The Geometry of flex tangents to a plane cubic and its parameterizations

Jean-Marc Couveignes (with Jean-Gabriel Kammerer)

INRIA Bordeaux Sud-Ouest et Institut de Mathématiques de Bordeaux

ECC 2011

Motivation

Find $P \in C$ with

$$x_P, y_P \in k(t, \sqrt[3]{R(t)}).$$

Examples by Icart, Kammerer, Lercier, Renault, Farashahi.
Encoding into and elliptic curve C over k where $\#k = 2 \bmod 3$.
Interresting topic in itself.
Contents

1. Solving cubic equations,
2. Duality in the projective plane,
3. A general recipe,
4. The geometry of flex tangents to a cubic,
5. Old and new parameterizations,
6. Rational curves on a K3 surface.

Tartaglia, Cardan, Viète, . . .

Let k with $\mathrm{car}(k) \notin \{2,3\}$. Choose $\zeta_3 \in \bar{k}$.

Consider $h(x) = x^3 - s_1x^2 + s_2x - s_3 \in k[x]$ with

$$h(x) = (x - r_0)(x - r_1)(x - r_2) \in \bar{k}[x].$$

Set

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

So

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

Tartaglia, Cardan, Viète, ...

Set $l = k(\zeta_3, \delta) \subset \bar{k}$ and $m = l(r_1, r_2, r_0) \subset \bar{k}$.

Assume $l \subsetneq m$ and apply Kummer theory.

Let $\sigma \in \mathrm{Gal}(m/l)$ with $\sigma(r_i) = r_{i+1}$. Set

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

So $\sigma(\rho) = \zeta_3 \rho$, thus $R = \rho^3$ is invariant by σ. Indeed

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

Similarly

$$\rho' = r_0 + \zeta_3 r_1 + \zeta_3^2 r_2 \text{ and } R' = \rho'^3 = s_1^3 + \frac{27}{2} s_3 - \frac{9}{2} s_1 s_2 + \frac{3}{2} \delta.$$

Bonus $\rho\rho' = r_0^2 + r_1^2 + r_2^2 - r_0 r_1 - r_1 r_2 - r_2 r_0 = s_1^2 - 3 s_2$.

Tartaglia, Cardan, Viète, . . .

Summary :

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

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

$$\rho\rho' = r_0^2 + r_1^2 + r_2^2 - r_0r_1 - r_1r_2 - r_2r_0 = s_1^2 - 3s_2,$$

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

And

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

does not involve ζ_3.

Viète

Algebraic geometrist, cryptographer, politician.
Use of letters as parameters in equations, Cryptanalysis, Algebraic equations.

Duality in the projective plane

Let $E = k^3$ and $\hat{E}$ its dual.
$U = (1,0,0)$, $V = (0,1,0)$, $W = (0,0,1)$, canonical basis of E, and (X, Y, Z) the dual basis.
Set

$$\mathbb{P} = \mathrm{Proj}(E) = \mathrm{Proj}\, k[X, Y, Z]$$

and

$$\hat{\mathbb{P}} = \mathrm{Proj}(\hat{E}) = \mathrm{Proj}\, k[U, V, W].$$

The point $[U : V : W] \in \hat{\mathbb{P}}$ represents the line with equation

$$UX + VY + WZ = 0 \subset \mathbb{P}.$$

Dual of a plane curve

Let $C \subset \mathbb{P}$ with equation $F(X,Y,Z) = 0$.
Set $F_X = \frac{\partial F}{\partial X}$, $F_Y = \frac{\partial F}{\partial Y}$, $F_Z = \frac{\partial F}{\partial Z}$. Tangent at 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

$$[F_X(X_P,Y_P,Z_P) : F_Y(X_P,Y_P,Z_P) : F_Z(X_P,Y_P,Z_P)].$$

Gauss map

$$\omega_C : \quad C \longrightarrow \hat{\mathbb{P}}$$

$$[X:Y:Z] \longmapsto [F_X(X,Y,Z) : F_Y(X,Y,Z) : F_Z(X,Y,Z)]$$

The dual curve $\hat{C} = \omega_C(C)$.

Dual of a cubic

Assume

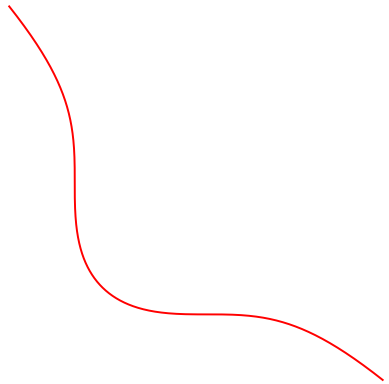
$$F(X,Y,Z) = X^3 + Y^3 + Z^3 - 3aXYZ,$$

then
$F_X = 3X^2 - 3aYZ$, $F_Y = 3Y^2 - 3aXZ$, $F_Z = 3Z^2 - 3aXY$.

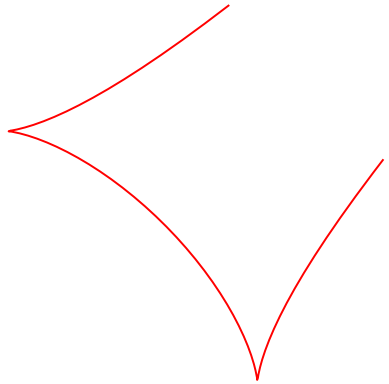
The dual $\hat{C} = \omega_C(C)$ has degree 6, 9 cusps, and equation

$$G(U,V,W) = U^6 + V^6 + W^6 - 6a^2(U^4VW + UV^4W + UVW^4)$$
$$+(4a^3 - 2)(U^3V^3 + U^3W^3 + V^3W^3) + (12a - 3a^4)U^2V^2W^2.$$

An example



The cubic $X^3 + Y^3 + Z^3 = 0$ and the sextic
$U^6 + V^6 + W^6 - 2U^3V^3 - 2V^3W^3 - 2U^3W^3 = 0$.



Pseudo-parameterization of a cubic

Assume $a \mapsto a^3$ is surjective. Let $a \mapsto \sqrt[3]{a}$ a section.
We look for $k \mapsto C(k)$.

General recipe : find a line $D \subset \mathbb{P}$ and compute $D.C$. Hope there is a rational point in this intersection, and we can compute it.

If D has equation $UX + VY + WZ = 0$, the intersection $D.C$ is given by a binary cubic form.

The only obstacle to the existence of a rational point in the intersection is the discriminant $\Delta(U, V, W)$.

This $\Delta(U, V, W)$ is the equation of the dual curve $\hat{C}$.

Pseudo-parameterization of a cubic

Restrict to a well chosen family of lines $(D_t)_t$ with equation

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

This family of lines corresponds to a rational curve $L \subset \hat{\mathbb{P}}$. This is the image in $\hat{\mathbb{P}}$ of

$$\phi : t \mapsto [U(t) : V(t) : W(t)].$$

We ask that the discriminant $\Delta(U(t), V(t), W(t))$ be a square in $k(t)$.

A rough geometric interpretation of this condition is that the unicursal curve L intersect $\hat{C}$ with all even multiplicities.

So we look for a unicursal curve $L \subset \hat{\mathbb{P}}$ having even intersection with $\hat{C}$.

Flexes

$$F(X,Y,Z) = X^3 + Y^3 + Z^3 - 3aXYZ,$$

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

Flexes of C	Cusps of $\hat{C}$
$(0 : -1 : 1)$	$(a : 1 : 1)$
$(-1 : 1 : 0)$	$(1 : 1 : a)$
$(1 : 0 : -1)$	$(1 : a : 1)$
$(-1 : \zeta_3 : 0)$	$(\zeta_3^2 : \zeta_3 : a)$
$(\zeta_3 : 0 : -1)$	$(\zeta_3 : a : \zeta_3^2)$
$(0 : -1 : \zeta_3)$	$(a : \zeta_3^2 : \zeta_3)$
$(\zeta_3 : -1 : 0)$	$(\zeta_3 : \zeta_3^2 : a)$
$(-1 : 0 : \zeta_3)$	$(\zeta_3^2 : a : \zeta_3)$
$(0 : \zeta_3 : -1)$	$(a : \zeta_3 : \zeta_3^2)$

The coconics

Lemma

Let C a plane cubic overt k with $p \notin \{2, 3\}$.
Assume $j \neq 0$. Remove three colinear flex points.
The tangents at the six remaining points are coconic.

The conic $UW - aV^2 = 0$ meets $\hat{C}$ at $(a : 1 : 1)$, $(1 : 1 : a)$, $(\zeta_3^2 : \zeta_3 : a)$, $(a : \zeta_3^2 : \zeta_3)$, $(\zeta_3 : \zeta_3^2 : a)$, $(a : \zeta_3 : \zeta_3^2)$.
$(1 : 0 : -1)$, $(\zeta_3 : 0 : -1)$, $(1 : 0 : \zeta_3)$ lye on $Y = 0$.

$U^2 + V^2 + W^2 + (a+1)(UV + UW + VW) = 0$, and
$X + Y + Z = 0$.
$U^2 + \zeta_3 V^2 + \zeta_3^2 W^2 + (a+1)(\zeta_3^2 UV + \zeta_3 UW + VW) = 0$ and
$X + \zeta_3 Y + \zeta_3^2 Z = 0$.
$\zeta_3 U^2 + V^2 + \zeta_3 W^2 + (a+\zeta_3^2)(UV + \zeta_3^2 UW + VW) = 0$ and
$\zeta_3 X + Y + \zeta_3 Z = 0$.

The coconics again

Let C the Hessian cubic with $a^3 \neq 1$. Let L the conic $UW - aV^2 = 0$. Let $U(t) = 1$, $V(t) = -t$, $W(t) = at^2$ a parameterization. The line D_t is $X - tY + at^2Z = 0$. Replacing X by $tY - at^2Z$ in the equation of C we find

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

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

$$s_1 = 3at,\ s_2 = 3a^2t^2,\ s_3 = \frac{a^3t^6-1}{t^3+1},$$

$$\delta = \frac{9(1+a^3t^3)}{1+t^3},\ R = -27\frac{a^3t^3+1}{t^3+1},\ R' = 0,$$

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

A nice quartic

Lemma

C a smooth plane cubic over k with $p \notin \{2,3\}$. Assume $j \neq 0$. Let $\hat{O}$ a cusp on $\hat{C}$. There is a unic quartic Q that cuts $\hat{C}$ at $\hat{O}$ with multiplicity 8 and the 8 remaining cusps with multiplicity 2.

$U^4+a(V^4+W^4)-2a(U^3V+U^3W+V^3W+VW^3)-(a^3+1)U(V^3+W^3)+3a^2U^2(V^2+W^2)+(a^4+2a)V^2W^2+(1-a^3)UVW(V+W)=0.$

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

$G(U(t),V(t),W(t))=$
$t^6(t+1)^2(t^2-t+1)^2(at-2)^2((a+1)t-1)^2((a^2-a+1)t^2+(1-2a)t+1)^2(a^2t^2+1-at)^2.$

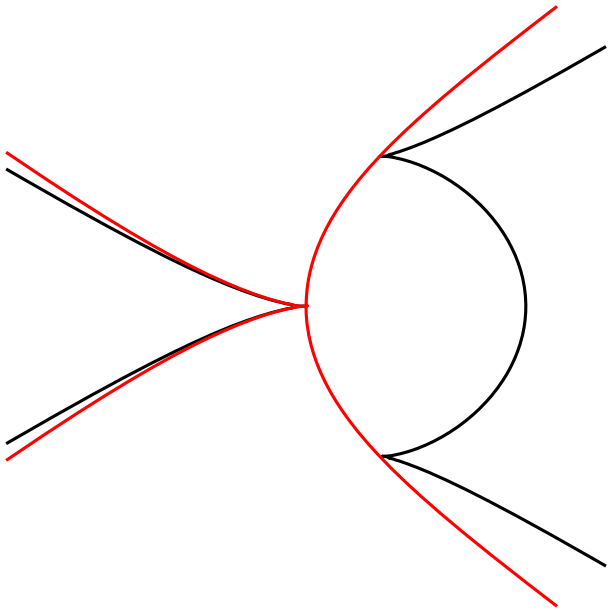
Weierstrass cubic

C the cubic $F(X,Y,Z) = Y^2Z - X^3 - aXZ^2 - bZ^3$, with $a \neq 0$, $O = (0:1:0)$ and $\hat{O} = (0:0:1)$.
Then Q is

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

and

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



The quartic again

Let C the Weierstrass cubic. Let L the quartic Q. The line D_t is

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

Set $x = X/Z$, $y = Y/Z$ and substitute y by $1/(6t^3) - at/2 - x/t$ in the Weierstrass equation. We find $x^3 - s_1x^2 + s_2x - s_3$ with

$$\begin{aligned}
s_1 &= 1/t^2,\ s_2 = 1/(3t^4),\\
s_3 &= (1/t^6 - 6a/t^2 - 36b + 9a^2t^2)/36,\\
\delta &= (-1/t^6 - 108b - 18a/t^2 + 27a^2t^2)/12,\\
R = 0,\ R' &= (-1/t^6 - 108b - 18a/t^2 + 27a^2t^2)/4,\\
x &= \frac{1}{3t^2} + \sqrt[3]{\frac{a^2t^2}{4} - \frac{1}{108t^6} - b - \frac{a}{6t^2}},\\
y &= Y/Z = \frac{1}{6t^3} - at/2 - x/t.
\end{aligned}$$

Rational curves on a surface

We have constructed solutions (u, v, h) to

$$h^2 = G(u, v, 1), \tag{2}$$

where $u = U(t)/W(t)$, $v = V(t)/W(t)$, $h = \delta(t)/W^3(t)$ in $k(t)$.
We call S the minimal model of the surface in Equation (2). This is a K3 surface. We are looking for rational curves on it.
The Néron-Severi group $\mathrm{NS}(S)$ classifies divisors on S up to algebraic (linear) equivalence. It is a free $\mathbb{Z}$-module. Its rank is ≤ 22. There is a quadratic (intersection) form.
Over $\mathbb{Z}[1/6, a]$ this rank is 19. Amenable rational curves lye on classes with self intersection -2.

Relations in $\mathrm{NS}(S)$

A basis of $\mathrm{NS}(S) \otimes \mathbb{Q}$ consists of the 18 exceptional components E_i and F_i for $1 \leq i \leq 9$ plus the pullback H of a line by $S \to \mathbb{P}$.
The coordinates of the nice conics

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

The coordinates of the nice quadrics

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

The set of classes with self intersection -2 is not a group ...

Elliptic fibrations

We can (in infinitely many different ways) provide S with the structure of an elliptic fibrations

$$\phi : S \to \mathbb{P}^1.$$

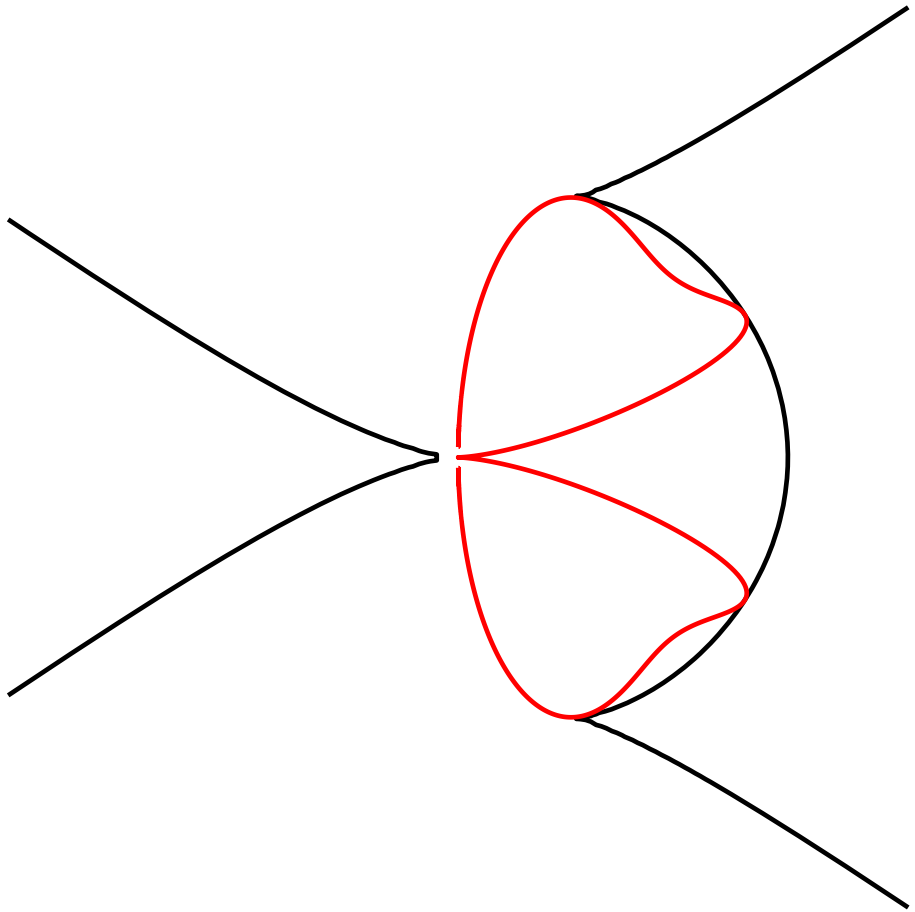
Every section of ϕ is a rational curve with self-intersection -2.
These sections form a group.
Missing part (trivial lattice) : components of singular fibers.
There are infinitely many (inequivalent) parameterizations corresponding to rational curves on S.

Another example

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

$$\begin{aligned} U(t) &= 4at^6 + 4t^2/27, \\ V(t) &= t(4at^6 + 4t^2/27), \\ W(t) &= a^2t^8 + 2at^4/27 + 4bt^6 + 1/81. \end{aligned} \tag{3}$$

Another example



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