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

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

January 19, 2011

Abstract

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

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 [Bo]. The difficulty is to deterministically find a field element x such that some polynomial in x is a square, see [Ko], 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 [Sh-Wo] proposed a first practical deterministic algorithm. In 2009, Icart [Ic] proposed another deterministic encoding for elliptic curves over a field 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 [Ka-Le-Re] proposed a different parameterization 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 [Fa] found yet another parameterization for such elliptic curves too. The point is that the map $x \mapsto x^3$ is bijective for finite fields with cardinality congruent to 2 modulo 3. So one looks for a parameterization of the cubic by cubic radicals. This is a special case of the problem of finding parameterizations of curves by radicals [Se-Se, Se-Wi-Pr].

It turns out that such parameterizations closely relate to the geometry of the dual curve of the elliptic curve. In a nutshell, the dual $\hat{C}$ of a curve C parameterizes the tangents to C. The tangents

*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".

†INRIA Bordeaux Sud-Ouest, Université de Toulouse le Mirail, Institut de Mathématiques de Bordeaux, CNRS.

‡DGA/MI, BP 7 35998 RENNES ARMEES.

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

at the flex points of C correspond to singular points on $\hat{C}$, namely cusps. From rational curves going through these cusps, we can derive pseudo-parameterizations of C.

In this paper we review the geometry of the nine flex tangents to a smooth plane cubic C, and we explain how this geometry relates to the parameterizations found by Icart, Farashahi, and Kammerer, Lercier, Renault. We will see that these parameterizations correspond to rational curves in a degree two covering of the dual plane ramified along the dual sextic $\hat{C}$ of C. Such rational curves can be constructed using the very special configuration formed by the 9 cusps of $\hat{C}$, which correspond to the nine flexes of C.

In Section 2 we recall notation and derive classical formulae for the solution of equations of degree 3, that will be used in the sequel. Section 3 briefly recalls the elementary properties of the dual of a smooth plane cubic curve. In Section 4 we study the geometry of the nine flex tangents to a smooth plane cubic. We show that the nine points in the dual plane, associated with these nine tangents, are not in generic position with respect to conics and quartics. We explain in the next Section 5 how to use this special configuration of nine points to parameterize the cubic by cubic radicals.

Throughout the paper, we denote by k a field with characteristic different from 2 and 3, by $\bar{k} \supset \bar{k}$ 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 [Wa] 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 [Du-Fo]. 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

$$\rho' = r_0 + \zeta_3 r_1 + \zeta_3^2 r_2$$

and we check that

$$R' = \rho'^3 = s_1^3 + \frac{27}{2}s_3 - \frac{9}{2}s_1 s_2 + \frac{3}{2}\delta.$$

We note that $\rho\rho' = r_0^2 + r_1^2 + r_2^2 - r_0 r_1 - r_1 r_2 - r_2 r_0$ 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:

$$\left\{ \begin{array}{rcl} r_0 + r_1 + r_2 & = & s_1 \\ r_0 + \zeta_3^{-1} r_1 + \zeta_3 r_2 & = & \rho \\ r_0 + \zeta_3 r_1 + \zeta_3^{-1} r_2 & = & \rho' \end{array} \right.$$

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 [Hi-Ko-To] and [Hi].

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 point $[U : V : W]$ in $\hat{\mathbb{P}}$ corresponds to the line with equation $UX + VY + WZ = 0$ in $\mathbb{P}$. Let $C \subset \mathbb{P}$ be a smooth cubic 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. To every point on C one can associate the point in $\hat{\mathbb{P}}$ corresponding to the tangent to C at P. The set of such points is the dual curve $\hat{C}$ of C. So $\hat{C}$ is the image of the so called Gauss morphism

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

The plane curve $\hat{C}$ has degree 6 and ω_C induces a birational equivalence between C and $\hat{C}$. 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

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

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

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

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

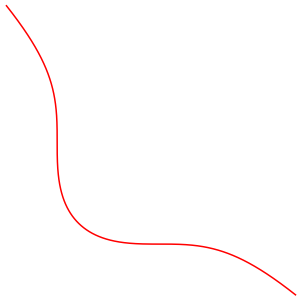

Figure 1: The cubic with equation $X^3 + Y^3 + Z^3 = 0$

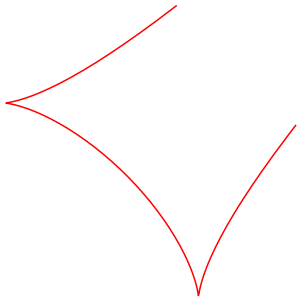

Figure 2: The dual curve with equation $U^6 + V^6 + W^6 - 2U^3V^3 - 2V^3W^3 - 2U^3W^3 = 0$

4 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 *unicursal* curves going through many of these nine cusps of $\hat{C}$. By a *unicursal* curve we mean a curve having geometric genus 0 and a rational point. This is equivalent to the existence of a rational parameterization, see [Se-Wi-Pr], 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 $(0 : -1 : 1)$ 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 cusps and their images by the Gauss map. We set $O = (0 : -1 : 1)$ and $\hat{O} = (a : 1 : 1)$

Flex of C	Cusp on $\hat{C}$
$(0 : -1 : 1)$	$(a : 1 : 1)$
$(-1 : 1 : 0)$	$(1 : 1 : a)$
$(1 : 0 : -1)$	$(1 : a : 1)$
$(-1 : \zeta_3 : 0)$	$(\zeta_3^2 : \zeta_3 : a)$
$(\zeta_3 : 0 : -1)$	$(\zeta_3 : a : \zeta_3^2)$
$(0 : -1 : \zeta_3)$	$(a : \zeta_3^2 : \zeta_3)$
$(\zeta_3 : -1 : 0)$	$(\zeta_3 : \zeta_3^2 : a)$
$(-1 : 0 : \zeta_3)$	$(\zeta_3^2 : a : \zeta_3)$
$(0 : \zeta_3 : -1)$	$(a : \zeta_3 : \zeta_3^2)$

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 points are colinear unless the modular invariant is zero. See the proof of Proposition 1 in Section 7.2 of [Br-Kn]. 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 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 $U^2+\zeta_3V^2+\zeta_3^2W^2+(a+1)(\zeta_3^2UV+\zeta_3UW+VW)=0$ 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 $X+\zeta_3Y+\zeta_3^2Z=0$. The action of $\mathcal{S}_3$ produces one more such conic.

The conic with equation $\zeta_3U^2+V^2+\zeta_3W^2+(a+\zeta_3^2)(UV+\zeta_3^2UW+VW)=0$ 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 $\zeta_3X+Y+\zeta_3Z=0$. 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 unicursal over $k(a)$ because they have an evident $k(a)$ rational point. The last one is unicursal 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 unicursal curves we use these remaining degrees of freedom to impose a big singularity at $\hat{O}=(a:1:1)$. 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 unicursal 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 unicursal 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 quadric 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 $\hat{C}$ is in black and 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 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 unicursal 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.)

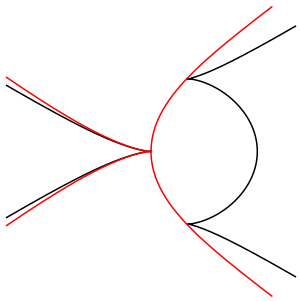

Figure 4: The real part of the intersection of $\hat{C}$ and Q.

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

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

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

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

5 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 $\sqrt[3]{} : k \to k$.

Let $C \subset \mathbb{P}^2$ be a plane projective smooth cubic curve over k. We want to construct k-rational points on C. More precisely, we look for a non-trivial map from k to $C(k)$. Since C has genus 1 it is not unicursal, and the map we are looking for cannot be a morphism of algebraic curves. We try to construct a map from k to $C(k)$ that could be expressed with rational fractions and the cubic root operator $\sqrt[3]{}$. The idea is to look for a one parameter family of lines $(D_t)_t$ in the projective plane such that, for every value of the parameter t, the intersection $D_t \cap C$ has a rational point in it. We observe that this intersection is described by a cubic extension (depending on t). So we ask that the twisted discriminant of this extension be a square for every value of the parameter t. If this is the case, we can construct a root (and the corresponding point in $C \cap D_t$) using the Tartaglia-Cardan formulae given in Section 2 and the cubic root map $\sqrt[3]{} : k \to k$ defined above.

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

$$UX + VY + WZ = 0. \tag{5}$$

The intersection $D.C$ is described by the homogeneous system consisting of Equation (5) and the equation of the cubic C. We can use Equation (5) to eliminate one of the three variables X, Y, Z in the equation of C. We obtain a binary cubic form whose twisted discriminant $\Delta(U, V, W)$ is essentially the equation of the dual curve $\hat{C}$ because it cancels when the intersection $D.C$ has multiplicities. In particular this twisted discriminant is not a square. However, if t is an indeterminate, and if we choose carefully U, V and W to be polynomials $U(t)$, $V(t)$ and $W(t)$ in $k[t]$, then the corresponding rational fraction $\Delta(t)$ might be a square in $k(t)$ or something close to a square. So we look for a unicursal curve $L \subset \hat{\mathbb{P}}$ that intersects the dual curve $\hat{C}$ with lots of even multiplicities. Note that L may be given by its projective equation, or as the image of a parameterization $\lambda : \mathbb{P}^1 \to \hat{\mathbb{P}}$ that maps the point $(t : 1)$ onto $(U(t) : V(t) : W(t))$.

The considerations in Section 4 provide several candidates for L.

5.1 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 unicursal 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 [Fa].

5.2 Intersecting the dual curve with a quartic

Assume now that we take L to be the unicursal 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 (3). The parameterization of Q given in Equation (4) 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 (3). 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 [Ic], up to the change of variable $t \leftarrow -1/t$.

5.3 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 $(a : 1 : 1)$ and $(1 : a : 1)$ 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. This situation is illustrated on Figure 5.

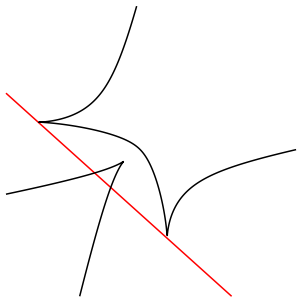

Figure 5: The intersection of $\hat{C}$ and L

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

$$h(i) = i^3 + \frac{3t(a + 2)i}{a^2 + a + 1} + \frac{3t(1 - t)}{a^2 + a + 1} \tag{6}$$

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

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

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

$$(a^2+a+1)S^2 = 9(a^2+a+1)T^2 + 2(2a+1)(a^2+a+7)TK + 9(a^2+a+1)K^2. \quad (8)$$

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

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

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

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

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

$$(3(a^2+a+1) - j)S + (3j - (2a+1)(a^2+a+7)j)T + (3j - 9(a^2+a+1)j)W = 0 \quad (9)$$

where j is a formal parameter.

Intersecting the conic in Equation (8) with the line in Equation (9) we find the parameterization

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

We now substitute t by $T(j)/W(j)$ in Equation (6) and find a cubic polynomial with coefficients in the field $k(a)(j)$. If we substitute t by $T(j)/W(j)$ in Equation (7) we find that $\Delta = \delta^2(j)$ where

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

We use the formulae and notation in Section 2. The polynomial h in Equation (6) 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 [Ka-Le-Re] hides a similar geometric situation.

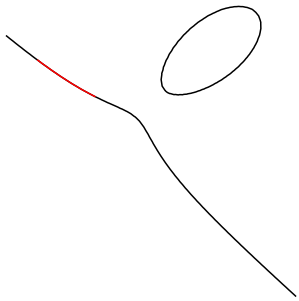

Figure 6: A pseudo parameterization

References

[Bo] D. Boneh and M. K. Franklin. Identity-Based Encryption from the Weil Pairing. *CRYPTO*, 2001.

[Br-Kn] E. Brieskorn and H. Knörrer. Plane algebraic curves. *Birkhäuser Verlag*,1986.

[Du-Fo] D. Dummit and R.M. Foote. Abstract Algebra. *Prentice Hall*, 1991.

[Fa] R. R. Farashahi. Hashing into Hessian Curves. *Cryptology ePrint Archive, Report 2010/373*, 2010.

[Hi] J.W.P. Hirschfeld. Projective geometries over finite fields. *Oxford Mathematical Monographs. The Clarendon Press Oxford University Press*, 1998.

[Hi-Ko-To] J.W.P. Hirschfeld, G. Korchmàros and F. Torres. Algebraic curves over a finite field. *Princeton University Press*, 2008.

[Ic] T. Icart. How to hash into elliptic curves. Proceedings of CRYPTO 2009, pages 303–316. *Lecure Notes in Computer Science, volume 5677. Springer*, 2009.

[Ka-Le-Re] J.-G. Kammerer, R. Lercier, and G. Renault. Encoding points on hyperelliptic curves over finite fields in deterministic polynomial time. International Conference on Pairing-Based Cryptography, 2010.

[Ko] N. Koblitz. Algebraic Aspects of Cryptography. Springer, 1999.

[Sh-Wo] A. Shallue and C. van de Woestijne. Construction of Rational Points on Elliptic Curves over Finite Fields. In Florian Hess, Sebastian Pauli, and Michael E. Pohst, editors, ANTS, pages 510-524. *Lecure Notes in Computer Science, volume 4076. Springer*, 2006.

[Se-Wi-Pr] J. R. Sendra, F. Winkler, and S. Prez-Diaz. Rational Algebraic Curves: A Computer Algebra Approach. *Springer*, 2007.

[Se-Se] R. Sendra and J. Sevilla. Radical Parametrization of Algebraic Curves by Adjoint Curves. ArXiv e-prints 0805.3214, 2008.

[Wa] Waterloo Maple Incorporated. Maple. Waterloo, Ontario, Canada. http://www.maplesoft.com/