The Geometry of Flex Tangents to a Cubic Curve and its Parameterizations*

Jean-Marc Couveignes†‡ and Jean-Gabriel Kammerer§¶

September 2, 2011

Abstract

We show how the study of the geometry of the nine flex tangents to a cubic produces pseudo-parameterizations, including the ones given by Icart, Kammerer, Lercier, Renault and Farashahi, and infinitely many new ones.

To Jean-Jacques Quisquater, on the occasion of his éméritat

1 Introduction

Much attention has been focused recently on the problem of computing points on a given elliptic curve over a finite field in deterministic polynomial time. This problem arises in a very natural manner in many cryptographic protocols when one wants to encode messages into the group of points of an elliptic curve. A good example of the algorithmic and cryptologic motivations in finding these parameterizations can be found in the identity-based encryption from [4]. The difficulty is to deterministically find a field element x such that some polynomial in x is a square, see [14], Section 6.1.8. For example, when the curve is given by a reduced Weierstrass equation $y^2 = x^3 + ax + b$, we deterministically search x such that $x^3 + ax + b$ is a square in the field.

In 2006, Shallue and Woestjine [20] proposed a first practical deterministic algorithm. In 2009, Icart [12] proposed another deterministic encoding for elliptic curves over a field k with q elements, when q is congruent to 2 modulo 3. Icart's algorithm has quasi-quadratic complexity in $\log q$. Kammerer, Lercier and Renault [13] proposed a different encoding under the additional condition that the elliptic curve has a rational point of order 3, and even for a special class of hyperelliptic curves. Farashahi [8] found yet another parameterization for such elliptic curves too. A crucial point in [12, 13, 8] is that the map $x \mapsto x^3$ is bijective for a finite field k having cardinality congruent to 2 modulo 3. Its inverse map is $x \mapsto x^e$ where $e \bmod q - 1$ is the inverse of $3 \bmod q - 1$ and $0 \leq e < q - 1$. Exponentiation by e can be computed in deterministic time $(\log q)^{2+o(1)}$ using the fast exponentiation algorithm. So in order to deterministically compute points on an elliptic curve C

*Research supported by the "Agence Nationale de la Recherche" through project ALGOL (ANR-07-BLAN-0248) and by the French "Délégation Générale pour l'Armement".

†Corresponding author, Université de Toulouse le Mirail, 5 allées Antonio Machado, 31058 Toulouse Cédex 9, France. email : couveig@univ-tlse2.fr, telephone 33561504131, fax 33561504173.

‡INRIA Bordeaux Sud-Ouest, Institut de Mathématiques de Bordeaux, CNRS.

§DGA/MI, BP 7 35998 RENNES ARMEES.

¶IRMAR, Université de Rennes 1, Campus de Beaulieu, F-35042 Rennes.

over such a finite field, one can afford the usual field operations together with cubic roots. In other words, one looks for a parameterization of the elliptic curve by cubic radicals. Such a parameterization will be called a *pseudo-parameterization* in this article. Finding such a pseudo-parameterization is a special case of the problem of finding parameterizations of curves by radicals [19].

We show how such pseudo-parameterizations can be obtained from the study of the dual curve of the elliptic curve C. In a nutshell, we produce points on C as intersection points between C and well chosen lines. If D is a line in the projective plane, then the intersection $D.C$ consists of three points, counting multiplicities. These three points can be computed by solving a cubic equation. We recall in Section 2 how to derive the Tartaglia-Cardan formulae for this purpose. Recall these formulae run in two steps. One first has to compute a square root of the discriminant. The three solutions are then calculated using the field operations and cubic roots. Since cubic roots are not a problem in our context, the only remaining difficulty is computing the square root of the discriminant. So we choose the line D in such a way that the discriminant of the intersection $D.C$ is a square, and we assume that we have an algebraic formula for its square root. More precisely, we consider a line D_t depending on a rational formal parameter t. This means that the coefficients in the projective equation of D_t are polynomials in the indeterminate t. The discriminant $\Delta(t)$ of the intersection $L_t.C$ is then a rational fraction in t. We ask that this discriminant be a square in $k(t)$. We compute once for all a formal square root $\delta(t)$ of $\Delta(t)$. For every value of t we can then produce a point on C using only the field operations and cubic roots.

We recall in Section 3 that the projective lines in $\mathbb{P}$ are parametrized by the dual plane $\hat{\mathbb{P}}$. The line in $\mathbb{P}$ with projective equation $UX + VY + WZ = 0$ is represented by the point $[U : V : W] \in \hat{\mathbb{P}}$. A rational family of lines $t \mapsto D_t$ thus gives rise to a rational curve L inside $\hat{\mathbb{P}}$. Indeed, if the projective equation of D_t is $U(t)X + V(t)Y + W(t)Z = 0$ then the map $t \mapsto [U(t) : V(t) : W(t)]$ parametrizes a rational curve inside $\hat{\mathbb{P}}$. The discriminant $\Delta(t)$ vanishes whenever $D_t.C$ has a multiple root. This happens if and only if D_t is *tangent* to C. Not every projective line is tangent to C. The subset of $\hat{\mathbb{P}}$ corresponding to lines that are tangent to C is a curve denoted $\hat{C}$ and called the *dual curve of* C. So $\Delta(t)$ describes the intersection between the rational curve L and the dual curve $\hat{C}$. And $\Delta(t)$ is a square if and only if every point in the intersection between L and $\hat{C}$ has even multipicity. So we will be interested in rational curves L in $\hat{\mathbb{P}}$ that have even intersection with the dual curve to the cubic curve C. The connection between such curves and pseudo-parameterizations is detailed in Section 4.

Because the dual curve $\hat{C}$ plays such an important role we will study it in Section 3. This curve has genus 1 and 9 singularities, all cusps. Indeed the nine cusps of $\hat{C}$ correspond to the nine flex tangents to C, while the smooth points on $\hat{C}$ parametrize the tangent lines to C that are not flexes. These nine points in the dual plane form an interresting configuration that we study in Section 5. We are particularly interested in rational curves L passing through several among these nine points. We will find that many such curves L have even intersection with $\hat{C}$. We will show in Section 6 that these curves give rise to all the known pseudo-parameterizations of C found by Icart, Farashahi, Kammerer, Lercier, Renault, and to several new ones. It is then natural to ask how many rational curves on $\hat{\mathbb{P}}$ have even intersection with $\hat{C}$. We shall see in Section 7 that there are infinitely many such rational curves, giving rise to infinitely many inequivalent pseudo-parameterizations. These curves lift to rational curves on the degree two covering Σ of the dual plane ramified along $\hat{C}$. This will lead us to the classical and beautiful topic of rational curves on $K3$ surfaces.

Throughout the paper, we denote by k a field with characteristic different from 2 and 3, by $\bar{k} \supset k$ an algebraic closure of k, and by $\zeta_3 \in \bar{k}$ a primitive third root of unity. We set $\sqrt{-3} = 2\zeta_3 + 1$.

The Maple [17] code for the calculations in this article can be found on the authors' web pages.

2 Solving cubic equations

In this section we recall the Tartaglia-Cardan formulae for solving cubic equations by radicals. A modern treatment can be found in [6]. We believe it is worth stating these equations in an unambiguous form, that is well adapted to our context, and does not make excessive use of radicals and roots of unity. In other words we need regular and generic formulae. Let $h(x) = x^3 - s_1x^2 + s_2x - s_3$ be a degree 3 separable polynomial in $k[x]$. Call r_0, r_1 and r_2 the three roots of $h(x)$ in $\bar{k}$. Set

$$\delta = \sqrt{-3}(r_1 - r_0)(r_2 - r_1)(r_0 - r_2)$$

and $\Delta = \delta^2$. Note that Δ is the usual discriminant multiplied by -3. We call it the *twisted discriminant*. Since it is a symmetric function of the roots, it can be expressed as a polynomial in s_1, s_2 and s_3. Indeed

$$\Delta = 81s_3^2 - 54s_3s_1s_2 - 3s_1^2s_2^2 + 12s_1^3s_3 + 12s_2^3.$$

In particular Δ lies in k. Let $l = k(\zeta_3, \delta) \subset \bar{k}$ be the field obtained by adjoining δ and a primitive third root of unity to k. We set $m = l(r_1, r_2, r_0)$.

If the extension $l \subset m$ is non-trivial then it is a cyclic cubic extension. Since l contains a primitive third root of unity, this cubic extension is a Kummer extension: it is generated by the cubic root of some element in l. Let σ be the generator of the Galois group that sends r_i to r_{i+1} for $i \in \{0, 1, 2\}$, with the convention that indices make sense modulo 3. We set

$$\rho = r_0 + \zeta_3^{-1}r_1 + \zeta_3^{-2}r_2$$

and we check that $\sigma(\rho) = \zeta_3\rho$. We set $R = \rho^3$ and we check that R is invariant by σ. So R is an invariant for the alternate group acting on $\{r_1, r_2, r_3\}$ and it can be expressed as a polynomial in s_1, s_2, s_3 and δ. Indeed we find

$$R = \rho^3 = s_1^3 + \frac{27}{2}s_3 - \frac{9}{2}s_1s_2 - \frac{3}{2}\delta.$$

Similarly we set

$$\rho' = r_0 + \zeta_3r_1 + \zeta_3^2r_2$$

and we check that

$$R' = \rho'^3 = s_1^3 + \frac{27}{2}s_3 - \frac{9}{2}s_1s_2 + \frac{3}{2}\delta.$$

We note that $\rho\rho' = r_0^2 + r_1^2 + r_2^2 - r_0r_1 - r_1r_2 - r_2r_0$ is invariant by the full symmetric group and is indeed equal to $s_1^2 - 3s_2$. So both ρ and ρ' are computed by extracting a single cubic root.

Finally, the three roots r_0, r_1, r_2 can be expressed in terms of ρ by solving the linear system:

$$\begin{cases} r_0 + r_1 + r_2 & = & s_1 \\ r_0 + \zeta_3^{-1}r_1 + \zeta_3r_2 & = & \rho \\ r_0 + \zeta_3r_1 + \zeta_3^{-1}r_2 & = & \rho' \end{cases}$$

In particular the formula for the root

$$r_0 = \frac{s_1 + \rho + \rho'}{3} \tag{1}$$

does not involve ζ_3.

3 The dual curve of a cubic

In this section we review the properties of the dual of a cubic curve. A thorough treatment of the duality for plane curves can be found in [9] , [11] and [10]. Let $E = k^3$ and let $\hat{E}$ be the dual of E. Let $U = (1, 0, 0)$, $V = (0, 1, 0)$ and $W = (0, 0, 1)$. So (U, V, W) is the canonical basis of E. Let (X, Y, Z) be the dual basis of (U, V, W). Let $\mathbb{P} = \mathrm{Proj}(E) = \mathrm{Proj}\, k[X, Y, Z]$ be the projective plane over k. Let $\hat{\mathbb{P}} = \mathrm{Proj}(\hat{E}) = \mathrm{Proj}\, k[U, V, W]$ be the dual projective plane. The main idea of projective dualy is that points in $\hat{\mathbb{P}}$ parametrize lines in $\mathbb{P}$, and conversely. The point $[U : V : W]$ in $\hat{\mathbb{P}}$ corresponds to the line with equation $UX + VY + WZ = 0$ in $\mathbb{P}$. And the point $[X : Y : Z]$ in $\mathbb{P}$ parametrizes the line $XU + YV + ZW = 0$ in $\hat{\mathbb{P}}$.

Now let $C \subset \mathbb{P}$ be an absolutly integral curve with equation $F(X, Y, Z) = 0$. Let $F_X = \frac{\partial F}{\partial X}$, $F_Y = \frac{\partial F}{\partial Y}$, $F_Z = \frac{\partial F}{\partial Z}$ be the three partial derivatives of F. The tangent to C at a smooth point $P = [X_P : Y_P, Z_P]$ has equation

$$F_X(X_P, Y_P, Z_P)U + F_Y(X_P, Y_P, Z_P)V + F_Z(X_P, Y_P, Z_P)W = 0.$$

The corresponding point in $\hat{\mathbb{P}}$ is $[F_X(X_P, Y_P, Z_P) : F_Y(X_P, Y_P, Z_P) : F_Z(X_P, Y_P, Z_P)]$. The Zariski closure of the set of all such points is the *dual* $\hat{C}$ of C. So $\hat{C}$ is the closure of the image of the so called Gauss morphism

$$\begin{array}{llcl} \omega_C : & C^{smo} & \longrightarrow & \hat{\mathbb{P}} \\ & [X : Y : Z] & \longmapsto & [F_X(X, Y, Z), F_Y(X, Y, Z), F_Z(X, Y, Z)], \end{array}$$

where C^{smo} is the locus of smooth points on C.

We assume that the characteristic of k is odd, and that not every point on the curve C is a flex or a singular point (in particular C is not a line). Then $\hat{C}$ is an absolutely integral curve. And the dual of $\hat{C}$ is C. This is the biduality theorem [11, Theorem 5.91]. Duality is very useful because it translates properties of C into properties of $\hat{C}$ and conversely. In particular the Gauss map ω_C is a birational map from C to $\hat{C}$. It maps the flexes of C onto the cusps of $\hat{C}$.

The first non-trivial example of duality concerns conics (smooth plane projective curves of degree 2). The dual of conic is a conic.

We now assume that C is a smooth cubic. Then $\hat{C}$ has degree 6 and to each of the nine flexes of C there corresponds an ordinary cusp on $\hat{C}$. Since $\hat{C}$ has geometric genus 1 and arithmetic genus $10 = (6-1)(6-2)/2$ we deduce that there is no other singularity on it than these nine cusps. For example, if C has equation $F(X, Y, Z) = 0$ where

$$F(X, Y, Z) = X^3 + Y^3 + Z^3 - 3aXYZ, \tag{2}$$

then the dual curve has equation $G(U, V, W) = 0$ where

$$\begin{aligned} G(U, V, W) = U^6 + V^6 + W^6 - 6a^2(U^4VW + UV^4W + UVW^4) \\ +(4a^3 - 2)(U^3V^3 + U^3W^3 + V^3W^3) + (12a - 3a^4)U^2V^2W^2. \end{aligned} \tag{3}$$

The equation of the dual is found by eliminating X, Y, and Z in the system

$$\left\{ \begin{array}{lcl} U & = & F_X(X, Y, Z) \\ V & = & F_Y(X, Y, Z) \\ W & = & F_Z(X, Y, Z) \end{array} \right.$$

The real loci of the two curves C and $\hat{C}$ are represented in Figure 1 and Figure 2 respectively in the case $a = 0$.

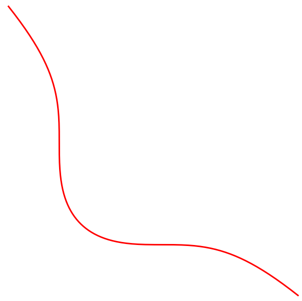

Figure 1: The cubic with equation $X^3 + Y^3 + Z^3 = 0$

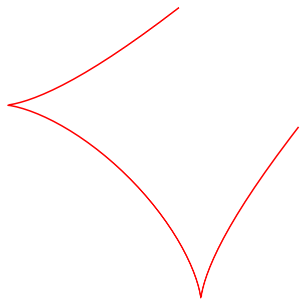

Figure 2: The dual curve with equation $U^6 + V^6 + W^6 - 2U^3V^3 - 2V^3W^3 - 2U^3W^3 = 0$

The equation of the dual curve arises naturally when one studies the intersection of the cubic C with a projective line D. Indeed such a line $D \subset \mathbb{P}$ meets C in exactly three points unless it is a tangent line to C (in which case we have one simple point and one double point) or even a flex (in which case we have one triple point). Assume that D is the line with equation

$$UX + VY + WZ = 0. \tag{4}$$

The intersection $D.C$ is described by the homogeneous system consisting of Equation (4) and the equation of the cubic C. We can use Equation (4) to eliminate one of the three variables X, Y, Z in the equation of C. We obtain a binary cubic homogeneous form in the two remaining variables, whose twisted discriminant $\Delta(U, V, W)$ is the equation of the dual curve $\hat{C}$ (up to a square). This is because this discriminant cancels exactly when the intersection $D.C$ has multiplicities.

4 Pseudo-parameterizations

Let C be an absolutely integral plane projective curve over a field k. A *parameterization* of C is a non-constant map from $\mathbb{P}^1$ onto C. In more concrete terms we have a point $P_t = [X(t) : Y(t) : Z(t)]$ on C, depending on one formal parameter t, the three projective coordinates beeing polynomials in $k[t]$. It is well known [19, theorem 4.11.] that a necessary condition for such a parameterization to exist is that C has geometric genus zero. In particular this never happens for an elliptic curve. One may relax the condition that the coordinates $X(t)$, $Y(t)$ and $Z(t)$ should lye in $k[x]$ and allow for more general algebraic functions. A typical restriction would be to ask that $X(t)$, $Y(t)$ and $Z(t)$ should belong to a radicial extension of $k(t)$. In other words they should be rational fractions in t and $\sqrt[e]{R(t)}$ for some positive integer e and some $R(t)$ in $k(t)$. As explained in the introduction we will be interested in the case when C is a smooth cubic, k is a field with characteristic different from 2 and 3, and $e = 3$. We want to parametrize plane cubics by cubic radicals. Such a parameterization will be called a *pseudo-parameterization* to avoid any confusion with rational parameterizations that do not exist for genus one curves. We will assume that $C(k)$ is non-empty. This is not a restriction if k is a finite field. We will even assume that C has a k-rational flex O. This is not a restriction either, because every cubic with a rational point is k-isomorphic to a plane cubic with a rational flex.

We sketched in the introduction how we claim to find pseudo-parameterizations. We consider a line

$$D_t : U(t)X + V(t)Y + W(t)Z = 0$$

in $\mathbb{P}$, depending on one rational parameter t. Since every line in $\mathbb{P}$ corresponds to a point in $\hat{\mathbb{P}}$ we can associate to the family D_t a rational curve $L \subset \hat{\mathbb{P}}$ which is the image of the map

$$t \mapsto [U(t) : V(t) : W(t)]. \tag{5}$$

We saw in Section 3 that the intersection $D_t.C$ is described by a cubic form whose twisted discriminant $\Delta(t)$ is, up to a square, equal to $G(U(t), V(t), W(t))$ where $G(U, V, W) = 0$ is the projective equation of the dual $\hat{C}$. So we look for polynomials $U(t)$, $V(t)$ and $W(t)$ such that $G(U(t), V(t), W(t))$ is a square in $k(t)$. A geometric interpretation of the latter condition is that the rational curve L meets the dual $\hat{C}$ with all even multiplicities. So we look for a rational curve $L \subset \hat{\mathbb{P}}$ that intersects the dual curve $\hat{C}$ with even multiplicities. Such a rational curve may be given by its projective equation, or as the image of a parameterization as in (5).

One may wonder if every pseudo-parameterization occurs in that way. We briefly explain why this is essentially the case. A pseudo-parameterization $t \mapsto P_t$ is a surjective map from a cyclic covering of $\mathbb{P}^1$ onto C. So we have two conjugated points P'_t and P''_t. Since C has a rational flex O, we have a chord and tangent group law, denoted $\oplus$, on it. We consider the sum $Q_t = P_t \oplus P'_t \oplus P''_t$. This is a point on C defined over $k(t)$, or equivalently a map $t \mapsto Q_t$. We saw that such a map must be constant because C has genus 1. So $P_t \oplus P'_t \oplus P''_t$ is a constant point $A \in C(k)$. If A is the origin O then for every value of the parameter t, the three points P_t, P'_t and P''_t are colinear. They lye on a line D_t with equation $U(t)X + V(t)Y + W(t)Z = 0$ where $U(t)$, $V(t)$ and $W(t)$ are in $k[t]$. So the pseudo-parameterization $t \mapsto P_t$ is of the type studied above. If A is not O, we may look for a point $B \in C(k)$ such that $B \oplus B \oplus B = A$. Such a point always exists if k is a finite field and $\#C(k)$ is not divisible by 3. Then we set $R_t = P_t \ominus B$ and check that $R_t \oplus R'_t \oplus R''_t = O$. So the pseudo-parameterization $t \mapsto P_t$ is of the type studied above, up to translation by a constant factor. In general, we set $R_t = P_t \oplus P_t \oplus P_t \ominus A$ and check that $R_t + R'_t + R''_t = O$. So $t \mapsto P_t$ is of the type studied above, up to a translation and a multiplication by 3 isogeny.

We will say that two pseudo-parameterizations $t \mapsto P_t$ and $t \mapsto Q_t$ are *equivalent* if there exists a birational fraction $\phi(t)$ such that $Q_t = P_{\phi(t)}$. We may wonder if two different families of projective lines $t \mapsto D_t$ and $t \mapsto E_t$ can give rise to equivalent pseudo-parameterization $t \mapsto P_t$ and $t \mapsto Q_t$. In that case $P_{\phi(t)} = Q_t$ lies in the intersection of $D_{\phi(t)}$ and E_t. If these two lines are distinct then their intersection consists of a single point $P_{\phi(t)} = Q_t$ defined over $k(t)$. Since every $k(t)$-rational point on C is constant we deduce that P_t and Q_t are constant. A contradiction. So $D_{\phi(t)} = E_t$ and the two families correspond by a change of variable. In particular the two associated rational curves in the dual plane are the same.

The conclusion is that finding pseudo-parameterizations boils down to finding rational curves L in the dual plane $\hat{\mathbb{P}}$ having even intersection with $\hat{C}$. It is natural to study first rational curves going through several cusps of $\hat{C}$, because the multiplicity intersection at a singular point is greater than and generically equal to 2. In the next section we look for such rational curves with a low degree.

5 The geometry of flexes

Let $C \subset \mathbb{P}$ be a smooth plane projective cubic. The nine flex points of C define a configuration in the plane $\mathbb{P}$. More interestingly, the nine flex tangents correspond to nine points in the dual plane $\hat{\mathbb{P}}$. We study the latter configuration. We are particularly interested in low degree *rational* curves going through many of these nine cusps of $\hat{C}$. Remind a *rational* curve is a curve with geometric genus 0 and a rational point. This is equivalent to the existence of a rational parameterization, see [19], theorem 4.11. We will first assume that C is the Hessian plane cubic given by Equation (2). Indeed, any smooth plane cubic can be mapped onto such an Hessian cubic by a projective linear transform, possibly after replacing k by a finite extension of it. The modular invariant of C is

$$j(a) = \frac{27a^3(a+2)^3(a^2-2a+4)^3}{(a-1)^3(a^2+a+1)^3}.$$

The nine flexes of C are the three points in the orbit of $O = (0 : -1 : 1)$ under the action of $\mathcal{S}_3$, plus the six points in the orbit of $(-1 : \zeta_3 : 0)$ under the action of $\mathcal{S}_3$. Let

$$\omega_C : (X : Y : Z) \mapsto (X^2 - aYZ : Y^2 - aXZ : Z^2 - aXY)$$

be the Gauss map associated with C. The images by ω_C of the nine flexes are the three points in the orbit of $(a : 1 : 1)$ under the action of $\mathcal{S}_3$ plus the six points in the orbit of $(\zeta_3^2 : \zeta_3 : a)$ under the action of $\mathcal{S}_3$. Figure 3 lists these flexes and their images by the Gauss map. We set $O = A_0 = (0 : -1 : 1)$ and $\hat{O} = B_0 = (a : 1 : 1)$.

Flex of C	Cusp on $\hat{C}$
$A_0 = (0 : -1 : 1)$	$B_0 = (a : 1 : 1)$
$A_1 = (-1 : 1 : 0)$	$B_1 = (1 : 1 : a)$
$A_2 = (1 : 0 : -1)$	$B_2 = (1 : a : 1)$
$A_3 = (-1 : \zeta_3 : 0)$	$B_3 = (\zeta_3^2 : \zeta_3 : a)$
$A_4 = (\zeta_3 : 0 : -1)$	$B_4 = (\zeta_3 : a : \zeta_3^2)$
$A_5 = (0 : -1 : \zeta_3)$	$B_5 = (a : \zeta_3^2 : \zeta_3)$
$A_6 = (\zeta_3 : -1 : 0)$	$B_6 = (\zeta_3 : \zeta_3^2 : a)$
$A_7 = (-1 : 0 : \zeta_3)$	$B_7 = (\zeta_3^2 : a : \zeta_3)$
$A_8 = (0 : \zeta_3 : -1)$	$B_8 = (a : \zeta_3 : \zeta_3^2)$

Figure 3: Flexes of C and the corresponding cusps on its dual

These nine points in the dual plane form an interesting configuration, depending on the single parameter a.

Position with respect to lines One can first check, e.g. by exhaustive search, that no three among these nine cusps in the dual plane are colinear unless the modular invariant is zero. See the proof of Proposition 1 in Section 7.2 of [5]. So the nine points in the dual plane corresponding to the nine flex lines are in general position with respect to lines. We deduce the following lemma by duality.

Lemma 1 *A smooth plane projective cubic over a field with prime to six characteristic has no three concurrent tangent flexes, unless its modular invariant is zero.*

Position with respect to conics We now consider the configuration of the nine flex tangents from the point of view of pencils of conics. Remember that six points in general position do not lie on any conic. Six pairwise distinct points lying on a conic are said to be *coconic*. Six pairwise distinct lines are said to be *coconic* if they all are tangent to a smooth conic.

Lemma 2 *Consider a smooth plane projective cubic over a field with prime to six characteristic and assume that its modular invariant is not zero. Remove* 3 *colinear flex points. The six tangents at the six remaining flexes are coconic. There are twelve such configurations of six coconic flex tangents.*

Note that we claim that the six flex tangents are coconic. Not the six flex points. Equivalently we claim that the six points in the dual plane corresponding to the six flex tangents are coconic.

We first note that the conic with equation $UW - aV^2 = 0$ meets $\hat{C}$ at $(a : 1 : 1)$, $(1 : 1 : a)$, $(\zeta_3^2 : \zeta_3 : a)$, $(a : \zeta_3^2 : \zeta_3)$, $(\zeta_3 : \zeta_3^2 : a)$, and $(a : \zeta_3 : \zeta_3^2)$. The three remaining flexes in $\mathbb{P}$ are $(1 : 0 : -1)$, $(\zeta_3 : 0 : -1)$ and $(1 : 0 : \zeta_3)$ and they lie on the line with equation $Y = 0$. The action of $\mathcal{S}_3$ produces two more similar conics.

The conic with equation $U^2 + V^2 + W^2 + (a+1)(UV + UW + VW) = 0$ meets $\hat{C}$ at the six points in the orbit of $(\zeta_3^2 : \zeta_3 : a)$ under the action of $\mathcal{S}_3$. The three remaining flexes in $\mathbb{P}$ are $(0 : -1 : 1)$, $(-1 : 1 : 0)$, and $(1 : 0 : -1)$. They lie on the line with equation $X + Y + Z = 0$.

The conic with equation $U^2 + \zeta_3 V^2 + \zeta_3^2 W^2 + (a+1)(\zeta_3^2 UV + \zeta_3 UW + VW) = 0$ meets $\hat{C}$ at the three points in the orbit of $(a : 1 : 1)$ under the action of $\mathcal{S}_3$. And also at the three points in the orbit of $(\zeta_3^2 : \zeta_3 : a)$ under the action of $\mathcal{S}_3$. The three remaining flexes in $\mathbb{P}$ are $(0 : \zeta_3 : -1)$, $(\zeta_3 : -1 : 0)$, and $(-1 : 0 : \zeta_3)$. They lie on the line with equation $X + \zeta_3 Y + \zeta_3^2 Z = 0$. The action of $\mathcal{S}_3$ produces one more such conic.

The conic with equation $\zeta_3 U^2 + V^2 + \zeta_3 W^2 + (a + \zeta_3^2)(UV + \zeta_3^2 UW + VW) = 0$ meets $\hat{C}$ at $(a : 1 : 1)$, $(1 : 1 : a)$, $(\zeta_3 : a : \zeta_3^2)$, $(a : \zeta_3^2 : \zeta_3)$, $(\zeta_3 : \zeta_3^2, a)$, $(\zeta_3^2 : a : \zeta_3)$. The three remaining flexes in $\mathbb{P}$ are $(1 : 0 : -1)$, $(-1 : \zeta_3 : 0)$, and $(0 : \zeta_3 : -1)$. They lie on the line with equation $\zeta_3 X + Y + \zeta_3 Z = 0$. The action of $\mathcal{S}_3$ produces five more conics.

We thus obtain twelve smooth conics that cross the dual curve $\hat{C}$ at six out of its nine cusps. Each of these conics is associated with one of the twelve triples of colinear flexes. □

Four among these twelve conics are especially interesting because their equations do not involve ζ_3. We note that three among these four conics are clearly rational over $k(a)$ because they have an evident $k(a)$ rational point. The last one is rational also because its quotient by the evident automorphism of order 3 is $\mathbb{P}^1$ over $k(a)$.

Position with respect to cubics Next we study the pencil of cubics going through the nine points in the dual plane associated with the nine flex tangents. It has projective dimension zero in general. The cubic with equation

$$a(U^3 + V^3 + W^3) = (a^3 + 2)UVW$$

goes through all these nine points in the dual plane. This cubic is in general non-singular. So it is not particularly interesting for our purpose.

Position with respect to quartics We now consider curves of degree 4 in the dual plane. The projective dimension of the space of plane quartics is 14. So we can force a quartic to meet the 9 points we are interested in and there remains 5 degrees of freedom. Since we are particularly interested in rational curves we use these remaining degrees of freedom to impose a big singularity at $\hat{O} = B_0 = (a:1:1)$. Indeed, two degrees of freedom suffice to cancel the degree 1 part in the Taylor expansion at $\hat{O}$. And three more degrees of freedom suffice to cancel the degree 2 part also. We find a rational quartic Q in $\hat{\mathbb{P}}$ passing through the nine cusps of $\hat{C}$ and having intersection multiplicity at least two at each of them (because they are cusps) and at least six at the cusp $\hat{O}$. The equation of this rational quartic Q is

$$\begin{aligned} U^4 + a(V^4+W^4) - 2a(U^3V + U^3W + V^3W + VW^3) - (a^3+1)U(V^3+W^3) \\ +3a^2U^2(V^2+W^2) + (a^4+2a)V^2W^2 + (1-a^3)UVW(V+W) = 0. \end{aligned}$$

This quartic is irreducible as soon as the modular invariant of C is non-zero, which we assume from now on. Computing the intersection with all lines through $\hat{O}$ we find the following parameterization of this quartic

$$\begin{aligned} U(t) &= a^2t^4 - 2at^3 + (a^3+2)t^2 - 2a^2t + a, \\ V(t) &= a^4t^4 + (1-3a^3)t^3 + 3a^2t^2 - 2at + 1, \\ W(t) &= at^4 - (a^3+1)t^3 + 3a^2t^2 - 2at + 1. \end{aligned}$$

Substituting U, V, and W by $U(t)$, $V(t)$, and $W(t)$ in the equation of $\hat{C}$ we find the degree 24 polynomial

$$t^6(t+1)^2(t^2-t+1)^2(at-2)^2((a+1)t-1)^2((a^2-a+1)t^2+(1-2a)t+1)^2(a^2t^2+1-at)^2.$$

We check that Q has two branches at $\hat{O}$. One branch corresponds to $t=0$, and it has intersection multiplicity 6 with $\hat{C}$. The other branch corresponds to $t = 2/a$, and it has intersection multiplicity 2 with $\hat{C}$. This is illustrated by Figure 4 where the real locus of $\hat{C}$ is in black and the real locus of Q is in red. So the total multiplicity of $Q.\hat{C}$ at $\hat{O}$ is 8. And the intersection $Q.\hat{C}$ only consists of cusps of $\hat{C}$; one with multiplicity 8 and the eight others with multiplicity 2. The real part of this intersection locus is visible on Figure 4.

Lemma 3 *Consider a smooth plane projective cubic C over a field with prime to six characteristic and assume that its modular invariant is not zero. Let $\hat{C}$ be the dual of C. Let $\hat{O}$ be one of the nine cusps of $\hat{C}$. There exists a rational quartic Q in the dual plane, such that the intersection $Q.\hat{C}$ has multiplicity 8 at $\hat{O}$ and 2 at each of the eight remaining cusps. In particular $Q.\hat{C}$ is an even combination of cusps of $\hat{C}$.*

We stress that the definition of the quartic Q involves one flex on the one hand, and the eight remaining flexes on the other hand. So we can define this quartic for any cubic having a rational flex, that is for any elliptic curve (and this makes a difference with the four conics constructed earlier, that distinguish a triple of colinear flexes, and therefore cannot always be defined over the base field.)

So we can take for C an elliptic curve with Weierstrass equation

$$F(X,Y,Z) = Y^2Z - X^3 - aXZ^2 - bZ^3. \tag{6}$$

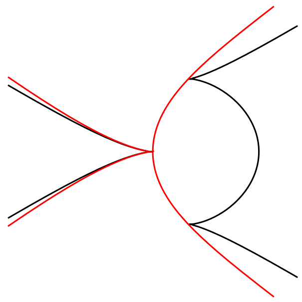

Figure 4: The real part of the intersection of $\hat{C}$ and Q.

We assume $a \neq 0$, so the modular invariant is non-zero either. The image of the origin $O = (0 : 1 : 0)$ by the Gauss map is $\hat{O} = (0 : 0 : 1)$, and the quartic $\hat{Q}$ given by Lemma 3 has equation

$$U^4 - 3V^4 + 6UV^2W = 0,$$

and parameterization

$$\begin{aligned} U(t) &= 6t^2, \\ V(t) &= 6t^3, \\ W(t) &= 3at^4 - 1. \end{aligned} \tag{7}$$

6 Intersecting a cubic with lines

In this section we assume that the map $a \mapsto a^3$ from k to k is surjective. This is the case if k is the field of real numbers for example. This is also the case if k is a finite field with q elements when q is congruent to 2 modulo 3. For every element a in k we choose once and for all a cubic root $\sqrt[3]{a}$ of a. This way we define a map $\sqrt[3]{} : k \rightarrow k$. We will use the general recipe in Section 4 and the rational curves exhibited in Section 5 to produce several pseudo-parameterizations of a plane cubic C.

6.1 Intersecting the dual curve with a conic

We may first take L to be one of the twelve conics in Lemma 2. So we assume that C is the Hessian cubic given by Equation (2) for some a such that $a^3 \neq 1$. Four conics, among the twelve conics given in Lemma 2, are rational over $k(a)$. The intersection $L.\hat{C}$ has degree 12 and contains six among the nine cusps of $\hat{C}$, each with multiplicity 2. So this intersection is exactly twice the sum of these six cusps. If we take for L the conic with equation $UW - aV^2 = 0$ then a convenient parameterization is given by $U(t) = 1$, $V(t) = -t$ and $W(t) = at^2$. The corresponding line D_t has equation

$$X - tY + at^2Z = 0.$$

We substitute X by $tY - at^2Z$ in the Hessian Equation (2) and find the degree 3 form in Y and Z

$$(t^3 + 1)Y^3 - 3at(t^3 + 1)Y^2Z + 3a^2t^2(t^3 + 1)YZ^2 + (1 - a^3t^6)Z^3$$

describing the intersection $C.D_t$. We divide by $(t^3+1)Z^3$ and we obtain a cubic polynomial in $y = Y/Z$ whose twisted discriminant is

$$\Delta(t) = \left(\frac{9(1+a^3t^3)}{1+t^3}\right)^2.$$

We use the formulae and notation in Section 2. We have

$$\begin{aligned}
s_1 &= 3at, \\
s_2 &= 3a^2t^2, \\
s_3 &= \frac{a^3t^6-1}{t^3+1}, \\
\delta &= \frac{9(1+a^3t^3)}{1+t^3}, \\
R &= -27\frac{a^3t^3+1}{t^3+1}, \\
R' &= 0.
\end{aligned}$$

So we find the solution

$$y = at - \sqrt[3]{\frac{a^3t^3+1}{t^3+1}},$$

and we deduce

$$x = X/Z = ty - at^2 = -t\sqrt[3]{\frac{a^3t^3+1}{t^3+1}},$$

This is the pseudo-parameterization found by Farashahi [8].

6.2 Intersecting the dual curve with a quartic

Assume now that we take L to be the rational quartic Q in Lemma 3. All the multiplicities in the intersection $Q.\hat{C}$ are even. So we expect the twisted discriminant to be a square. This time we may as well take for C the Weierstrass cubic in Equation (6). The parameterization of Q given in Equation (7) provides a one parameter family of lines $(D_t)_t$ with equation

$$6t^2X + 6t^3Y + (3at^4 - 1)Z = 0.$$

We divide by Z, we set $x = X/Z$, $y = Y/Z$ and we substitute y by $1/(6t^3) - at/2 - x/t$ in the Weierstrass Equation (6). We find a cubic equation $x^3 - s_1x^2 + s_2x - s_3$ in $x = X/Z$, where

$$\begin{aligned}
s_1 &= 1/t^2, \\
s_2 &= 1/(3t^4), \\
s_3 &= (1/t^6 - 6a/t^2 - 36b + 9a^2t^2)/36.
\end{aligned}$$

Using the formulae and notation in Section 2 we find

$$\begin{aligned}
\delta &= (-1/t^6 - 108b - 18a/t^2 + 27a^2t^2)/12, \\
R &= 0, \\
R' &= (-1/t^6 - 108b - 18a/t^2 + 27a^2t^2)/4.
\end{aligned}$$

So we find the solution

$$x = X/Z = \frac{1}{3t^2} + \sqrt[3]{\frac{a^2t^2}{4} - \frac{1}{108t^6} - b - \frac{a}{6t^2}}$$

and

$$y = Y/Z = \frac{1}{6t^3} - at/2 - x/t.$$

This is the pseudo-parameterization found by Icart [12], up to the change of variable $t \leftarrow -1/t$.

6.3 Intersecting the dual curve with a line

Assume finally that we take for L a line passing through two rational cusps of $\hat{C}$. So we assume that C is the Hessian cubic given by Equation (2) for some $a^3 \neq 1$. Assume L is the unique line passing through the two cusps $B_0 = (a : 1 : 1)$ and $B_2 = (1 : a : 1)$ of $\hat{C}$. The intersection $L.\hat{C}$ has degree 6. Since $(a : 1 : 1)$ and $(1 : a : 1)$ each have intersection multiplicity ≥ 2, there remains at most two intersection points. An illustration of this situation in the real projective plane is given on Figure 5.

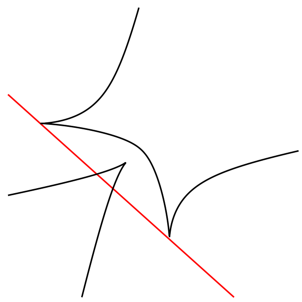

Figure 5: The intersection of $\hat{C}$ and L

Not all the multiplicities in the intersection $L.\hat{C}$ are even, but only two multiplicities are odd. So we expect $\Delta(t)$ to be a square times a degree 2 polynomial in t. Points on $L \subset \hat{\mathbb{P}}$ represent a linear pencil of lines in $\mathbb{P}$ generated by the tangents to C at $(0 : -1 : 1)$ and $(1 : 0 : -1)$. The first tangent has equation $aX + Y + Z = 0$. The second tangent has equation $X + aY + Z = 0$. So let t be a formal parameter and consider the line D_t with equation $(at+1)X + (t+a)Y + (t+1)Z = 0$. The tangent at $(0 : -1 : 1)$ corresponds to the value $t = \infty$. The tangent at $(1 : 0 : -1)$ corresponds to the value $t = 0$. The line D_t meets the fixed point $(1 : 1 : -a-1)$ and the moving point $(1, -t, t-1)$. So a parametric description of D_t is given by

$$i \mapsto (i + 1 : i - t : t - 1 - (a + 1)i).$$

We substitute X by $i + 1$, Y by $i - t$ and Z by $t - 1 - (a + 1)i$ in Equation (2) and divide by the leading coefficient. We find the degree three polynomial

$$h(i) = i^3 + \frac{3t(a+2)i}{a^2+a+1} + \frac{3t(1-t)}{a^2+a+1} \tag{8}$$

defining the intersection $D_t.C$. The twisted discriminant of h is

$$\Delta(t) = 81t^2 \frac{9(a^2+a+1)t^2 + 2(2a+1)(a^2+a+7)t + 9(a^2+a+1)}{(a^2+a+1)^3}. \tag{9}$$

This is not quite a square in $k(a)(t)$. However, it only has two roots with odd multiplicity. So if we substitute t by a well chosen rational fraction, we can turn Δ into a square. So we look for a parameterization of the plane projective conic with equation

$$(a^2+a+1)S^2 = 9(a^2+a+1)T^2 + 2(2a+1)(a^2+a+7)TK + 9(a^2+a+1)K^2. \qquad (10)$$

This conic has two evident k-rational points, namely $(3:1:0)$ and $(3:0:1)$. The line through these two points has equation

$$-S+3T+3K=0.$$

The tangent at $(3:0:1)$ has equation

$$3(a^2+a+1)S-(2a+1)(a^2+a+7)T-9(a^2+a+1)K=0.$$

The generic line in the linear pencil generated by these two lines has equation

$$(3(a^2+a+1)-j)S+(3j-(2a+1)(a^2+a+7)j)T+(3j-9(a^2+a+1)j)K=0 \qquad (11)$$

where j is a formal parameter.

Intersecting the conic in Equation (10) with the line in Equation (11) we find the parameterization

$$\begin{cases} S(j) &= 3j^2-2(a+2)^3j+3(a+2)^3(a^2+a+1), \\ T(j) &= j(j-3(a^2+a+1)), \\ K(j) &= (a^2+a+1)((a+2)^3-3j). \end{cases}$$

We now substitute t by $T(j)/K(j)$ in Equation (8) and find a cubic polynomial with coefficients in the field $k(a)(j)$. If we substitute t by $T(j)/K(j)$ in Equation (9) we find that $\Delta = \delta^2(j)$ where

$$\delta(j) = \frac{9j(3j^2-2(a+2)^3j+3(a^2+a+1)(a+2)^3)(3(a^2+a+1)-j)}{((a+2)^3-3j)^2(a^2+a+1)^3}.$$

We use the formulae and notation in Section 2. The polynomial h in Equation (8) has coefficients 1, $-s_1$, s_2 and $-s_3$ with

$$\begin{aligned} s_1 &= 0 \\ s_2 &= -\frac{3j(a+2)(3(a^2+a+1)-j)}{(a^2+a+1)^2((a+2)^3-3j)} \\ s_3 &= \frac{3j(3(a^2+a+1)-j)((a^2+a+1)(a+2)^3-j^2)}{(a^2+a+1)^3((a+2)^3-3j)^2}. \end{aligned}$$

We deduce the following pseudo-parameterization of the cubic C

$$\begin{aligned} R(j) &= \frac{27j^2(3(a^2+a+1)-j)}{((a+2)^3-3j)(a^2+a+1)^3} \\ \rho(j) &= \sqrt[3]{R(j)} \\ \rho'(j) &= \frac{9j(a+2)(3(a^2+a+1)-j)}{(a^2+a+1)^2((a+2)^3-3j)\rho(j)} \\ i(j) &= \frac{\rho(j)+\rho'(j)}{3} \\ t(j) &= \frac{j(3(a^2+a+1)-j)}{(a^2+a+1)((a+2)^3-3j)} \\ P(j) &= (i(j)+1 : i(j)-t(j) : t(j)-1-(a+1)i(j)). \end{aligned}$$

where $P(j)$ is the point on C associated with the parameter j.

We illustrate this situation on Figure 6 in the case $a = 2$. The red segment corresponds to the parameter j taking values in the interval $[-4, -0.3]$. We also note that the computation in Section 3.1 of [13] hides a similar geometric situation.

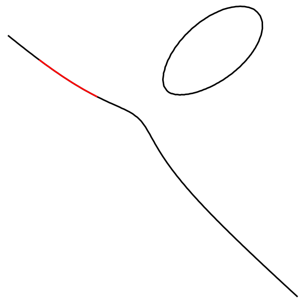

Figure 6: A pseudo-parameterization

7 Classifying pseudo-parameterization

We have seen many different pseudo-parameterizations of a plane cubic, each associated with a rational curve in $\hat{\mathbb{P}}$ having even intersection with the dual curve $\hat{C}$ in Equation (3). We may wonder if there exist more such rational curves, leading to more pseudo-parameterizations. We may also try to put some structure on the set of such curves. This is our purpose of this section. We assume that the reader has some familiarity with algebraic surfaces as presented in [22, 1], and particularly with elliptic and K3 surfaces [18, 7, 3]. We shall not enter into the details. Any rational curve L having even intersection with $\hat{C}$ lifts to a rational curve on the degree two covering Σ of $\hat{\mathbb{P}}$ branched along $\hat{C}$. To define Σ we consider the function field $k(a)(U/W, V/W)$ of $\hat{\mathbb{P}}$ over $k(a)$. We define a quadratic extension of this field by adding a square root γ of $G(U, V, W)/W^6$ where $G(U, V, W)$ is the equation of $\hat{C}$. The normal closure of $\hat{\mathbb{P}}$ inside $k(a)(U/W, V/W, \gamma)$ is Σ. It has nine singularities. One above each of the nine cusps of $\hat{C}$. In order to obtain a smooth model for Σ, we first blow up $\hat{\mathbb{P}}$ at each of the cusps of $\hat{C}$. We call Π the resulting surface. The inverse image of $\hat{C}$ by $\Pi \to \hat{\mathbb{P}}$ consists of one smooth genus one curve and 9 rational curves tangent to it. We call S the normal closure of Π in $k(a)(U/W, V/W, \gamma)$. This is a smooth surface, the minimal model of Σ.

We call σ_1 the automorphism of $\hat{\mathbb{P}}$ that maps $[U : V : W]$ onto $[V, W, U]$. We call σ_2 the automorphism of $\hat{\mathbb{P}}$ that maps $[U : V : W]$ onto $[U, \zeta_3 V, \zeta_3^2 W]$. We call σ_3 the automorphism of $\hat{\mathbb{P}}$ that maps $[U : V : W]$ onto $[V, U, W]$. We extend these three automorphisms to $k(a)(U/W, V/W, \gamma)$ by sending γ to itself. The resulting automorphisms are called σ_1, σ_2 and σ_3 also. They induce automorphisms of Π, Σ and S denoted σ_1, σ_2 and σ_3 again. We call σ_4 the unique non-trivial automorphism of $k(a)(U/W, V/W, \gamma)$ over $k(a)(U/W, V/W)$. It induces automorphisms of Σ and S denoted σ_4. The action of σ_1, σ_2, σ_3 on the B_i is given by the following three permutations of the indices

$$\begin{aligned} \sigma_1 &= (0,1,2)(3,4,5)(6,7,8), \\ \sigma_2 &= (0,5,8)(1,3,6)(2,4,7), \\ \sigma_3 &= (0,2)(1)(3,6)(4,8)(5,7). \end{aligned}$$

The group generated by σ_1 and σ_2 has order nine. It acts simply transitively on the nine cusps, and also on the nine corresponding rational curves on the blow up Π. We choose one of the two rational curves on S above B_0 and call it E_0. For $1 \leq i \leq 9$ we call E_i the image of E_0 by the unique automorphism in $< \sigma_1, \sigma_2 >$ that maps B_0 onto B_i. We call F_i the image of E_i by σ_4. We thus obtain eighteen rational curves on S. Let H be the inverse image by $S \to \hat{\mathbb{P}}$ of any line in $\hat{\mathbb{P}}$. The lattice generated by the E_i, F_i and H in the Néron-Severi group has rank 19, and discriminant 2.3^9. The intersection indices are

$$
\begin{aligned}
E_i.F_i &= 1,\\
E_i^2 &= -2,\\
F_i^2 &= -2,\\
E_i.E_j &= 0 \text{ for } i \neq j,\\
E_i.F_j &= 0 \text{ for } i \neq j,\\
E_i.H &= 0,\\
F_i.H &= 0,\\
H^2 &= 2.
\end{aligned}
$$

Let D be a generic line in $\hat{\mathbb{P}}$ through B_0. The intersection of $D.\hat{C}$ is $2B_0$ plus an effective degree four divisor. So the inverse image of D in S is the union of E_0, F_0 and a genus one curve with at least two rational points : the intersection points with E_0 and F_0. Thus the inverse image by $S \to \hat{\mathbb{P}}$ of the pencil of lines through B_0 defines an elliptic fibration $f : S \to \mathbb{P}^1$ of S, with two sections E_0 and F_0, so S is an elliptic K3 surface. The following lemma [15, 2.3] is usefull when looking for rational curves on a K3 surface.

Lemma 4 *Let D be a class with self-intersection -2 in the Néron-Severi group of a K3 surface. Then either D or $-D$ contains an effective divisor. If this divisor is irreducible then it is a smooth rational curve.*

We may also look for singular rational curves in classes with positive self-intersection. One can even count rational curves in such classes [2, 16, 21]. Since there are many of them, they are unlikely to be defined over the base field. Indeed, all the rational curves in Section 5 lift to smooth rational curves on S having self-intersection -2. For example the conic in $\hat{\mathbb{P}}$ passing through B_0, B_1, B_2, B_3, B_4, B_5 lifts to a rational curve I_{012345} on S. We have $H.I_{012345} = 2$, $E_0.I_{012345} = E_1.I_{012345} = E_2.I_{012345} = 1$ and $F_3.I_{012345} = F_4.I_{012345} = F_5.I_{012345} = 1$ and I_{012345} has zero intersection with the remaining E_i and F_i. We deduce the following identity in the Néron-Severi group

$$3I_{0,1,2,3,4,5} = 3H - 2(E_0 + E_1 + E_2) - (F_1 + F_2 + F_3) - (E_3 + E_4 + E_5) - 2(F_3 + F_4 + F_5),$$

and $I_{0,1,2,3,4,5}$ has self-intersection -2. We find similarly, and with evident notation,

$$3I_{0,1,3,4,7,8} = 3H - 2(E_0 + E_3 + E_7) - (F_0 + F_3 + F_7) - (E_1 + E_4 + E_8) - 2(F_1 + F_4 + F_8),$$

and

$$3I_{0,1,3,5,6,8} = 3H - 2(E_0 + E_5 + E_8) - (F_0 + F_5 + F_8) - (E_1 + E_3 + E_6) - 2(F_1 + F_3 + F_6).$$

The action of $< \sigma_1, \sigma_2, \sigma_3, \sigma_4 >$ produces 24 similar smooth rational curves on S with self intersection -2. This is the contribution of conics in Lemma 2.

Now consider the quartic given by Lemma 3. It lifts to a rational curve J_0 on S, such that $J_0.H = 4$, $J_0.E_0 = 2$, $J_0.F_0 = 1$, $J_0.E_i = 1$, $J_0.F_i = 0$ for $1 \leq i \leq 8$. We have the following identity in the Néron-Severi group

$$3J_0 = 6H - 5E_0 - 4F_0 - \sum_{1 \leq i \leq 8} (2E_i + F_i).$$

The action of $< \sigma_1, \sigma_2, \sigma_4 >$ produces 18 such rational curves with self intersection -2. The lattice generated by H, the nine E_i, the nine F_i, and the $24 + 18$ classes coming from conics and quartics, has dimension 19 and discriminant 54. This is the full Néron-Severi group of S when k has characteristic zero and a is a transcendental. Using the knowledge of this Néron-Severi group we can prove that there are infinitely many rational curves on S, leading to infinitely many pseudo-parameterizations of the cubic C. We consider an elliptic-fibration of S, for example the fibration $f : S \to \mathbb{P}^1$ introduced above. We choose the section E_0 as origin. The generic fiber of f is an elliptic curve over the function field $k(t)$ of $\mathbb{P}^1$. Fibers of f map onto lines through B_0 in $\hat{\mathbb{P}}$. The height singular fibers of f map onto the lines B_0B_i for $1 \leq i \leq 8$. Each of them has Kodaira type I_3, the three irreducible components being E_i, F_i, and a third rational curve G_i crossing E_0 and F_0. Let $T \subset \mathrm{NS}(S)$ be the group generated by the zero section E_0 and the fiber components E_i, F_i, G_i for $1 \leq i \leq 8$. The Mordell-Weil group of the generic fiber is isomorphic [18, Theorem 6.3] to the quotient $\mathrm{NS}(S)/T$. Since $E_i + F_i + G_i = H - E_0 - F_0$ does not depend on i for $1 \leq i \leq 8$, the rank of T is 18 and the rank of $\mathrm{NS}(S)$ is one. So we have infinitely many sections of f. The images of these sections all are rational curves with self intersection -2. We draw one of these rational curves (rather its image in $\hat{\mathbb{P}}$) on Figure 7. In case C is the Weierstrass cubic in Equation (6), a parameterization of this rational curve is

$$\begin{aligned} U(t) &= 4at^6 + 4t^2/27, \\ V(t) &= t(4at^6 + 4t^2/27), \\ W(t) &= a^2t^8 + 2at^4/27 + 4bt^6 + 1/81. \end{aligned} \tag{12}$$

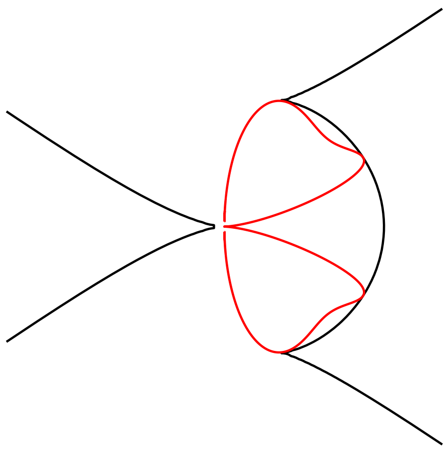

Figure 7: One more rational curve having even intersection with $\hat{C}$.

References

[1] Lucian Bădescu. *Algebraic surfaces*. Universitext. Springer-Verlag, New York, 2001. Translated from the 1981 Romanian original by Vladimir Maşek and revised by the author.

[2] Arnaud Beauville. Counting rational curves on $K3$ surfaces. *Duke Math. J.*, 97(1):99–108, 1999.

[3] J. Bertin. Réseaux de Kummer et surfaces $K3$. *Invent. Math.*, 93(2):267–284, 1988.

[4] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. *SIAM J. Comput.*, 32(3):586–615, 2003.

[5] Egbert Brieskorn and Horst Knörrer. *Plane algebraic curves*. Birkhäuser Verlag, Basel, 1986. Translated from the German by John Stillwell.

[6] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[7] Noam D. Elkies. Shimura curve computations via $K3$ surfaces of Néron-Severi rank at least 19. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 196–211. Springer, Berlin, 2008.

[8] Reza Rezaeian Farashahi. Hashing into hessian curves. In *AFRICACRYPT*, pages 278–289, 2011.

[9] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, resultants, and multidimensional determinants*. Mathematics: Theory & Applications. Birkhäuser Boston Inc., Boston, MA, 1994.

[10] J. W. P. Hirschfeld. Codes on curves and their geometry. *Rend. Circ. Mat. Palermo (2) Suppl.*, (51):123–137, 1998.

[11] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres. *Algebraic curves over a finite field*. Princeton Series in Applied Mathematics. Princeton University Press, Princeton, NJ, 2008.

[12] Thomas Icart. How to hash into elliptic curves. In *CRYPTO*, pages 303–316, 2009.

[13] Jean-Gabriel Kammerer, Reynald Lercier, and Guénaël Renault. Encoding points on hyperelliptic curves over finite fields in deterministic polynomial time. In *Pairing*, pages 278–297, 2010.

[14] Neal Koblitz. *Algebraic aspects of cryptography*, volume 3 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 1998. With an appendix by Alfred J. Menezes, Yi-Hong Wu and Robert J. Zuccherato.

[15] Abhinav Kumar. *K3 surfaces of high rank*. ProQuest LLC, Ann Arbor, MI, 2006. Thesis (Ph.D.)–Harvard University.

[16] Junho Lee and Naichung Conan Leung. Yau-Zaslow formula on $K3$ surfaces for non-primitive classes. *Geom. Topol.*, 9:1977–2012 (electronic), 2005.

[17] Michael B. Monagan, Keith O. Geddes, K. Michael Heal, George Labahn, Stefan M. Vorkoetter, James McCarron, and Paul DeMarco. *Maple 10 Programming Guide*. Maplesoft, Waterloo ON, Canada, 2005.

[18] Matthias Schütt and Tetsuji Shioda. Elliptic surfaces. In *Algebraic geometry in East Asia—Seoul 2008*, volume 60 of *Adv. Stud. Pure Math.*, pages 51–160. Math. Soc. Japan, Tokyo, 2010.

[19] J. Rafael Sendra, Franz Winkler, and Sonia Pérez-Díaz. *Rational algebraic curves*, volume 22 of *Algorithms and Computation in Mathematics*. Springer, Berlin, 2008. A computer algebra approach.

[20] Andrew Shallue and Christiaan E. van de Woestijne. Construction of rational points on elliptic curves over finite fields. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 510–524. Springer, Berlin, 2006.

[21] Baosen Wu. The number of rational curves on $K3$ surfaces. *Asian J. Math.*, 11(4):635–650, 2007.

[22] Oscar Zariski. *Algebraic surfaces*. Classics in Mathematics. Springer-Verlag, Berlin, 1995. With appendices by S. S. Abhyankar, J. Lipman and D. Mumford, Preface to the appendices by Mumford, Reprint of the second (1971) edition.