Explicit equations in the plane for elliptic curves given as space quartics

Qiaochu Yuan

under the direction of
Ryan Reich
Harvard Graduate School of Arts and Sciences

November 12th, 2007

1 Introduction

Qiaochu Yuan

Curves of genus one are usually studied in the context of elliptic curves in the plane given by cubic Weierstrass equations (see, for example, Silverman [8]). Another explicit form for a curve of genus one, however, is as the intersection of quadric surfaces in space.[3] A *quadric surface* is a collection of points $\mathcal{S}(\mathbf{A}) = \{\mathbf{X} \in \mathbb{CP}^3 : \mathbf{X}\mathbf{A}\mathbf{X}^T = 0\}$, where $\mathbf{A}$ is an invertible symmetric 4×4 matrix with complex entries[1], and the curves we are studying are of the form

$$\mathcal{C}(\mathbf{A}, \mathbf{B}) = \mathcal{S}(\mathbf{A}) \cap \mathcal{S}(\mathbf{B}) \tag{1}$$

where $\mathbf{A}$ is not a scalar multiple of $\mathbf{B}$. Because quadric surfaces are computationally simple, the analysis of such curves is a matter of practical interest to computer-aided design. In that field, these curves are considered in real affine space $\mathbb{RA}^3$ and are referred to as QSICs; see [7], [10], and [11]. Our interests are more algebraic than graphical, so we will instead use the term *space quartic*.[2]

For the purposes of this paper, an *elliptic curve* is a curve $\mathcal{C}$ of genus 1 (not necessarily smooth) together with a point $\mathbf{O}$ on $\mathcal{C}$. Space quartics are therefore elliptic curves; a group law can be defined on the points of a space quartic $\mathcal{C}$, and a birational map can be constructed to a planar elliptic curve $\mathcal{C}'$. Explicit equations for these curves will allow us to use techniques associated with planar elliptic curves to study space quartics; for example, to find rational points on $\mathcal{C}$ (as in [4]), we would find instead rational points on $\mathcal{C}'$.

In section 2 of this paper we discuss the characteristic polynomials of isomorphism classes of space quartics. In section 3 we describe an explicit normal form for each isomorphism class. In section 4 we describe an explicit birational map from space quartics to planar curves

[1]The results in this paper hold equally well when $\mathbb{C}$ is replaced by $\bar{K}$, where K is a perfect field of characteristic not equal to 2, but for notational familiarity and convenience we will work over $\mathbb{C}$.

[2]Note that a generic smooth quartic has genus 3. Here, 'Space quartic' means 'space curve of genus 1 given by the intersection of two quadric surfaces'; these quartics are singular, but will still be treated as elliptic curves in this paper.

using Edwards normal form. Finally, in section 5 we demonstrate a geometric construction of the algebraic group law given by Edwards that explains why the tangent-chord construction fails for a curve in Edwards form in the plane.

2 Background

2.1 Characteristic polynomials

The set of quadric surfaces $\mathcal{P}(\mathbf{A}, \mathbf{B}) = \{\mathcal{S}(\alpha\mathbf{A} - \beta\mathbf{B}) : \alpha, \beta \in \mathbb{C}\}$ is called the (quadric) *pencil* of $\mathcal{C}(\mathbf{A}, \mathbf{B})$. Because $\mathcal{C}$ is contained in every surface in $\mathcal{P}$, we call $\mathcal{C}$ the *base curve* of $\mathcal{P}$. We are interested in the case where $\mathcal{C}$ is a space quartic, so we need to exclude various degenerate cases.

Farouki, Neff, and O'Connor [6] use the *Segre characteristic* of a pencil $\mathcal{P}$ to determine whether its base curve $\mathcal{C}$ is degenerate. First, we define

$$P(\lambda) \equiv \det(\mathbf{A} - \lambda\mathbf{B}), \lambda \in \mathbb{CP}^1 \tag{2}$$

to be a *characteristic polynomial* of $\mathcal{P}$ (equivalently, of $\mathcal{C}$, or of $\mathbf{A}, \mathbf{B}$).[3] The Segre characteristic is defined in terms of the set of multiplicities of the roots of $P(\lambda)$, and it is well known that a given quadric pencil defines a space quartic if and only if its Segre characteristic is [1 1 1 1], that is, all four roots are distinct.[4] In fact, since $\mathcal{P}(\mathbf{A}, \mathbf{B}) = \mathcal{P}(k\mathbf{A}, k\mathbf{B})$ (for any $k \neq 0$), characteristic polynomials are defined only up to multiplication by a constant, and are therefore described by their roots.

[3] Farouki et al. [6] use the term *discriminant polynomial* (not the discriminant of P!). We prefer the use of the term 'characteristic polynomial' if only because $P(\lambda)$ is precisely the characteristic polynomial of $\mathbf{A}\mathbf{B}^{-1}$, up to multiplication by a constant.

[4] Farouki et al. describe this case as 'nonsingular space quartic'; they are not considering the singularities that will in general only appear over an algebraically closed field.

2.2 Uniqueness and invariance

$\mathcal{P}(\mathbf{A}, \mathbf{B})$ is a vector space of dimension 2, so any two linearly independent surfaces $\mathcal{S}(\mathbf{C}), \mathcal{S}(\mathbf{D})$ in it form a basis.[5] Although a different choice of matrices $\mathbf{C}, \mathbf{D}$ produces a different characteristic polynomial, we can speak of the set of characteristic polynomials of a given pencil. Moreover, given two matrices $\mathbf{A}, \mathbf{B}$ and their characteristic polynomial $P(\lambda)$, the matrices $a\mathbf{A} + b\mathbf{B}, c\mathbf{A} + d\mathbf{B}$ have the characteristic polynomial

$$Q(\lambda) \equiv \det((-c\lambda + a)\mathbf{A} - (d\lambda - b)\mathbf{B}). \tag{3}$$

Since $P(\lambda) = \frac{c\lambda+d}{ad-bc} Q\left(\frac{a\lambda+b}{c\lambda+d}\right)$, if z is a root of P then $\frac{az+b}{cz+d}$ is a root of Q;[6] this is a fractional linear transformation, and if the two matrices $a\mathbf{A} + b\mathbf{B}, c\mathbf{A} + d\mathbf{B}$ are linearly independent, then this transformation is invertible. Because fractional linear transformations preserve multiplicity, the Segre characteristic of a pencil is therefore the same regardless of the choice of $\mathbf{A}, \mathbf{B}$ and a quadric pencil associated with a given characteristic polynomial $P(\lambda)$ is also associated with the equivalence class of $P(\lambda)$ under fractional linear transformation.

Consider isomorphisms $\mathbb{CP}^3 \to \mathbb{CP}^3$ of the form $\mathbf{X} \mapsto \mathbf{XM}$, where $\mathbf{M}$ is a 4×4 invertible matrix with coefficients in $\mathbb{C}$. This transformation is a change of coordinates which takes a quadric surface $\mathcal{S}(\mathbf{A})$ to $\mathcal{S}(\mathbf{MAM}^T)$; it is therefore an isomorphism of varieties $\mathcal{C}(\mathbf{A}, \mathbf{B}) \mapsto \mathcal{C}(\mathbf{MAM}^T, \mathbf{MBM}^T)$. Moreover, the characteristic polynomials of the latter are precisely $\det(\mathbf{M})^2$ times the characteristic polynomials of the former; characteristic polynomials are therefore invariant, up to multiplication by a constant, under change of coordinates.

Using only the tools of characteristic polynomials and coordinate changes, we can now begin to establish useful results.

[5] In this paper we will restrict our discussion to surfaces $\mathcal{S}(\mathbf{M})$ such that $\mathbf{M}$ is invertible. The surfaces such that $\mathbf{M}$ is not invertible are the 'projective cones' of the quadric pencil, and we ignore them here.

[6] When we speak of the polynomial $P(\lambda) = \det(\mathbf{A} - \lambda\mathbf{B})$ we are really referring to the polynomial $P(\alpha : \beta) = \det(\alpha\mathbf{A} - \beta\mathbf{B})$, where $\lambda = (\alpha : \beta) \in \mathbb{CP}^1$. The use of λ rather than $(\alpha : \beta)$ is a notational convenience. The fractional linear transformation $z \mapsto \frac{az+b}{cz+d}$ is actually the transformation $(\alpha : \beta) \mapsto (a\alpha + b\beta : c\alpha + d\beta)$

3 A normal form for space quartics

3.1 Eigenvectors

We can think of the roots $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ of the characteristic polynomial of $\mathcal{C}(\mathbf{A}, \mathbf{B})$ as the eigenvalues of $\mathbf{AB^{-1}}$; when $\mathcal{C}$ is a space quartic, these eigenvalues are distinct, so there are then corresponding eigenvectors[7] $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4$ such that

$$\mathbf{v}_i \mathbf{A} \mathbf{B}^{-1} = \lambda_i \mathbf{v}_i \Leftrightarrow \mathbf{v}_i \mathbf{A} = \lambda_i \mathbf{v}_i \mathbf{B}, i = 1, 2, 3, 4. \tag{4}$$

Lemma 3.1. $i \neq j \implies \mathbf{v}_i \mathbf{A} \mathbf{v}_j^T = \mathbf{v}_i \mathbf{B} \mathbf{v}_j^T = 0$.

Proof. Note that $\mathbf{v}_i \mathbf{A} \mathbf{v}_j^T = \lambda_i \mathbf{v}_i \mathbf{B} \mathbf{v}_j^T$ by (4); but we also have $\mathbf{v}_i \mathbf{A} \mathbf{v}_j^T = \mathbf{v}_i (\lambda_j \mathbf{B} \mathbf{v}_j^T) = \lambda_j \mathbf{v}_i \mathbf{B} \mathbf{v}_j^T$ by the same logic, and the eigenvalues are distinct. Hence for $i \neq j$, we have $\mathbf{v}_i \mathbf{A} \mathbf{v}_j^T = 0 \Leftrightarrow \mathbf{v}_i \mathbf{B} \mathbf{v}_j^T = 0$. □

Now consider the matrix with the eigenvectors as its rows,

$$\mathbf{E} = \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \mathbf{v}_3 \\ \mathbf{v}_4 \end{pmatrix}.$$

Applying the change of coordinates $\mathbf{X} \mapsto \mathbf{XE}$ to $\mathcal{C}(\mathbf{A}, \mathbf{B})$, we have the equations

$$\mathbf{X}(\mathbf{E}\mathbf{A}\mathbf{E}^T)\mathbf{X}^T = (X\mathbf{v}_1 + Y\mathbf{v}_2 + Z\mathbf{v}_3 + W\mathbf{v}_4)\mathbf{A}(X\mathbf{v}_1^T + Y\mathbf{v}_2^T + Z\mathbf{v}_3^T + W\mathbf{v}_4^T) \tag{5}$$

Because all terms in which two different eigenvectors (hence, variables) are multiplied

[7] The left and right eigenvectors of a symmetric matrix are transposes of each other; we will be dealing with row (left) eigenvectors without loss of generality.

together vanish by Lemma 3.1, the final form of (5) is algebraically simple.

Theorem 3.2. *Any space quartic $\mathcal{C}$ is isomorphic to the curve defined by*

$$\begin{aligned} X^2 + Y^2 + Z^2 + W^2 &= 0 \\ \lambda_1 X^2 + \lambda_2 Y^2 + \lambda_3 Z^2 + \lambda_4 W^2 &= 0 \end{aligned}$$

where λ_i are the roots of a characteristic polynomial of $\mathcal{C}$.

Proof. When expanding (5), all terms cancel except those where the same eigenvector is involved via Lemma (3.1); in other words,

$$\begin{aligned} \mathbf{X}(\mathbf{E}\mathbf{A}\mathbf{E}^T)\mathbf{X}^T &= (\mathbf{v}_1\mathbf{A}\mathbf{v}_1^T)X^2 + (\mathbf{v}_2\mathbf{A}\mathbf{v}_2^T)Y^2 + (\mathbf{v}_3\mathbf{A}\mathbf{v}_3^T)Z^2 + (\mathbf{v}_4\mathbf{A}\mathbf{v}_4^T)W^2 \\ &= (\lambda_1\mathbf{v}_1\mathbf{B}\mathbf{v}_1^T)X^2 + (\lambda_2\mathbf{v}_2\mathbf{B}\mathbf{v}_2^T)Y^2 + (\lambda_3\mathbf{v}_3\mathbf{B}\mathbf{v}_3^T)Z^2 + (\lambda_4\mathbf{v}_4\mathbf{B}\mathbf{v}_4^T)W^2 \\ \mathbf{X}(\mathbf{E}\mathbf{B}\mathbf{E}^T)\mathbf{X}^T &= (\mathbf{v}_1\mathbf{B}\mathbf{v}_1^T)X^2 + (\mathbf{v}_2\mathbf{B}\mathbf{v}_2^T)Y^2 + (\mathbf{v}_3\mathbf{B}\mathbf{v}_3^T)Z^2 + (\mathbf{v}_4\mathbf{B}\mathbf{v}_4^T)W^2 \end{aligned}$$

Recall that an eigenvector can be scaled arbitrarily; in particular, for each eigenvector $\mathbf{v}_i$ we either have $\mathbf{v}_i\mathbf{B}\mathbf{v}_i^T = 0$ (in which case the corresponding term drops out of both $\mathbf{X}(\mathbf{E}\mathbf{A}\mathbf{E}^T)\mathbf{X}^T, \mathbf{X}(\mathbf{E}\mathbf{B}\mathbf{E}^T)\mathbf{X}^T$, contradicting our assumption that $\mathcal{C}(\mathbf{A}, \mathbf{B})$ is a space quartic) or we can scale $\mathbf{v}_i$ so that $\mathbf{v}_i\mathbf{B}\mathbf{v}_i^T = 1$. This gives us the desired form. □

Corollary 3.3. *Two space quartics that share a common characteristic polynomial are isomorphic.*

Proof. By Theorem 3.2, space quartics $\mathcal{C}, \mathcal{D}$ that share a common characteristic polynomial $P(\lambda)$ with roots $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ are both isomorphic to the space quartic given by Equation (6), hence isomorphic to each other. □

3.2 Degrees of freedom

The moduli space of elliptic curves is one-dimensional (the most common modulus being the j-invariant), so we might expect a normal form for space quartics with one free parameter like the Legendre form $y^2 = x(x-1)(x-l)$ and the Edwards form $x^2 + y^2 = a^2 + a^2x^2y^2$.

Lemma 3.4. *Every space quartic has a characteristic polynomial of the form*

$$Q(\lambda) = \lambda(\lambda - 1)(\lambda - l) \tag{6}$$

where l is a cross ratio *of the roots of any characteristic polynomial of the space quartic.*[8]

Proof. The invertible fractional linear transformation

$$\gamma : z \to \frac{(p-r)(z-q)}{(p-q)(z-r)} \tag{7}$$

takes four distinct values p, q, r, s (in this case, four roots of some characteristic polynomial P) to $1, 0, \infty, l$ respectively, where $l = \frac{(p-r)(s-q)}{(p-q)(s-r)}$ is the cross ratio of p, q, r, s, an invariant of ordered[9] quadruples under fractional linear transformation (see [2]). Given a characteristic polynomial $P(z)$ with roots $z = p, q, r, s$, the polynomial $Q(z) = P(\gamma^{-1}(z))$ therefore has roots $1, 0, \infty, l$, and the value of l does not depend on the choice of polynomial $P(z)$ (since it is an invariant under fractional linear transformation). □

[8] Recall that $Q(\lambda)$ is a notational convenience; in this case, for $Q(\alpha : \beta) = \alpha\beta(\beta - \alpha)(\beta - l\alpha)$.

[9] Changing the order of p, q, r, s produces six different values of l, which comprise the orbit of the group of fractional linear transformations generated by $l \mapsto \frac{1}{l}, l \mapsto 1 - l$. We will consider these six values of l be equivalent in the sense that they represent the same equivalence class of unordered quadruples p, q, r, s under fractional linear transformation.

3.3 Edwards form

Lemma 3.5. *Every space quartic has a characteristic polynomial of the form*

$$Q(\lambda) = (\lambda - 1)(\lambda + 1)(\lambda - a^2)(\lambda + a^2) \tag{8}$$

for some $a \in \mathbb{C}$ such that $a^5 \neq a$.

Proof. Beginning from a characteristic polynomial of the form $P(\lambda) = \lambda(\lambda - 1)(\lambda - l)$, which exists by Lemma 3.4, the fractional linear transformation

$$\epsilon : x \to \frac{2a^2x + (1 - a^2)}{2x - (1 - a^2)} \tag{9}$$

takes $1 \to 1, 0 \to -1, \infty \to a^2, l \to -a^2$, where $(a^2 - 1)^2 - 4a^2l = 0$. This fractional linear transformation produces another characteristic polynomial $Q(\lambda)$ with the desired roots. The transformation is invertible if and only if $a^5 \neq a$, since when either $a^2 = \pm 1$ or $a^2 = -a^2$ we have roots of multiplicity higher than one. □

Corollary 3.6. *Every space quartic is isomorphic to a curve of the form*

$$\begin{aligned} X^2 + Y^2 + Z^2 + W^2 &= 0 \\ X^2 - Y^2 + a^2Z^2 - a^2W^2 &= 0. \end{aligned}$$

Proof. The conclusion follows from Theorem 3.2 and Lemma 3.5. □

Theorem 3.7. *Every space quartic is isomorphic to a curve of the form*

$$\begin{aligned} XY - ZW &= 0 \\ X^2 + Y^2 - a^2Z^2 - a^2W^2 &= 0. \end{aligned} \tag{10}$$

Proof. Beginning from the form given in Corollary 3.6, the change of coordinates $\mathbf{X} \mapsto \mathbf{XN}$, where

$$\mathbf{N} = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{i}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & -\frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & -\frac{i}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix},$$

produces the desired form of Equation (10).[10] □

Theorem 3.8. *Every space quartic is birationally equivalent*[11] *to a planar elliptic curve in Edwards form* $R^2T^2 + S^2T^2 = a^2T^4 + a^2R^2S^2$.[12]

Proof. Abhyankar and Bajaj [1] give a method for rationally parameterizing a quadric surface by a stereographic projection from a point on the surface to the plane at infinity. Such a parameterization of the surface $XY - ZW = 0$ via a projection from the point $(0 : 0 : 0 : 1)$ is given by

$$X = RT, Y = ST, Z = T^2, W = RS$$

where $(R : S : T : 0)$ is the plane at infinity. The projection is in fact a birational transformation.[13] Substituting this parameterization into the other quadric surface in Equation (10) (a technique employed by Wang et al. [11]), we obtain the desired Edwards form in

[10] This transformation is possible even if we replace $\mathbb{C}$ by $\bar{K}$, where K is a perfect field of characteristic not equal to 2; in particular, i denotes a root of the polynomial $x^2 + 1 = 0$, which is defined over any field K, and $\sqrt{2}$ denotes a root of the polynomial $x^2 - 2 = 0$, which is defined over any field K of characteristic not equal to 2.

[11] Birational equivalence between a space quartic and a planar elliptic curve is not an isomorphism of varieties; the space quartic is singular while the planar curve is not.

[12] Edwards demonstrates that a given elliptic curve can be represented by Edwards form using one of 24 values of a. The polynomial relating a and the cross ratio (of which there are 6) is of degree 4, which gives us 24 values. One can verify that fractional linear transformations sending other permutations of $1, 0, \infty, L$ to $1, -1, a^2, -a^2$ give our 24 values of a.

[13] The inverse map takes $(X : Y : Z : W)$ to $(X : Y : Z)$.

projective coordinates

$$R^2T^2 + S^2T^2 = a^2T^4 + a^2R^2S^2 \tag{11}$$

which concludes the proof. □

4 Explicit planar forms for space quartics

Theorem 4.1. *Any space quartic with a given characteristic polynomial $P(\lambda)$ is birationally equivalent to a planar elliptic curve of the form*

$$y^2 = P(x).$$

Proof. From Theorem 3.7, any space quartic $\mathcal{C}$ is birationally equivalent to a planar curve $\mathcal{C}'$ of the form given by Equation (11). Edwards [5] uses a related normal form defined by the substitution $UT^2 = S(T^2 - a^2R^2)$ (also birationally equivalent), which produces from Equation (11) the equation

$$U^2T^2 = (a^2T^2 - R^2)(T^2 - a^2R^2).$$

Recall that we are working in projective coordinates. Without loss of generality, we can identify $(R : U : T)$ with $(r : u : a)$.[14] Then our equation becomes

$$u^2 = (a^4 - r^2)(1 - r^2).$$

This is an elliptic curve whose right hand side is a characteristic polynomial of $\mathcal{C}$ by Lemma 3.5. Fractional linear transformations (such as Equations (9) and (7)) can then be used to recover any desired characteristic polynomial $P(\lambda)$. □

[14] $T = 0$ corresponds to two points, both of which are singular.

Remark This result is already in the literature (see An, Kim, Marshall, Marshall, McCallum, Perlis [3]), but the proof given in this paper is independent and uses only basic geometric tools, whereas An et al. rely on classical invariant theory.

5 A geometric construction of the Edwards group law

The standard geometric construction for the group law on a planar cubic is as follows: given two points $\mathbf{P}', \mathbf{Q}'$[15] on a curve $\mathcal{C}'$, let $\mathbf{P}' * \mathbf{Q}'$ be the third intersection point of $\mathcal{C}'$ and the line through $\mathbf{P}', \mathbf{Q}'$.[16] Then the group law is given by $\mathbf{P}' \oplus \mathbf{Q}' = \mathbf{O}' * (\mathbf{P}' * \mathbf{Q}')$, where $\mathbf{O}'$ is an arbitrarily designated identity of the group.

This geometric construction is sensible even within the context of space quartics. Wang et al. [11] use Abhyankar et al.'s techniques [1] to find a stereographic projection from a space quartic $\mathcal{C}$ onto a planar cubic (rather than quartic) curve $\mathcal{C}'$; this projection is from a point $\mathbf{O}$ on the space quartic, and therefore the image of $\mathbf{O}$ is in fact the identity point $\mathbf{O}'$ at infinity on $\mathcal{C}'$. Because $\mathbf{P}', \mathbf{Q}', \mathbf{P}' * \mathbf{Q}'$ are collinear, it then follows that $\mathbf{P}, \mathbf{Q}, \mathbf{P} * \mathbf{Q}, \mathbf{O}$ are coplanar (here $\mathbf{P} * \mathbf{Q}$ denotes the pre-image of $\mathbf{P}' * \mathbf{Q}'$). We can therefore define the operation $*$ similarly on points on a space quartic; $\mathbf{P} * \mathbf{Q}$ is the fourth intersection point of $\mathcal{C}$ and the plane through $\mathbf{P}, \mathbf{Q}, \mathbf{O}$.[17]

How does this relate to our use of Edwards form, which is quartic rather than cubic? One of the primary motivations for Edwards' use of his normal form is that the group law

[15] We use $\mathbf{P}'$ to denote a point on a planar curve because in this section it is considered as the image of a map from a space quartic $\mathcal{C}$ to some planar curve $\mathcal{C}'$. $\mathbf{P}$ will then denote a point on the space quartic $\mathcal{C}$.

[16] If $\mathbf{P}'$ and $\mathbf{Q}'$ are identical, we consider instead the tangent line at $\mathbf{P}'$ (an intersection of multiplicity two); this construction is commonly referred to as the *tangent-chord construction*, and is valid because of Bezout's Theorem [9].

[17] This point is also guaranteed to exist uniquely because of Bezout's Theorem.

takes on an algebraic form analogous to the addition formulas for the sine and cosine:[18]

$$(p, q) \oplus (r, s) = \left(\frac{1}{a} \cdot \frac{ps + qr}{1 + pqrs}, \frac{1}{a} \cdot \frac{qs - pr}{1 - pqrs} \right). \tag{12}$$

The standard tangent-chord construction, however, breaks down. When we adapted Wang et al.'s projection to Edwards' form in Equation 11, we did not project from a point on our curve $\mathcal{C}$. Rather, we projected from a point $(0 : 0 : 0 : 1)$ on one of the surfaces defining $\mathcal{C}$ but not on the other. Because this point is not on $\mathcal{C}$, and in particular does not map to the identity $\mathbf{O'}$ (which in Edwards form is the point $(0, a)$), coplanarity in space no longer implies collinearity on the plane. However, our geometric depiction of the group law as a function of the intersection of $\mathcal{C}$ with a plane is still valid.

Theorem 5.1. *Given a space quartic $\mathcal{C}$ defined as in Equation* (10) *and two points $\mathbf{P'}(p, q), \mathbf{Q'}(r, s)$ on the corresponding Edwards plane curve (in affine coordinates) $C' : x^2 + y^2 = a^2 + a^2x^2y^2$, the points*

$$\mathbf{O}(0, a, 0), \mathbf{P}(p, q, pq), \mathbf{Q}(r, s, rs), (u, -v, -uv)$$

are coplanar, where $(u, v) = \mathbf{P'} + \mathbf{Q'}$ and $\mathbf{O}(0, a, 0)$ is the pre-image of the identity $\mathbf{O'}$ on $\mathcal{C}'$ and therefore the identity on $\mathcal{C}$.

Proof. For convenience, we are working in affine rather than projective coordinates. $\mathcal{C}$ is therefore the intersection of the quadric surfaces $xy = z, x^2 + y^2 = a^2 + a^2z^2$.

First, let's consider the case where $\mathbf{P}, \mathbf{Q}, \mathbf{O}$ are pairwise distinct points. They then define the plane

$$Ax + B(y - a) + Cz = 0$$

where $A = rs(q - a) - pq(s - a), B = pr(q - s), C = p(s - a) - r(q - a)$. We then wish to

[18] For the sine and cosine, 'addition' refers to angle summation in the same way that addition on a planar elliptic curve refers to summation of the parameter of a pair of elliptic functions parameterizing the curve [9] [8] [5]; in particular, these equations are given by $(p, q) \oplus (r, s) = (ps + qr, qs - pr)$, where $(p, q) = (\sin\theta, \cos\theta), (r, s) = (\sin\phi, \cos\phi), (ps + qr, qs - pr) = (\sin(\theta + \phi), \cos(\theta + \phi))$.

show that the point $(u, -v, -uv)$ is a point on this plane. Now,

$$Au + B(-v - a) - Cuv = \frac{N}{a^2(1 + pqrs)(1 - pqrs)}$$

where

$$\begin{aligned} N &= a^2pq^2r + q^3r^2s + a^3pqp^2q^2rr^2s^2 - a^3pp^2q^2rsr^2s^2 + app^2q^2r^3s - ap^3qrr^2s^2 \\ &+ app^2q^2rs^3 - a^2pp^2q^2rs^2 + a^2pq^2rr^2s^2 - a^2qr^2s + apqr^3 + a^2p^2qs - apq^3rr^2s^2 \\ &+ a^3prs - apq^2rs + apqrs^2 - a^2prs^2 - pq^2r^3 + p^3rs^2 - a^2p^2q^2qr^2s - p^2qs^3 \\ &+ a^2p^2qr^2s^2s - ap^3rs - a^3pqr. \end{aligned}$$

The clustering of p^2q^2 and r^2s^2 terms is intentional. When the substitutions $p^2q^2 = \frac{p^2+q^2-a^2}{a^2}$ and $r^2s^2 = \frac{r^2+s^2-a^2}{a^2}$ are made anywhere p^2q^2, r^2s^2 appear and we collect terms, we find that $N = 0$; hence, $(u, -v, -uv)$ is on the plane when $\mathbf{P}, \mathbf{Q}, \mathbf{O}$ are distinct.

When $\mathbf{P} = \mathbf{Q}$ we have $(u, v) = \left(\frac{1}{a} \cdot \frac{2pq}{1+p^2q^2}, \frac{1}{a} \cdot \frac{q^2-p^2}{1-p^2q^2}\right)$ and we consider the plane containing $\mathbf{O}$ and the tangent line at $\mathbf{P}$ (an intersection of multiplicity two, analogous to the tangent-chord construction). The tangent line to an intersection of quadric surfaces $\mathbf{X}\mathbf{A}\mathbf{X}^T = \mathbf{X}\mathbf{B}\mathbf{X}^T = 0$ at an arbitrary point $\mathbf{X}_0$ is the intersection of the tangent planes

$$\mathbf{X}_0\mathbf{A}\mathbf{X}^T = \mathbf{X}_0\mathbf{B}\mathbf{X}^T = 0.$$

The set of linear combinations of these tangent planes defines a *linear pencil* which is precisely the set of planes containing the tangent line at $\mathbf{X}_0$. Letting $\mathbf{X}_0 = \mathbf{P}$, we find that

$$\mathbf{P}\mathbf{A}\mathbf{X}^T = \frac{1}{2}(qx + py - z - pq) = 0, \mathbf{P}\mathbf{B}\mathbf{X}^T = px + qy - a^2pqz - a^2 = 0$$

and therefore that an appropriate plane in the linear pencil that also contains $\mathbf{O}$ is given by

$$2q\mathbf{PAX}^T - p\mathbf{PBX}^T = (aq + p^2)x + p(a + q)y - a(1 + p^2qz) - ap(a + q) = 0$$

We wish to show that $(u, -v, -uv)$ is a point on this plane. Substituting, the left hand side can be factored as

$$\frac{p(a + q)(p^2 + q^2 - a^2 - a^2p^2q^2)}{a(1 + p^2q^2)}$$

which vanishes when (p, q) is on $\mathcal{C}'$; hence, $(u, -v, -uv)$ is on the plane when $\mathbf{P} = \mathbf{Q}$.

Finally, when $\mathbf{Q} = \mathbf{O}$ (without loss of generality) we have $(u, v) = (p, q)$ and we consider the plane containing $\mathbf{P}$ and the tangent line at $\mathbf{O}$. The tangent line at $\mathbf{O}$ is the intersection of the tangent planes $ax - z = 0, a(y - a) = 0$. The corresponding plane that contains both the tangent line at $\mathbf{O}$ and the point $\mathbf{P}(p, q, pq)$ is given by

$$ax + p(y - a) - z = 0$$

Intersecting the plane with the quadric surface $xy - z = 0$ gives

$$(x - p)(a - y) = 0$$

and the only allowed values of (x, y) are $(0, a), (p, q), (p, -q)$. Hence $(u, -v, -uv)$ is on the plane when $\mathbf{Q} = \mathbf{O}$. □

In other words, the image of the point $\mathbf{P} \oplus \mathbf{Q} = \mathbf{O} * (\mathbf{P} * \mathbf{Q})$ under projection to $\mathcal{C}' : x^2 + y^2 = a^2 + a^2x^2y^2$ is precisely $\mathbf{P'} \oplus \mathbf{Q'}$, so the same geometric operation $*$ that describes the group law when we project from a space quartic $\mathcal{C}$ to a cubic planar curve also describes the group law when we project from a space quartic $\mathcal{C}$ to a planar curve in Edwards form. It is simply the fact that the point of projection in the latter is not on $\mathcal{C}$ that

causes the tangent-chord construction to fail in the plane. Nevertheless, our more general construction holds.

6 Conclusion

In this paper we gave an explicit normal form for curves of genus one in $\mathbb{CP}^3$, and used this normal form to construct a birational equivalence between any such curve to planar curves of genus one in $\mathbb{CP}^2$. We then demonstrated a geometric approach to the group law that generalized the tangent-chord construction to accomodate planar equations in Edwards form.

The geometric result relates directly to Edwards' discussion of so-called 'algebraic variations' in Section 10 of his paper.[5] The algebraic variations of a collection of points on a space quartic and a plane give rise to precisely the geometric group law we constructed, so this is an explicit validation of Abel's approach to the group law. The corresponding constraints in terms of holomorphic differentials, as well as the implications that examining elliptic curves in three dimensions have for the theory of elliptic functions, are beyond the scope of this paper and remain to be researched.

In addition, it is possible that using Edwards form rather than Weierstrass or Legendre form could simplify or otherwise shed light on calculations involving the group of rational points, the Selmer groups, the Tate-Shafarevich group, and so forth. The Edwards form itself is rather new, and this paper demonstrates only one of what could be many computational uses for it. The potential of this tool remains to be tapped.

7 Acknowledgments

I would like to thank Ryan Reich of the Harvard Mathematics Department, my RSI mentor, for providing me with vital background and guidance in in my research; Professor David Jerison, our coordinator, for his expertise and for suggesting my project idea; Professor Chris Skinner of Princeton University for introducing the topic of elliptic curves and projective space in the mathematics lectures at RSI; Dr. John Rickert, my RSI tutor, for his daily dose of feedback and support; Dr. Kent Merryfield for an enlightening discussion; Winston Luo, Benjamin Dozier, Jen Balakrishnan, Gabriel D. Carroll, Mark Kantrowitz, Scott Kominers, Zach Frankel, and David Farris for editing and commenting on various drafts of this paper; and finally, the Center for Excellence in Education, the Research Science Institute, and the Massachusetts Institute of Technology and other sponsors for allowing me the opportunity to conduct this research.

References

[1] S.S. Abhyankar, C. Bajaj. Automatic parameterization of rational curves and surfaces I: conics and conicoids. Comput. Aided Des. 19 (1) (1987) 11-14.

[2] L. V. Ahlfors. Complex Analysis (Third Edition). New York City: McGraw-Hill, 1979.

[3] S.Y. An, S.Y. Kim, D.C. Marshall, S.H. Marshall, W.G. McCallum, A.R. Perlis. Jacobians of genus one curves. Journal of Number Theory 90 (2001) 304-315.

[4] J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon, M. Stoll. Explicit n-descent on elliptic curves, I. Algebra. arXiv:math/0606580v1.

[5] H.M. Edwards. A normal form for elliptic curves. AMS Bulletin 44 (3) (2007) 393-422.

[6] R.T. Farouki, C.A. Neff, M.A. O'Connor. Automatic parsing of degenerate quadric-surface intersections. ACM Transactions on Graphics 8 (3) (1989) 174-203.

[7] J.Z. Levin. A parametric algorithm for drawing pictures of solid objects composed of quadrics. Comm. ACM 19 (10) (1976) 555-563.

[8] J.H. Silverman. The Arithmetic of Elliptic Curves. New York City: Springer, 1986.

[9] J.H. Silverman, J. Tate. Rational Points on Elliptic Curves. New York City: Springer, 1992.

[10] W. Wang, R. Goldman, C. Tu. Enhancing Levin's method for computing quadric-surface intersections. Computer Aided Geometric Design 20 (2003) 401-422.

[11] W. Wang, B. Joe, R. Goldman. Computing quadric surface intersections based on an analysis of plane cubic curves. Graphical Models 64 (2003) 335-367.