x(t)$ is not the zero polynomial, it follows by factoring out $x(t)$ that
\[
a(t)w(t) + q(t)x(t) + r(t)y(t) = 0.
\]
But again the columns of $N$ represented by these polynomials are linearly independent. Hence it must be that $a(t) = q(t) = r(t) = 0$. Thus the $3n + 2p$ columns of $N$ corresponding to the polynomials
\[
t^n x w, t^n w^2, t^n x^2, \quad k = 0, \ldots, n - 1 \quad \text{and} \quad t^{k_1} y w, \ldots, t^{k_p} y w, t^{k_1} x w, \ldots, t^{k_p} x w
\]
are linearly independent. Therefore 
\[
\text{rank}(N) \geq 3n + 2p = 2(2n + p) - n = 2\text{rank}(M) - n.
\]
\[\square\]

**Proposition 5.3.** Let $x = x(t)/w(t)$, $y = y(t)/w(t)$ be a rational curve of degree $2n$. Then there are $p$ linearly independent moving lines of degree $n - 1$ that follow the curve if and only if 
\[
\text{rank}(x y w t x t y w \ldots t^{n-1} x t^{n-1} y t^{n-1} w) = 3n - p.
\]
In particular, there is a moving line of degree $n - 1$ that follows the curve if and only if 
\[
\det(x y w t x t y w \ldots t^{n-1} x t^{n-1} y t^{n-1} w) = 0.
\]
Proof. To find moving lines of degree \( n - 1 \) that follow the rational curve \( x = x(t)/w(t), \ y = y(t)/w(t) \), we must solve the following system of linear equations:

\[
[x \ y \ w \ldots t^{n-1}x \ t^{n-1}y \ t^{n-1}w] \cdot [A_0 \ B_0 \ C_0 \ldots A_{n-1} \ B_{n-1} \ C_{n-1}]^T = 0,
\]

where the rows of the \( 3n \times 3n \) coefficient matrix \([x \ y \ w \ldots t^{n-1}x \ t^{n-1}y \ t^{n-1}w]\) are indexed by the powers of \( t \) and the columns are the coefficients of the polynomials \( t^kx, t^ky, t^kw, \ k = 0, \ldots, n - 1 \). The number of linearly independent solutions of this system is equal to the rank of the null space of the coefficient matrix. Therefore there are \( p \) linearly independent moving lines of degree \( n - 1 \) that follow the curve if and only if

\[
\text{rank}(x \ y \ w \ tx \ ty \ tw \ldots t^{n-1}x \ t^{n-1}y \ t^{n-1}w) = 3n - p.
\]

\[\square\]

We are now ready to derive a necessary and sufficient condition for the method of moving conics to generate the implicit equation of an even degree rational curve.

Theorem 5.4. The method of moving conics generates the implicit equation for a rational curve of degree \( 2n \) with no base points if and only if there is no moving line of degree \( n - 1 \) that follows the curve. Moreover, when there is a moving line of degree \( n - 1 \) that follows the curve, any determinant generated by the method of moving conics is identically zero.

Proof. Suppose there are \( p > 0 \) moving lines of degree \( n - 1 \) that follow a degree \( 2n \) rational curve \( x = x(t)/w(t), \ y = y(t)/w(t) \) with no base points. Let

\[
M = (x \ y \ w \ tx \ ty \ tw \ldots t^{n-1}x \ t^{n-1}y \ t^{n-1}w)
\]
denote the \( 3n \times 3n \) matrix whose columns are the coefficients of the polynomials \( t^x, t^y, t^w, \ k = 0, \ldots, n - 1 \). If there are \( p \) linearly independent moving lines of degree \( n - 1 \) that follow the curve, then by Proposition 5.3 \( \text{rank}(M) = 3n - p \). Let

\[
N = (x^2 \ xy \ y^2 \ xw \ yw \ w^2 \ldots t^{n-1}x^2 \ t^{n-1}xy \ t^{n-1}y^2 \ t^{n-1}xw \ t^{n-1}yw \ t^{n-1}w^2)
\]
denote the \( 5n \times 6n \) matrix whose columns are the coefficients of the polynomials \( t^x, t^y, t^w, t^{kx}, t^{ky}, t^{kxw}, t^{kxy}, t^{kwy}, t^{kw}, \ k = 0, \ldots, n - 1 \). Then by Proposition 5.2, \( \text{rank}(N) \geq 5n - 2p \). Therefore there are at most \( n + 2p \) linearly independent conics of degree \( n - 1 \) that follow the curve.

Now each moving line of degree \( n - 1 \) that follows the curve generates 3 linearly independent moving conics of degree \( n - 1 \) that follow the curve, because we can multiply each such moving line by either \( x \) or \( y \) or \( w \) to form \( 3 \) moving conics. Hence \( 3p \) out of the potential \( n + 2p \) conics are generated by moving lines. Therefore in any collection of \( n \) linearly independent moving conics of degree \( n - 1 \) that follow the curve at least \( p \) must be generated from moving lines; that is, at least \( p \) are of the form \( f(x, y)L(x, y, t) \), where \( f(x, y) \) is a linear polynomial and \( L(x, y, t) \) is a moving line that follows the curve. Let \( C(x, y) \) be a matrix containing \( n \) linearly independent moving conics that follow the curve. Then \( \det(C(x, y)) = f_1(x, y) \cdots f_p(x, y) \det(C^*(x, y)) \), where \( C^*(x, y) \) is the matrix \( C(x, y) \) with the polynomials \( f_1(x, y), \ldots, f_p(x, y) \) factored out of their corresponding rows. Thus \( \det(C(x, y)) \) factors into \( p \) linear factors and one factor of degree \( 2n - p \). But by Theorem 1.1, the implicit polynomial representing the rational curve must be an irreducible polynomial of degree \( 2n \). Hence \( \det(C(x, y)) = 0 \) is not the
implicit equation of the rational curve. Since this determinant vanishes when \( x, y \) lies on the curve, it follows by Theorem 1.1 that \( \det(C(x, y)) \) must be identically zero. Thus the method of moving conics fails when there is at least one moving line of degree \( n - 1 \) that follows the curve.

Suppose then that there is no moving line of degree \( n - 1 \) that follows the curve. Then by Proposition 5.2, \( \text{rank}(N) = 5n \). Thus there are exactly \( n \) linearly independent moving conics of degree \( n - 1 \) that follow the curve. To show that the method of moving conics works, it is enough to show that there is one \( n \times n \) matrix of moving conics that follows the curve whose determinant is the implicit equation of the rational curve because any other collection of \( n \) linearly independent moving conics that follow the curve will differ from this matrix by multiplication with a nonsingular matrix. To construct this matrix, we begin with two linearly independent moving lines of degree \( n \) that follow the curve.

Two such moving lines must exist for the following reason: Consider a moving line of degree \( n \)

\[
(A_n x + B_n y + C_n) t^n + \cdots + (A_1 x + B_1 y + C_1) t + (A_0 x + B_0 y + C_0) = 0.
\]

For this moving line to follow the rational curve \( x = x(t)/w(t), y = y(t)/w(t) \), we must have

\[
(A_n x(t) + B_n y(t) + C_n w(t)) t^n + \cdots + (A_0 x(t) + B_0 y(t) + C_0 w(t)) = 0.
\]

This polynomial equation generates \( 3n + 1 \) homogeneous linear equations in the \( 3n + 3 \) unknowns—\( A_k, B_k, C_k, k = 0, \ldots, n - 1 \); hence there must be at least two linearly independent solutions

\[
p(t) = p_n(x, y) t^n + \cdots + p_0(x, y) \\
q(t) = q_n(x, y) t^n + \cdots + q_0(x, y).
\]

Since, by assumption, there is no moving line of degree \( n - 1 \) that follows the curve, the moving lines \( p(t) \) and \( q(t) \) have no non-trivial factors. Hence they can have no common factor involving \( t \). Now consider the Bezout resultant matrix \( B(x, y) \) of \( p(t) \) and \( q(t) \).

Since \( p(t) \) and \( q(t) \) have no common factor, \( \det(B(x, y)) \) is not identically zero. But by construction (see Section 2), the Bezout matrix of \( p(t) \) and \( q(t) \) is an \( n \times n \) matrix whose entries are quadratic in \( x \) and \( y \). Moreover each of the rows of \( B(x, y) \) follows the curve because each row is of the form

\[
r_k(t) = g_k(t)p(t) - f_k(t)q(t)
\]

and the lines \( p(t) \) and \( q(t) \) follow the curve. Hence the rows of \( B(x, y) \) are the coefficients of moving conics that follow the curve. Thus for points on the curve, \( \det(B(x, y)) = 0 \), since for points on the curve the columns of \( B(x, y) \) are linearly dependent. We conclude that \( \det(B(x, y)) \) is a nonzero polynomial of degree \( 2n \) that vanishes on the rational curve \( x = x(t)/w(t), y = y(t)/w(t) \). Hence by Theorem 1.1, \( \det(B(x, y)) = 0 \) is the implicit equation of the rational curve. Since the rows of \( B(x, y) \) are moving conics that follow the curve, the method of moving conics always gives the correct implicit equation for curves of degree \( 2n \) when there is no moving line of degree \( n - 1 \) that follows the curve.

There are explicit formulas for the entries of the Bezout resultant, but no such explicit formulas are known for the entries of the matrix generated by the method of moving conics. Thus to generate the implicit equation of a rational curve of degree \( 2n \) using
moving conics, we need to solve a system of $5n$ equations in $6n$ unknowns. However, the proof of Theorem 5.4 suggests an alternative approach. Instead of solving lots of equations in lots of unknowns, we need only find two linearly independent moving lines of degree $n$ that follow the curve and then take the Bezout resultant of these moving lines. Two such moving lines can be found by solving a smaller system of equations—$3n + 1$ equations in $3n + 3$ unknowns—or by performing Gaussian elimination on the $2n \times 2n$ Bezout resultant for the implicit equation. This approach works for the following reason. Each row of the Bezout matrix represents a moving line

$$L_k(t) = L_{k,2n-1}(x,y)t^{2n-1} + \cdots + L_{k,1}(x,y)t + L_{k,0}(x,y) = 0$$

of degree $2n - 1$ that follows the curve. Thus we have $2n$ lines $L_k(t), \ k = 1, \ldots, 2n,$ of degree $2n - 1$ that follow the curve. Let $x_0 = x(0)/w(0)$ and $y_0 = y(0)/w(0).$ Since $L_k(t)$ follows the curve, the line $L_k(0) = L_{k,0}(x,y)$ must pass through the point $(x_0, y_0).$ Therefore the lines $L_{k,0}(x,y), \ k = 1, \ldots, 2n,$ are concurrent, so any three of these lines are linearly dependent. Thus we can use Gaussian elimination to zero out all but the first two elements in the last column of $R(x,y).$ Since the rows of this new matrix are linear combinations of moving lines that follow the curve, these rows are again moving lines that follow the curve. If we remove the first two rows and last column of this matrix, then the remaining moving lines have the form

$$\Lambda_k(t) = \Lambda_{k,2n-1}(x,y)t^{2n-1} + \cdots + \Lambda_{k,1}(x,y)t.$$ 

Factoring out $t,$ we obtain a $(2n - 2) \times (2n - 1)$ matrix of $2n - 2$ moving lines of degree $2n - 2$ that follow the curve. Repeating this Gaussian elimination $n$ times, we arrive at two moving lines of degree $n$ that follow the curve. Now the Bezout resultant of these two lines generates the desired $n \times n$ matrix of moving conics without solving a large system of linear equations.

5.2. THE AFFECT OF SINGULARITIES ON THE METHOD OF MOVING CONICS

Theorem 5.4 tells us when the method of moving conics will succeed or fail in terms of the existence of certain low degree moving lines. We now explore the effect of singularities on the method of moving conics.

**Corollary 5.5.** The method of moving conics fails for rational curves of degree $2n$ with no base points if there is a singular point of order $\geq n + 1.$

**Proof.** Let $x = x(t)/w(t), \ y = y(t)/w(t)$ be a rational curve of degree $2n$ with a singularity of order $\geq n + 1.$ Without loss of generality we may assume that this high order singularity is located at the origin. Then there exist polynomials $f(t), g(t), h(t)$ such that:

i. $x(t) = f(t)g(t), \ y(t) = f(t)h(t),$ 

ii. $\text{degree}(f(t)) \geq n + 1, \ \text{degree}(g(t)) \leq n - 1, \ \text{degree}(h(t)) \leq n - 1.$

It follows that

$$h(t)x(t) - g(t)y(t) = 0. \quad (*)$$
Let
\[ g(t) = \alpha_{n-1}t^{n-1} + \cdots + \alpha_1 t + \alpha_0 \]
\[ h(t) = \beta_{n-1}t^{n-1} + \cdots + \beta_1 t + \beta_0 . \]
Then by (**)
\[ \beta_{n-1}(t^{n-1}x) + \cdots + \beta_1 (tx) + \beta_0 x - \alpha_{n-1}(t^{n-1}y) - \cdots - \alpha_1 (ty) - \alpha_0 y = 0. \] (5.6)
Hence the columns of the matrix \((x \ y \ w \ tx \ ty \ tw \ldots t^{n-1}x \ t^{n-1}y \ t^{n-1}w)\) are linearly dependent. Therefore by Proposition 5.3, there is a moving line of degree \(n - 1\) that follows the curve, so by Theorem 5.4, the method of moving conics fails. □

**Corollary 5.6.** The method of moving conics works for rational curves of degree \(2n\) with no base points if there is a singular point of order \(n\).

**Proof.** Let \(x = x(t)/w(t),\ y = y(t)/w(t)\) be a rational curve of degree \(2n\) with a singularity of order \(n\). Again without loss of generality we may assume that the singularity of order \(n\) is at the origin. Then there exist polynomials \(f(t), g(t), h(t)\) such that:

i. \(x(t) = f(t)g(t),\ \ y(t) = f(t)h(t);\)
ii. \(\text{degree}(f(t)) = \text{degree}(g(t)) = n;\)
iii. \(f(t)\) does not divide \(w(t);\)
iv. \(g(t)\) and \(h(t)\) have no common factor.

To show that the method of moving conics works, we will show that there is no moving line of degree \(n - 1\) that follows the curve. Suppose to the contrary that there is a moving line of degree \(n - 1\) that follows the curve. Then by Proposition 5.3, the columns of \((x \ y \ w \ tx \ ty \ tw \ldots t^{n-1}x \ t^{n-1}y \ t^{n-1}w)\) must be linearly dependent, so there must be non-trivial constant \(\alpha_k, \beta_k, \gamma_k, k = 0, \ldots, n - 1,\) such that
\[ \alpha_{n-1}(t^{n-1}x) + \cdots + \alpha_0 x + \beta_{n-1}(t^{n-1}y) + \cdots + \beta_0 y + \gamma_{n-1}(t^{n-1}w) + \cdots + \gamma_0 w = 0. \] (∗)
Let
\[ p(t) = \alpha_{n-1}t^{n-1} + \cdots + \alpha_1 t + \alpha_0 \]
\[ q(t) = \beta_{n-1}t^{n-1} + \cdots + \beta_1 t + \beta_0 \]
\[ r(t) = \gamma_{n-1}t^{n-1} + \cdots + \gamma_1 t + \gamma_0 . \]
Then by (∗)
\[ p(t)x(t) + q(t)y(t) + r(t)w(t) = 0. \] (∗∗)
Now by ii and iii, \(f(t)\) divides \(x(t)\) and \(y(t)\) but not \(w(t)\). Therefore by (∗∗) \(f(t)\) must divide \(r(t).\) But \(\text{degree}(f(t)) = n\) and \(\text{degree}(r(t)) = n - 1;\) hence \(r(t)\) must be identically zero. Moreover by ii and iv, \(g(t)\) divides \(x(t)\) but not \(y(t).\) Hence by (∗∗) \(g(t)\) must divide \(q(t).\) But \(\text{degree}(g(t)) = n\) and \(\text{degree}(q(t)) = n - 1;\) hence \(q(t)\) must be identically zero. Therefore by (∗∗) \(p(t)x(t)\) must be identically zero. But \(x(t)\) is not the zero polynomial, so \(p(t)\) must be identically zero. It follows that the columns of \((x \ y \ w \ tx \ ty \ tw \ldots t^{n-1}x \ t^{n-1}y \ t^{n-1}w)\) are linearly independent. Therefore by Proposition 5.3, there is no moving line of degree \(n - 1\) that follows the curve, so by Theorem 5.4, the method of moving conics must work. □
Applying Corollaries 5.5 and 5.6, we can use singularities to characterize exactly when the method of moving conics correctly implicitizes a rational quartic curve. The following result was first derived in Sederberg et al. (1984) by exploiting techniques peculiar to rational quartics.

**Corollary 5.7.** For rational quartic curves the method of moving conics works if and only if there is no triple point.

**Proof.** This result follows immediately from Corollaries 5.5 and 5.6. □

By Corollary 5.5 we know that the method of moving conics fails when the rational curve has a high order singularity. We are now going to prove that the method of moving conics almost always succeeds for rational curves of degree 2n when all the singularities have order < n. To do so, we first need to show that the determinant generated by the method of moving conics factors into the implicit equation and a constant factor depending only on the coefficients of the functions \(x(t), y(t), w(t)\). We begin by demonstrating that the determinant whose vanishing guarantees the existence of degree \(n - 1\) moving lines that follow a rational curve of degree 2n is an irreducible polynomial in the coefficients of \(x(t), y(t), w(t)\).

**Lemma 5.8.** \(\det(x y w \ldots t^{n-1} x t^{n-1} y t^{n-1} w)\) is an irreducible polynomial in the coefficients of \(x, y, w\).

**Proof.** Since \(\det(x y w \ldots t^{n-1} x t^{n-1} y t^{n-1} w)\) bears some resemblance to the Sylvester resultant of two polynomials, our proof closely mimics the proof of the irreducibility of the resultant given in Macaulay (1916). Let \(x(t) = \Sigma a_k t^k, y(t) = \Sigma b_k t^k, w(t) = \Sigma c_k t^k\), and let \(R = \det(x y w \ldots t^{n-1} x t^{n-1} y t^{n-1} w)\). Then up to sign,

\[
R = \det(x \ldots t^{n-1} x y \ldots t^{n-1} y w \ldots t^{n-1} w).
\]

Multiplying the entries along the diagonal of this determinant, we obtain the term \(a_0^b b_0^c c_{2n}^d\), and it is easy to see that this is the only term in \(R\) that contains the factor \(a_0^b b_0^c\). Moreover if \(c_{2n} = 0\), then \(b_{2n} c_{2n-1}^d a_0^b b_0^c\) is the only term of \(R\) containing \(a_0^b b_0^c\). Therefore writing \(R\) in powers of \(a_0^b b_0^c\), we find that

\[
R = c_{2n}^d a_0^b b_0^c + d a_0^b b_0^c + \cdots
\]

\[
d = b_{2n} c_{2n-1}^d + c_{2n} f
\]

for some polynomial \(f\) in the variables \(a_k, b_k, c_k, k = 0, \ldots, 2n\). Hence if \(R\) can be written as the product of two factors, then expanding in powers of \(a_0^b b_0^c\),

\[
R = (c_{2n}^\alpha a_0^\beta b_0^\gamma + \cdots)(c_{2n}^\rho a_0^\sigma b_0^\tau + \cdots)
\]

where \(\alpha + \rho = \beta + \sigma = \gamma + \tau = n\). Moreover either \(\alpha = 0\) or \(\rho = 0\); otherwise the coefficient of \(a_0^b b_0^c\) would be zero or divisible by \(c_{2n}\), which we know is not the case. But \(R\) is a homogeneous polynomial in \(a_k, b_k, c_k, k = 0, \ldots, 2n\); hence its factors too must be homogeneous polynomials in these variables. Since either \(\alpha = 0\) or \(\rho = 0\), it follows by homogeneity that one of the factors of \(R\) must be independent of the \(c_k, k = 0, \ldots, 2n\). A symmetric argument shows that one of the factors must be independent of \(b_k, k = 0, \ldots, 2n\) and one of the factors must be independent of \(a_k, k = 0, \ldots, 2n\).
Thus if $R$ factors, then we can write $R$ as
\[ R = (c_{2n} + \cdots)(a_0^0 b_0^n + \cdots) = c_{2n}(a_0^0 b_0^n + \cdots) \]
since the entire coefficient of $a_0^0 b_0^n$ in $R$ is $c_{2n}^n$. But in this way we could never generate the term $b_{2n}c_{2n-1}^0 a_0^0 b_0^{n-1}$ which we know to be in $R$. Hence $R$ must be irreducible. □

**Theorem 5.9.** Let $x = x(t)/w(t)$, $y = y(t)/w(t)$ be a rational curve of degree $2n$ with no base points. Let Moving Conics denote an $n \times n$ matrix whose rows represent $n$ linearly independent moving conics of degree $n-1$ that follow this rational curve, and let $R = \det(x y w \ldots t^{n-1} x t^{n-1} y t^{n-1} w)$. Then
\[ \det(\text{Moving Conics}) = R^p \times \text{Resultant}(xw(t) - x(t), yw(t) - y(t)). \]

**Proof.** By Proposition 5.3 and Theorem 5.4 if $R = 0$, then $\det(\text{Moving Conics}) = 0$. Since by Lemma 5.8 $R$ is irreducible, it follows that some power of $R$ must be a factor of $\det(\text{Moving Conics})$. Moreover by Theorem 5.4, if $R \neq 0$, then $\det(\text{Moving Conics})$ is the implicit equation of the rational curve. Hence $\text{Resultant}(xw(t) - x(t), yw(t) - y(t))$ must also be a factor of $\det(\text{Moving Conics})$. But the degree in $x$ and $y$ of $\det(\text{Moving Conics})$ and $\text{Resultant}(xw(t) - x(t), yw(t) - y(t))$ is the same, so no power of $\text{Resultant}(xw(t) - x(t), yw(t) - y(t))$ greater than one can factor $\det(\text{Moving Conics})$. Finally, $\det(\text{Moving Conics})$ can have no other non-trivial factors; otherwise it would vanish when these factors vanish and in these cases fail to be the implicit equation of the rational curve, contradicting Theorem 5.4. □

**Corollary 5.10.** The method of moving conics almost always works for rational curves of degree $2n$ with no base points if there is no singular point of order $> n$.

**Proof.** By Theorem 5.9, the method of moving conics fails if and only if
\[ \det(x y w \ldots t^{n-1} x t^{n-1} y t^{n-1} w). \]
But this determinant represents an algebraic variety of degree $3n$ in the space of all rational curves of degree $2n$. Thus the method of moving conics works for all curves except those belonging to this low dimensional variety. Hence the method of moving conics almost always works. □

Although the method of moving conics almost always works if the rational curve has no base points and no high order singularities, there are cases where the method fails. Next we present one such example.

**Example:** Consider the rational sextic curve
\[
\begin{align*}
x &= (2t^6 - t^5 + t^4 + 2t^2 + 1)/(t^6 - t^4 + t^2) \\
y &= (-t^6 + 2t^5 + t^3)/(t^6 - t^4 + t^2).
\end{align*}
\]
Using Mathematica, we verified that this curve has 10 distinct double points—four real and six complex. But the method of moving conics fails on this curve due to the existence of a moving line of degree 2 that follows the curve. This example shows that the method of moving conics may fail even in the absence of high order singularities.
5.3. THE METHOD OF MOVING CONICS IN THE PRESENCE OF BASE POINTS

So far all our analysis for moving conics has been for rational curves with no base points. What happens if there are base points? As with moving lines, the method of moving conics must be modified to accommodate base points because a degree $2n$ rational curve with $2r$ base points is represented by an irreducible algebraic curve of degree $2n - 2r$. When base points are present, there are three possible ways to proceed:

1. Remove the base points by canceling common factors; then continue as before.
2. Apply Gaussian elimination, much as in the case of moving lines (see Section 4), to generate an $(n - r) \times (n - r)$ matrix of moving conics whose determinant represents the implicit equation.
3. Observe that when there are $2r$ base points there are $2r$ linearly independent moving lines of degree $n - 1$ that follow the curve. Thus we can still make use of moving conics of degree $n - 1$ to generate an $n \times n$ matrix whose determinant represents the implicit equation of degree $2n - 2r$, provided we choose $2r$ linearly independent moving lines and $n - 2r$ linearly independent moving conics polynomially independent from the moving lines.

Since our goal is to understand how to extend our methods to rational surfaces, we shall not pursue the first technique because base points cannot, in general, be factored out of rational surfaces. The second method is quite similar to the discussion leading up to Theorem 4.2 (see too, Lemma 5.12 below). Since we have nothing essentially new to add, we shall not pursue this topic further here. Instead we will concentrate on the third technique, which has been shown empirically by Sederberg and Chen (1995) to extend in many cases to rational surfaces.

To make the third technique precise, here is what we intend. In general, we know we can find $n$ linearly independent moving conics of degree $n - 1$ that follow a rational curve of degree $n$. If we collect these moving conics in an $n \times n$ matrix

$$C(x, y) = (C_{ij}(x, y)) \quad i = 1, \ldots, n \quad j = 0, \ldots, n - 1.$$  

Theorem 5.4 asserts that when there are no base points and no moving lines of degree $n - 1$ that follow the curve, $\det(C(x, y)) = 0$ is the implicit equation of the rational curve. What we hope to happen when there are $2r$ base points is that $2r$ moving conics can be replaced by $2r$ moving lines in $C(x, y)$. This would lower the degree of the implicit equation by $2r$ as required. Theorem 5.13 generalizes Theorem 5.4 by stating a precise condition under which this generalized method of moving conics is guaranteed to yield the implicit equation for a rational curve even in the presence of base points. But before we proceed, we need some preparatory lemmas.

**Lemma 5.11.** Suppose there are $d$ linearly independent moving lines of degree $n$ that follow a rational curve. Then there are at least $d - 2r$ linearly independent moving lines of degree $n - r$ that follow the same rational curve.

**Proof.** Let

$$p_k(t) = L_{k,n}(x, y)t^n + \cdots + L_{k,1}(x, y)t + L_{k,0}(x, y) = 0 \quad k = 1, \ldots, d$$

be $d$ linearly independent moving lines that follow the rational curve $x = x(t)/w(t)$, $y = y(t)/w(t)$. Then $p_k(0) = L_{k,0}(x, y)$ must pass through the point $(x(0)/w(0), y(0)/w(0))$. 

Hence any three polynomials \( L_{k,0}(x,y) \) must be linearly dependent since the corresponding lines are concurrent. Reindexing if necessary, we can use linear combinations of \( p_{d-1}(t) \) and \( p_d(t) \) to zero out the term \( L_{k,0}(x,y) \) in \( p_k(t) \), \( k = 0, \ldots, d - 2 \). Now factoring out \( t \) from \( p_k(t) \), \( k = 1, \ldots, d - 2 \), yields \( d - 2 \) linearly independent moving lines of degree \( n - 1 \) that follow the curve. Iterating this same procedure \( r \) times generates \( d - 2r \) linearly independent moving lines of degree \( n - r \) that follow the curve. \( \square \)

**Lemma 5.12.** Suppose there are \( d \) linearly independent moving conics of degree \( n \) that follow a rational curve. Then there are at least \( d - 5r \) linearly independent moving conics of degree \( n - r \) that follow the same rational curve.

**Proof.** Here we use the fact that any six conics passing through a common point are linearly dependent. The rest of the proof is the same as the proof of Lemma 5.11. \( \square \)

**Theorem 5.13.** The generalized method of moving conics generates the implicit equation for a rational curve of degree \( 2n \) with \( 2r \) base points if there is no moving line of degree \( n - r - 1 \) that follows the curve.

**Proof.** Consider a degree \( 2n \) rational curve \( x = x(t)/w(t), y = y(t)/w(t) \) with \( 2r \) base points. Then \( x(t), y(t), w(t) \) have a common factor of degree \( 2r \). Removing this common factor, we obtain a rational curve of degree \( 2(n - r) \) with no base points. Suppose now that there is no moving line of degree \( n - r - 1 \) that follows this rational curve. Then by Proposition 5.2, there are exactly \( n - r \) linearly independent moving conics of degree \( n - r - 1 \) that follow this curve (with the base points removed). Moreover there are exactly two linearly independent moving lines of degree \( n - r \) that follow this curve. Clearly there are at least two such moving lines, since removing the common factor of degree \( 2r \) from the identity

\[
(A_{n-r}x(t) + B_{n-r}y(t) + C_{n-r}w(t))t^{n-r} + \cdots + (A_0x(t) + B_0 + y(t) + C_0w(t)) = 0
\]

generates \( 3(n - r) + 1 \) homogeneous linear equations in \( 3(n - r + 1) \) unknowns. If there were such three linearly independent moving lines, then by Lemma 5.11 there would exist a moving line of degree \( n - r - 1 \) that follows the curve. But this is contrary to assumption. Hence there exist exactly two linearly independent moving lines of degree \( n - r \) that follow the curve.

Next we shall show that there are exactly \( n + 4r \) linearly independent moving conics and exactly \( 2r \) linearly independent moving lines of degree \( n - 1 \) that follow the curve. Certainly there are at least \( n + 4r \) such moving conics, since removing the common factor of degree \( 4r \) from the identity

\[
(A_{n-1}x^2(t) + B_{n-1}x(t)y(t) + C_{n-1}y^2(t) + D_{n-1}x(t)w(t) + E_{n-1}y(t)w(t) + F_{n-1}w^2(t))t^{n-1}
\]

\[
+ (A_0x^2(t) + B_0x(t)y(t) + C_0y^2(t) + D_0x(t)w(t) + E_0y(t)w(t) + F_0w^2(t)) = 0.
\]

generates \( 5n - 4r \) homogeneous linear equations in \( 6n \) unknowns. Moreover if there were more than \( n + 4r \) linearly independent moving conics of degree \( n - 1 \) that followed the curve, then by Lemma 5.12 there would be more than \( n - r \) linearly independent moving conics of degree \( n - r - 1 \) that follow the curve, contrary to what we have already proved.
A similar argument shows that there are exactly \(2r\) linearly independent moving lines of degree \(n - 1\) that follow the curve.

Now each moving line of degree \(n - 1\) that follows the curve accounts for three moving conics of the same degree, since we can multiply each moving line by \(x\) or \(y\) or \(w\) to generate a moving conic. Thus there are exactly \(n - 2r\) linearly independent moving conics of degree \(n - 1\) that follow the curve that are also polynomially independent from the \(2r\) moving lines of degree \(n - 1\) that follow the curve. Therefore to show that the generalized method of moving conics works, we need only show that there is one \(n \times n\) matrix of \(n - 2r\) moving conics and \(2r\) moving lines of degree \(n - 1\) whose determinant is the implicit equation of the rational curve because any other such matrix will differ from this matrix by multiplication with a nonsingular matrix. This we now proceed to do by applying the hybrid Sylvester–Bezout resultant.

Let \(p(t)\) and \(q(t)\) be two linearly independent moving lines of degree \(n - r\) that follow the curve and let \(R_r(x, y)\) be their hybrid Sylvester–Bezout resultant of order \(r\). Since by assumption there is no moving line of degree \(n - r - 1\) that follows the curve, the polynomials \(p(t)\) and \(q(t)\) can have no non-trivial common factors. Hence, by Corollary 2.5, \(\det(R_r(x, y))\) is not identically zero. Moreover, by construction, the rows of \(R_r(x, y)\) consist of \(n - 2r\) moving conics (the Bezout rows) and \(2r\) moving lines (the Sylvester rows) of degree \(n - 1\) that follow the curve. Therefore for points on the curve, the columns of \(R_r(x, y)\) are dependent; hence for points on the curve, \(\det(R_r(x, y)) = 0\).

Since \(\text{degree}\{\det(R_r(x, y))\} = 2n - 2r\), it follows from Theorem 1.1 that \(\det(R_r(x, y)) = 0\) represents the implicit equation of the rational curve with the base points removed. \(\Box\)

The converse of Theorem 5.13 is false. That is, given a rational curve of degree \(2n\) with \(2r\) base points, the generalized method of moving conics may still succeed even if there is a moving line of degree \(n - r - 1\) that follows the curve. Consider, for example, a curve of degree \(4m\) \((n = 2m)\) with \(2m\) \((r = m)\) base points. Then the generalized method of moving conics generates a \(2m \times 2m\) matrix all of whose rows represent moving lines that follow the curve. If we remove the base points from the parametrization by canceling common factors, then we obtain a rational curve of degree \(2m\), and by Theorem 4.1 we know that for a rational curve with no base points the method of moving lines always successfully implicitizes the rational curve. Thus the \(2m \times 2m\) matrix of moving lines generated by the generalized method of moving conics must represent the implicit equation of the rational curve, even if there is a moving line of degree \(2m - 1\) that follows the curve. In effect, the more base points we introduce the more likely the method of moving conics is to succeed. If there is a moving line of degree \(n - 1\) that follows a rational curve of degree \(2n\), then by Theorem 5.4 the method of moving conics is guaranteed to fail. But as we raise the degree by introducing more and more base points or equivalently as we increase the size of the matrix and replace more and more moving conics by moving lines, the method is more and more likely to succeed. Nevertheless, exact necessary and sufficient conditions under which the generalized method of moving conics successfully implicitizes a rational curve of degree \(2n\) with \(2r\) base points are difficult to describe and remain an open question.

Implicitization using the method of moving conics has several advantages over standard implicitization techniques using resultants. The method of moving conics generates a smaller matrix. For rational curves of degree \(2n\), moving conics generate an \(n \times n\) matrix, while the Bezout resultant yields a \(2n \times 2n\) matrix. Thus the method of moving conics may lead to faster computations than the method of resultants. Moreover, as we have
just seen, the generalized method of moving conics often works even in the presence of base points, where resultants are known to fail. Thus we are encouraged to try to extend this method to surfaces where base points play a much more critical role.

References