AN IMPLICIT EQUATION GIVEN CERTAIN PARAMETRIC EQUATIONS

James Bruening and Hao Hao Wang

Abstract. This paper concerns finding the implicit equation of a given monomial parametrization of projective surfaces. The discussion is concentrated on the irreducibility of the equation.

1. Introduction. The implicitization problem is to convert a parametrization into a defining equation for a curve or surface. Parametric surfaces are widely used in computer aided design projects since it is easy to describe the points of the surface by means of the parameter values. Given the parametric equations, the computer can plot points on the surface by evaluating the equations for different parameter values. But it is hard to decide whether a point is on the surface which is parametrically presented. To describe the set of points which are common to two different parametrically presented surfaces is a difficult problem using the parametric descriptions. If the surfaces are described by means of external, i.e. implicit equations, then to find the set of common points of two surfaces reduces to the less complicated problem of finding the common solutions of two explicitly given polynomial equations. Thus, there is a need for being able to go back and forth between a parametric and an implicit description of a surface. This is, in essence, the implicitization problem.

Describing surfaces of arbitrary shape by parametric curves is a primary interest of design engineers and mathematicians. Different parametrizations will give rise to various surfaces which are used in aircraft and automobile designs. When it becomes necessary to find the intersection of two connecting surfaces, a good method for doing so is by solving the system of polynomial equations which describe the surfaces implicitly.

The class of monomial parametric equations which we investigate in this paper is a family of surfaces that can be presented implicitly. Figure 1 gives the affine view (set $w = 1$) of one of the surfaces in this family. Follow-up research will investigate other classes of parametric equations.

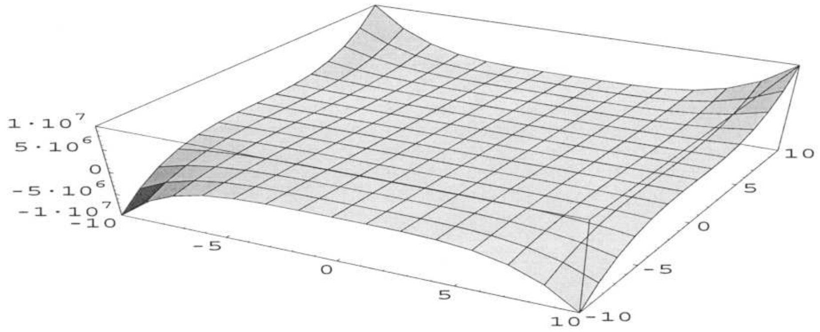

FIGURE 1. Affine view of $x^4y^3 - zw^6 = 0$

Suppose we are given a surface in the complex projective space expressed by the following monomial parametric equations of homogeneous form of bidegree (m, n)

$$\begin{cases} x = s^m v^n, \\ y = u^m t^n, \\ z = s^m t^n, \\ w = s^p u^{m-p} t^q v^{n-q}, \end{cases} \tag{1}$$

where m, n, p, q are positive integers with $\gcd(m, n) = \gcd(m, p) = \gcd(n, q) = 1$, and the total degree on the s, u variables is m and the total degree on the t, v variables is n. Our goal in this paper is to find an implicit equation for the parametrization; that is, convert this parametrization into an irreducible defining implicit equation. A function $f(x, y, z, w) = 0$ is an implicit equation if it satisfies the following two properties:

1. $f(x, y, z, w) = 0$ whenever $(x : y : z : w)$ is a point on the parametrized surface;
2. f is irreducible, that is, f is not the product of two non-units in $R = \mathbb{C}[x, y, z, w]$.

In Section 2, we will show how to eliminate the parameters s, u, t, v to produce an equation which satisfies criterion 1. Next, in Section 3, we discuss when a function of the form $f(x, y, z, w) = w^m x^n - y^p z^q$ is irreducible. Finally, in Section 4, we will prove that the equation derived in Section 2 satisfies criterion 2, and we will present two examples.

2. Elimination. Elimination Theory assures us that for any parametrization, the implicit equation can be found via eliminating the parameters (for details, see [1]), but general methods are often inefficient for special cases.

For the class of parametric equations given by Equation (1), we give the following formula for the implicit equation:

Proposition 2.1. Eliminating the parameters s, u, t, v in Equation (1) produces the equation

$$x^{m(n-q)}y^{n(m-p)} - z^{mn-mq-np}w^{mn} = 0. \qquad (2)$$

Proof. If $z \neq 0$ in Equation (1), we have

$$u^m = \frac{y}{z}s^m, \quad v^n = \frac{x}{z}t^n,$$

and

$$\begin{aligned} w^{mn} &= (s^p u^{m-p} t^q v^{n-q})^{mn} \\ &= s^{pmn}(u^m)^{(m-p)n} t^{qmn} (v^n)^{(n-q)m} \\ &= s^{pmn}\left(\frac{y}{z}s^m\right)^{(m-p)n} t^{qmn}\left(\frac{x}{z}t^n\right)^{(n-q)m} \\ &= \frac{(s^m t^n)^{mn} y^{n(m-p)} x^{m(n-q)}}{z^{2mn-np-mq}} \\ &= \frac{z^{mn} y^{n(m-p)} x^{m(n-q)}}{z^{2mn-np-mq}} \\ &= \frac{y^{n(m-p)} x^{m(n-q)}}{z^{mn-np-mq}}. \end{aligned}$$

Thus, $w^{mn}z^{mn-np-mq} = y^{n(m-p)}x^{m(n-q)}$, and Equation (2) is derived.

If $z = 0$, then either $s = 0$ or $t = 0$. If $s = 0$, then $x = z = w = 0$ and this satisfies Equation (2). If $t = 0$, then $y = z = w = 0$ and this also satisfies Equation (2).

Therefore, $x^{m(n-q)}y^{n(m-p)} - z^{mn-mq-np}w^{mn} = 0$ is the equation after eliminating the parameters s, u, t, v in Equation (1).

To prove this equation is the implicit equation, we only need to show that it is irreducible. We will do so by proving the following.

3. Irreducibility.

Proposition 3.1. If $f = x^a y^b - z^c w^d$ is a polynomial with positive integer exponents a, b, c, d, and $\gcd(a, b, c, d) = 1$, then f is irreducible in $R = \mathbb{C} - [x, y, z, w]$.

Proof. Let $A = \mathbb{C}[y, z, w]$. If we replace x by X, then we show that $f(X) = X^a y^b - z^c w^d$ is irreducible in $A[X] = R$. Since A is a unique factorization domain (UFD), by Lemma 6.13 [2], this is equivalent to showing that f is irreducible in $K[x]$, where $K = \mathbb{C}(y, z, w)$ is the fraction field of A. Since w is a unit in K, this is equivalent to proving the irreducibility of

$$X^a - \frac{z^c w^d}{y^b}$$

in $K[X]$. The result will follow from the following two lemmas.

Lemma 3.2. For any divisor k of a with $k > 1$,

$$\sqrt[k]{\frac{z^c w^d}{y^b}} \notin K = \mathbb{C}(y, z, w),$$

where $\gcd(a, b, c, d) = 1$.

Proof. Suppose

$$\sqrt[k]{\frac{z^c w^d}{y^b}} = \frac{P}{Q} \in K$$

with polynomials $P, Q \in \mathbb{C}[y, z, w]$ and P, Q have no common factor. This gives

$$y^b P^k = z^c w^d Q^k. \tag{3}$$

Since $\gcd(a, b, c, d) = 1$, we have that k cannot divide all of b, c, d.

Suppose $k \nmid b$. Then Equation (3) shows that $y|Q$, so let $Q = y^e \bar{Q}$ with y prime to $\bar{Q}$. Then Equation (3) becomes

$$y^b P^k = z^c w^d y^{ek} \bar{Q}^k. \tag{4}$$

Equation (4) shows that $ek \geq b$, but $ek = b$ is impossible since $k \nmid b$. Hence, $ek > b$. Therefore, we obtain the following equation by cancelling y^b

$$P^k = z^c w^d y^{b'} \bar{Q}^k, \quad b' \geq 1. \tag{5}$$

Equation (5) shows that $y|P$. This is a contradiction, since we assume P, Q have no common factor. Therefore, $k|b$.

Suppose $k \nmid c$. Then Equation (3) shows that $z|P$; that is, $P = z^i \bar{P}$ with z prime to $\bar{P}$. Therefore, Equation (3) becomes

$$y^b z^{ik} \bar{P}^k = z^c w^d Q^d. \tag{6}$$

Equation (6) shows that $ik \geq c$. Since $k \nmid c$, we must have $ik > c$. Cancelling z^c, we have

$$y^b z^{c'} \bar{P}^k = w^d Q^k, \quad c' \geq 1. \tag{7}$$

Equation (7) shows that $z|Q$. This is a contradiction, since P, Q have no common factor. Therefore, $k|c$.

Suppose $k \nmid d$. Then Equation (3) shows that $w|P$; that is, $P = w^j \bar{P}$ with w prime to $\bar{P}$. Therefore, Equation (3) becomes

$$y^b w^{jk} \bar{P}^k = z^c w^d Q^k. \tag{8}$$

Equation (8) shows that $jk \geq d$. Since $k \nmid d$, we must have $jk > d$. Cancelling w^d, we have

$$y^b w^{d'} \bar{P}^k = z^c Q^d, \quad d' \geq 1. \tag{9}$$

Equation (9) shows that $w|Q$. This is a contradiction, since P, Q have no common factor. Therefore, $k|d$.

This says that if

$$\sqrt[k]{\frac{z^c w^d}{y^b}} = \frac{P}{Q} \in K,$$

it is impossible that $\gcd(a, b, c, d) = 1$, which is a contradiction to our condition. Therefore, our assumption is false.

In conclusion, for any divisor k of a with $k > 1$ and $\gcd(a, b, c, d) = 1$, we have

$$\sqrt[k]{\frac{z^c w^d}{y^b}} \notin K = \mathbb{C}(y, z, w).$$

Lemma 3.3. Let K be a field that contains a primitive n-th root of unity (so in particular $charK \nmid n$). Let $a \in K$ be an element such that $\sqrt[d]{a} \notin K$ for any divisor d of n with $d > 1$. Then $X^n - a$ is irreducible in $K[X]$.

Proof. By assumption the group of n-th roots of unity

$$\mu_n = \{1, \beta, \beta^2, \ldots, \beta^{n-1}\} \subseteq K.$$

This is cyclic of order n. The elements $\sqrt[n]{a}$ belong to an algebraic closure $\bar{K}$ of K under our hypotheses, and $K(\sqrt[n]{a})$ is a Galois extension of K. The point is that

1. $X^n - a$ is a separable polynomial over K, since $char K \nmid n$.
2. Once we adjoin $\sqrt[n]{a}$ to K, all roots of

$$X^n - a = \prod_{i=0}^{n-1} (X - \beta^i \sqrt[n]{a})$$

are in $K(\sqrt[n]{a})$ since we are assuming that $\mu_n \subseteq K$. Therefore, $K(\sqrt[n]{a})$ is a normal extension of K.

Let $m = [K(\sqrt[n]{a}) : K]$, and let $\Phi(X) \in K[X]$ be the monic irreducible polynomial for $\sqrt[n]{a}$. Hence, $\deg \Phi(X) = m$. Now, $\Phi(X)$ divides $X^n - a$ since $\sqrt[n]{a}$ is a root of the latter. To prove the lemma, we only need to show that $m = n$, for then, $\Phi(X) = X^n - a$ is irreducible.

Suppose $m < n$. Every $\alpha \in \mathrm{Gal}(K(\sqrt[n]{a})/K)$ sends $\sqrt[n]{a}$ to another root of $\Phi(X)$, hence, to a $\beta_\alpha \sqrt[n]{a}$, where β_α is some n-th root of unity. The map

$$G = \mathrm{Gal}(K(\sqrt[n]{a})/K) \to \mu_n$$

which sends α to β_α is an injective homomorphism that identifies G with a subgroup of the cyclic group μ_n of order n. Therefore, $|G| = [K(\sqrt[n]{a}) : K] = m$ and $m|n$. We write $n = md$, and $d > 1$ by the assumption $m < n$. Consider the norm $N : K(\sqrt[n]{a}) \to K$ with $N(\gamma) = \prod_{\alpha \in G} \alpha \cdot \gamma$. This gives

$$N(\sqrt[n]{a}) = \prod_{\alpha \in G} (\beta_\alpha \cdot \sqrt[n]{a}) = \bar{\beta} \cdot (\sqrt[n]{a})^m.$$

In other words, $N(\sqrt[n]{a}) = (n\text{-th root of unit}) \cdot \sqrt[n]{a} \in K$. Since all n-th roots of unity are in K, this shows that $\sqrt[d]{a} \in K$ for a divisor d of n with $d > 1$. This violates our assumptions, so $m < n$ is impossible. Therefore, we must have $m = n$, and $X^n - a$ is irreducible.

4. Conclusion.

Theorem 4.1. $x^{m(n-q)} y^{n(m-p)} - z^{mn-mq-np} w^{mn} = 0$ with $\gcd(m,n) = \gcd(m,p) = \gcd(n,q) = 1$ is irreducible, and therefore, it is the implicit equation of the given parametrization (1).

Proof. The result follows by Proposition 3.1 and the following lemma.

Lemma 4.2.

$$\gcd(m,n)=\gcd(m,p)=\gcd(n,q)=1 \iff \\ \gcd(m(n-q),n(m-p),mn-mq-np,mn)=1.$$

Proof. We only need to show

$$\gcd(m,n)=\gcd(m,p)=\gcd(n,q)=1 \iff \\ \gcd(mn-mq,mn-np,mn)=1,$$

since

$$\begin{aligned} &\gcd(m(n-q),n(m-p),mn-mq-np,mn)\\ =&\gcd(mn-mq,mn-np,mn-mq-np,mn)\\ =&\gcd(mn-mq,mn-np,mn). \end{aligned}$$

Suppose $\gcd(mn-mq,mn-np,mn)=1$. If $x|m$, then $x\nmid n$, and $x\nmid p$. Therefore, $\gcd(m,n)=\gcd(m,p)=1$. If $x|n$, then $x\nmid m$ and $x\nmid q$. Therefore, $\gcd(m,n)=\gcd(n,q)=1$. Suppose $\gcd(m,n)=\gcd(m,p)=\gcd(n,q)=1$. If $\gcd(mn-mq,mn-np,mn)\neq 1$ and $x\neq 1$ is an irreducible common factor, then $x|mn$, $x|np$, and $x|mq$. $x|np$ implies that $x|n$ or $x|p$. If $x|n$, then $x\nmid m$, so $x|q$. This says $\gcd(n,q)=x\neq 1$, which is a contradiction to our assumption. If $x|p$, then $x\nmid m$, so $x|n$ and $x|q$. This says $\gcd(n,q)=x\neq 1$. This is also a contradiction to our assumption. Therefore, $\gcd(mn-mq,mn-np,mn)=1$.

Example 4.3. The implicit equation for the parametric equations

$$x=s^2v^3,$$

$$y=u^2t^3,$$

$$z=s^2t^3,$$

$$w=sutv^2$$

is $x^4y^3-zw^6=0$ by Theorem 4.1. (See Figure 1 for the affine view of the surface.)

Example 4.4. The implicit equation for the parametric equations

$$x = s^3 v^5,$$

$$y = u^3 t^5,$$

$$z = s^3 t^5,$$

$$w = s^2 utv^4$$

is $x^{12} y^5 - z^2 w^{15} = 0$.

Acknowledgement. We would like to thank Mangho Ahuja and Paul Deiermann for their suggestions.

References

1. D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms,* 2nd edition, Springer-Verlag, New York, 1996.

2. T. Hungerford, *Algebra*, Springer-Verlag, New York, New York, 1974.

Mathematics Subject Classification (2000): 13A05, 11A05

James Bruening
Department of Mathematics
Southeast Missouri State University
Cape Girardeau, MO 63701
email: jbruening@semo.edu

Hao Hao Wang
Department of Mathematics
Southeast Missouri State University
Cape Girardeau, MO 63701
email: hwang@semo.edu