The geometry of some parameterizations and encodings

Jean-Marc Couveignes (with Reynald Lercier)

INRIA Bordeaux Sud-Ouest et Institut de Mathématiques de Bordeaux

CIAO 2020, Bordeaux

Parameterizations by radicals

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 $\#K = 2 \bmod 3$.
Contents

1. Radical morphisms,
2. Torsors,
3. A general recipe,
4. Genus one curves,
5. Genus two curves,
6. Variations,
7. Genus curves with 5-torsion and beyond.

Radicals

Lemma

K a field, $d \geq 1$, and $a \in K^*$. The polynomial $x^d - a$ is irreducible iff

- *For every prime l dividing d, a is not the l-th power in K^*,*
- *If 4 divides d, then $-4a$ is not a 4-th power in K^*.*

For $S \subset \mathbb{P}$ a field extension L/K is said *S-radical* if

$$L \simeq K[x]/(x^d - a)$$

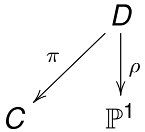
for $d \in S$ and $a \in K^*$ not a d-th power.
L/K is *S-multiradical* if

$$K = K_0 \subset K_1 \subset \cdots \subset K_n = L$$

with each K_{i+1}/K_i an S-radical extension.

Radical morphisms

$f : C \to D$ an epimorphism of (projective, smooth, absolutely integral) curves over K is said to be a *radical morphism* if $K(D) \subset K(C)$ is radical.
Define similarly multiradical morphisms, S-radical morphisms, S-multiradical morphisms.
An *S-parameterization* is



with ρ an S-multiradical map and π an epimorphism.
In this situation one says that C/K is *parameterizable* by S-radicals.

Torsors

Let $\Gamma = \mathrm{Gal}(\bar{K}/K)$ and A a finite set acted on by Γ. Then A is a finite Γ-set. Define

$$\mathrm{Alg}(A) = \mathrm{Hom}_\Gamma(A, \bar{K}).$$

A finite Γ-group is a finite Γ-set G with a group structure compatible with the Γ-action.
If A is a Γ-set acted on by simply transitively by a finite Γ-group G, and if the action of G on A is compatible with the actions of Γ on G and A, then A is a G-torsor.
Torsors are classified by $H^1(\Gamma, G)$.
A finite Γ-group G is said to be *S-resoluble* if there exists

$$1 = G_0 \subset G_1 \subset \cdots \subset G_i \subset \cdots \subset G_l = G$$

with $G_{i+1}/G_i \simeq \mu_{p_i}$ for some $p_i \in S$.

Radical maps

K a finite field with characteristic p and cardinality q. S a set of prime integers. Assume $p \notin S$ and $S \cap \mathsf{Supp}(q-1) = \emptyset$. $f : C \to D$ a radical morphism of degree $d \in S$. $X \subset C$ the ramification locus let $Y = f(X) \subset D$ the branch locus. Induced map on K-points $F : C(K) \to D(K)$ is a bijection.

Proof : A branched point Q in $D(K)$ is totally ramified, so has a unique preimage P in $C(K)$. For a non-branched point $Q \in D(K) - Y(K)$ the fiber $f^{(-1)}(Q)$ is a μ_d-torsor. Since $H^1(K, \mu_d) = K^*/(K^*)^d = 0$ this torsor is μ_d. Since $H^0(K, \mu_d) = \mu_d(K) = \{1\}$ there is a unique K-rational point in $f^{(-1)}(Q)$. $\square$

The reciprocal map $F^{(-1)} : D(K) \to C(K)$ can be evaluated in deterministic polynomial time.

Encodings

K a finite field with characteristic p and cardinality q. S a set of prime integers. Assume $p \notin S$ and $S \cap \mathrm{Supp}(q-1) = \emptyset$. An S-parameterization

$$\begin{array}{ccc} & & D \\ & \swarrow^{\pi} & \downarrow \rho \\ C & & \mathbb{P}^1 \end{array}$$

induces $R : D(K) \to \mathbb{P}^1(K)$ and $\Pi : D(K) \to C(K)$.
The composition $\Pi \circ R^{(-1)}$ is called an *encoding*.

Tartaglia-Cardan formulae

K a field with characteristic prime to 6, $\Gamma = \mathrm{Gal}(\bar{K}/K)$.
$\mathrm{Sym}(\mu_3)$ is a acted on by Γ. And $\mu_3 \subset \mathrm{Sym}(\mu_3)$ is normal.
$\mathrm{Stab}(1) \simeq \mu_2$. So $\mathrm{Sym}(\mu_3) \simeq \mu_3 \rtimes \mu_2$.
Let $\zeta_3 \in \bar{K}$ a primitive third root of unity and set $\sqrt{-3} = 2\zeta_3 + 1$.
Take $h(x) = x^3 - s_1 x^2 + s_2 x - s_3$ separable. Set

$$R = \mathrm{Roots}(h) \subset \bar{K}$$

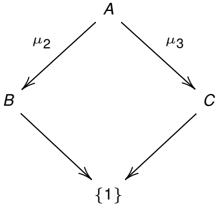
and

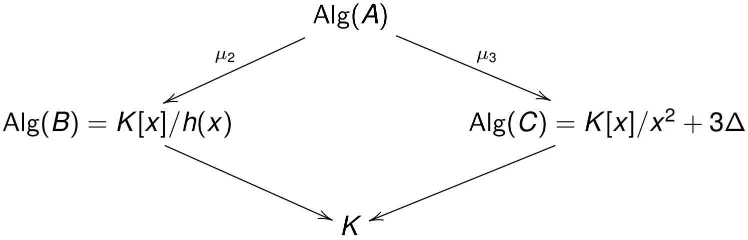
$$A = \mathrm{Bij}(\mathrm{Roots}(h), \mu_3).$$

For $\gamma \in \Gamma$ and $f \in A$ set ${}^{\gamma}f = \gamma \circ f \circ \gamma^{-1}$.
Action of $\mathrm{Sym}(\mu_3)$ on the left.

Tartaglia-Cardan formulae

$A = \mathrm{Bij}(\mathrm{Roots}(h), \mu_3)$ a $\mathrm{Sym}(\mu_3)$-torsor. The quotient $C = A/\mu_3$ is a μ_2-torsor. The quotient $B = A/\mu_2$ is a Γ-set.





Tartaglia-Cardan formulae

$A = \mathrm{Bij}(\mathrm{Roots}(h), \mu_3)$ a $\mathrm{Sym}(\mu_3)$-torsor. The quotient $C = A/\mu_3$ is a μ_2-torsor. The quotient $B = A/\mu_2$ is a Γ-set.
A function ξ in $\mathrm{Alg}(B) \subset \mathrm{Alg}(A)$ is

$$\xi : \quad B \longrightarrow \bar{K}$$

$$f \longmapsto f^{(-1)}(1).$$

The algebra $\mathrm{Alg}(B)$ is generated by ξ, and the characteristic polynomial of ξ is $h(x)$. So

$$\mathrm{Alg}(B) \simeq K[x]/h(x).$$

Tartaglia-Cardan formulae

Tartaglia-Cardan formulae construct functions in $\mathrm{Alg}(A)$.
These functions can be constructed with radicals because $\mathrm{Sym}(\mu_3) = \mu_3 \rtimes \mu_2$ is resoluble.
Define first $\delta \in \mathrm{Alg}(C) \subset \mathrm{Alg}(A)$ by

$$\delta : \quad A \longrightarrow \bar{K}$$

$$f \longmapsto \sqrt{-3}\big(f^{(-1)}(\zeta) - f^{(-1)}(1)\big)\big(f^{(-1)}(\zeta^2) - f^{(-1)}(\zeta)\big)\big(f^{(-1)}(1) - f^{(-1)}(\zeta^2)\big).$$

Note $\sqrt{-3}$ balances the Galois action on μ_3. The algebra $\mathrm{Alg}(C)$ is generated by δ and

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

is the *twisted discriminant*.

Tartaglia-Cardan's formulae

Define $\rho \in \mathrm{Alg}(A)$ as

$$\rho : \quad A \longrightarrow \bar{K}$$

$$f \longrightarrow \sum_{r \in R} r \times f(r) = \sum_{\zeta \in \mu_3} \zeta \times f^{(-1)}(\zeta).$$

ρ^3 is invariant by $\mu_3 \subset \mathrm{Sym}(\mu_3)$ so $\rho^3 \in \mathrm{Alg}(C)$. Indeed

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

A variant of ρ is

$$\rho' : \quad A \longrightarrow \bar{K}$$

$$f \longrightarrow \sum_{r \in R} r^{-1} \times f(r).$$

Tartaglia-Cardan's formulae

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

and

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

Further

$$\rho\rho' = s_1^2 - 3s_2.$$

The root ξ of $h(x)$ can be expressed in terms of ρ and ρ' as

$$\xi = \frac{s_1 + \rho + \rho'}{3}.$$

Tartaglia-Cardan's formulae

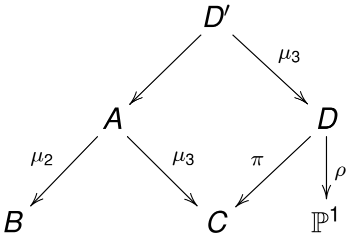
$\mathrm{Alg}(A)$ is not the Galois closure of $K[x]/h(x)$.

Galois closure associated with the $\mathrm{Sym}(\{1,2,3\})$-torsor $\mathrm{Bij}(R,\{1,2,3\})$. Not resoluble.

However $\mathrm{Alg}(A) \supset \mathrm{Alg}(B) \simeq K[x]/h(x)$ because the quotient of $\mathrm{Bij}(\mathrm{Roots}(h),\mu_3)$ by $\mathrm{Stab}(1) \subset \mathrm{Sym}(\mu_3)$ is isomorphic to the quotient of $\mathrm{Bij}(R,\{1,2,3\})$ by $\mathrm{Stab}(1) \in \mathrm{Sym}(\{1,2,3\})$.

Note that the quotient of $\mathrm{Bij}(R,\{1,2,3\})$ by $(123) \in \mathrm{Sym}(\{1,2,3\})$ is associated with $K[x]/(x^2-\Delta)$ while the quotient of $\mathrm{Bij}(R,\mu_3)$ by $(1\zeta\zeta^2) \in \mathrm{Sym}(\mu_3)$ is associated with $K[x]/(x^2+3\Delta)$.

Curves with a $\mu_3 \rtimes \mu_2$ action

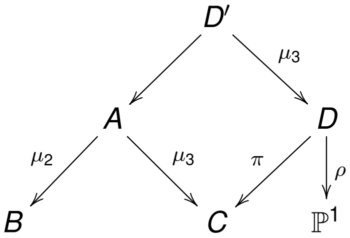


Set $S' = S \cup \{3\}$ and $\rho' : D' \xrightarrow{\mu_3} D \xrightarrow{\rho} \mathbb{P}^1$, and π' the composite map

$$\pi' : D' \longrightarrow A \xrightarrow{\mu_2} B.$$

Then (D', ρ', π') is an S'-parameterization of B. Say that C is the *resolvent* of B.

Curves with a $\mu_3 \rtimes \mu_2$ action

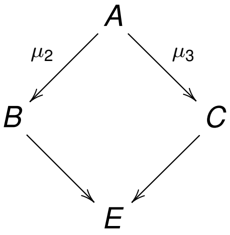


D' isabsolutely integral:

1. When $C = \mathbb{P}^1$ and π and ρ are trivial.
2. When the μ_3-quotient $A \to C$ is branched at some P of C, and π is not. When C has genus 1 we may compose π with a translation to ensure that it is not branched at P.
3. When the degree of π is prime to 3. The resulting parameterization π' has degree prime to 3 also. We can iterate in that case.

Selecting curves

Find curve A with a $\mu_3 \rtimes \mu_2$ action. Set $E = A/(\mu_3 \rtimes \mu_2)$.



We know how to parameterize C. We want to parameterize B.
Take $E = \mathbb{P}^1$ (more generic).
r the number of branched points of $B \to E$, r_s the number of simple branched points, r_t the number of fully branched points.

Selecting curves

$$g_B = \frac{r_s}{2} + r_t - 2, \text{ and } g_A = \frac{3r_s}{2} + 2r_t - 5, \quad \text{and} \quad g_C = \frac{r_s}{2} - 1.$$

Call

$$m = r - 3 = r_s + r_t - 3$$

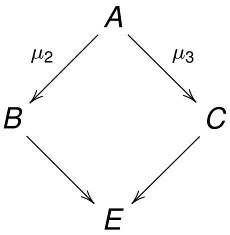
and call it the *modular dimension*. *Genericity condition*

$$r_s + 4r_t \leq 12 - 2\epsilon(\frac{r_s}{2} + r_t - 2),$$

where $\epsilon(0) = 3$, $\epsilon(1) = 1$, and $\epsilon(n) = 0$ for $n \geq 2$.

1. Set $g_C = 0$. So $r_s = 2$, $g_B = r_t - 1$ and the genericity condition reads $r_t \leq 2$. Only $r_t = 2$ is of interest. Farashahi and Kammerer, Lercier, Renault.
2. Set $g_C = 1$. So $r_s = 4$ and $g_B = r_t$. The genericity assumption reads $r_t \leq 2$. The case $r_t = 2$ provides encodings for genus 2 curves.

$r_s = r_t = 2$



$g_C = 0$, $g_B = 1$, $g_A = 2$, and $B \to \mathbb{P}^1$ has degree 3 with two fully branched points and two simply branched points.
Call P_0 and P_∞ the two fully ramified points. Assume $P_0, P_\infty \in B(K)$. The difference $P_0 - P_\infty$ is in $J_B[3]$.

Genus 1 curve with 3-torsion

Genus 1 curve B/K and two points P_0, P_∞ in $B(K)$ s. t. $P_\infty - P_0$ has order 3. $z \in K(B)$ with divisor $3(P_0 - P_\infty)$.
$\sigma : B \to B$ involution sending P_0 onto P_∞.
There exists $a_{0,0} \in K^*$ s. t. $\sigma(z) \times z = a_{0,0}$.
x a degree 2 function, invariant by σ, with $(x)_\infty = P_0 + P_\infty$.
The sum $z + \sigma(z)$ belongs to $K(x)$. As a function on $\mathbb{P}^1$ it has a single pole of multiplicity 3 at $x = \infty$.

$$z + \frac{a_{0,0}}{z} = x^3 + a_{1,1}x + a_{0,1}.$$

The image of $x \times z : B \to \mathbb{P}^1 \times \mathbb{P}^1$ has equation

$$Z_0 Z_1 \left(X_1^3 + a_{1,1} X_1 X_0^2 + a_{0,1} X_0^3 \right) = X_0^3 \left(Z_1^2 + a_{0,0} Z_0^2 \right).$$

Genus 1 curve with 3-torsion

$$Z_0 Z_1 \left(X_1^3 + a_{1,1} X_1 X_0^2 + a_{0,1} X_0^3 \right) = X_0^3 \left(Z_1^2 + a_{0,0} Z_0^2 \right).$$

$B^\star \subset \mathbb{P}^1 \times \mathbb{P}^1$ with arithmetic genus 2. Call $S = (j, k)$ the singular point. We find

$$a_{0,0} = k^2, \; a_{1,1} = -3j^2, \; a_{0,1} = 2k + 2j^3.$$

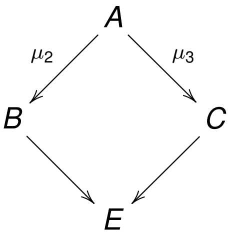
$$z^2 + k^2 = z \left(x^3 - 3j^2 x + 2(k + j^3) \right). \qquad (1)$$

This is a degree 3 equation in x with twisted discriminant $81(1 - k/z)^2$ times

$$h(z) = z^2 - (2k + 4j^3)z + k^2.$$

The resolvent C has equation $t^2 = h(z)$ and genus 0. We can parameterize B with cubic radicals.

$r_s = 4$ and $r_t = 2$



$g_C = 1$, $g_B = 2$, $g_A = 5$, and $B \to \mathbb{P}^1$ has degree 3 with two fully branched points and four simply branched points.
Call P_0 and P_∞ the two fully ramified points. Assume $P_0, P_\infty \in B(K)$. The difference $P_0 - P_\infty$ is in $J_B[3]$.

Genus 2 curve with 3-torsion

Genus 2 curve B/K and P_0, P_∞ in $B(K)$ with $P_\infty - P_0$ of order 3. Assume $\sigma(P_0) \neq P_\infty$.
x a degree 2 function with a zero at P_0 and a pole at P_∞.
z with divisor $3(P_0 - P_\infty)$.
Image of $x \times z : B \to \mathbb{P}^1 \times \mathbb{P}^1$ has equation

$$\sum_{\substack{0\leqslant i\leqslant 3\\ 0\leqslant j\leqslant 2}} a_{i,j} X_1^i X_0^{3-i} Z_1^j Z_0^{2-j} = 0.$$

z is ∞ at a single point, and x has a pole at this point. So if we set $Z_0 = 0$ we find a multiple of $Z_1^2 X_0^3$. We deduce that

$$a_{3,2} = a_{2,2} = a_{1,2} = 0, a_{0,2} \neq 0.$$

Similarly

$$a_{2,0} = a_{1,0} = a_{0,0} = 0, a_{3,0} \neq 0.$$

Genus 2 curve with 3-torsion

Plane affine model

$$(a_{3,0}+a_{3,1}z)x^3+(a_{1,1}+a_{2,1}x)zx+(a_{0,1}+a_{0,2}z)z=0.$$

Degree 3 equation in x with twisted discriminant $z^2(a_{3,0}+a_{3,1}z)^{-4}$ times

$$\begin{aligned}
h(z) \quad = \quad & (9a_{0,2}a_{3,1})^2z^4+(12a_{0,2}a_{2,1}^3+162a3,0a_{0,2}^2a_{3,1}-54a_{1,1}a_{2,1}a_{0,2}a_{3,1}+162a_{0,1}a_{3,1}^2a_{0,2})z^3\\
+ \quad & (81a_{3,0}^2a_{0,2}^2+12a_{0,1}a_{2,1}^3-54a_{1,1}a_{2,1}a_{0,1}a_{3,1}+324a_{3,0}a_{0,1}a_{0,2}a_{3,1}-3a_{1,1}^2a_{2,1}^2\\
& -54a_{3,0}a_{1,1}a_{2,1}a_{0,2}+81a_{0,1}^2a_{3,1}^2+12a_{3,1}a_{1,1}^3)z^2\\
+ \quad & (12a_{1,1}^3a_{3,0}-54a_{3,0}a_{1,1}a_{2,1}a_{0,1}+162a_{3,0}^2a_{0,1}a_{0,2}+162a_{3,0}a_{0,1}^2a_{3,1})z+(9a_{3,0}a_{0,1})^2.
\end{aligned}$$

We can parameterize B with cubic radicals. We first parameterize the elliptic curve with equation $t^2=h(z)$. We deduce a parameterization of B applying Tartaglia-Cardan formulae to the cubic equation.

Genus 2 curve with 3-torsion

Degree 2 in z

$$a_{0,2}z^2 + (a_{3,1}x^3 + a_{2,1}x^2 + a_{1,1}x + a_{0,1})z + a_{3,0}x^3 = 0.$$

Discriminant

$$\Delta(x) = (a_{3,1}x^3 + a_{2,1}x^2 + a_{1,1}x + a_{0,1})^2 - 4a_{0,2}a_{3,0}x^3.$$

A Weierstrass model for B is then $u^2 = \Delta(x)$.
Conversely, from $u^2 = m_6(x)$, write $m(x)$ as a difference $m_3(x)^2 - m_2(x)^3$. Send the roots of m_2 to 0 and ∞.
Succeeds for every genus two curve having a rational 3-torsion point in its jacobian that splits e.g. can be represented as a difference between two rational points on B.

Example

K the field with 83 elements. B curve $y^2 = f(x)$ with

$$f(x) = x^6 + 39x^5 + 64x^4 + 7x^3 + x^2 + 19x + 36.$$

Write $f(x) = b^2 - a^3$ with $b(x) = 68x^3 + 53x^2 + 37x + 76$ and $a(x) = 53x^2 + 29x + 54 = 53(x - 10)(x - 38)$.
Change of variable $x \leftarrow (10x + 38)/(x + 1)$ turns f into

$$(42x^3 + 43x^2 + 45x + 25)^2 - 77x^3.$$

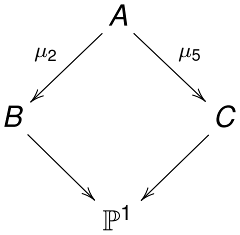
$$a_{3,1} = 42, a_{2,1} = 43, a_{1,1} = 45, a_{0,1} = 25, a_{0,2} = 40, a_{3,0} = 1.$$

The resolvent is elliptic curve

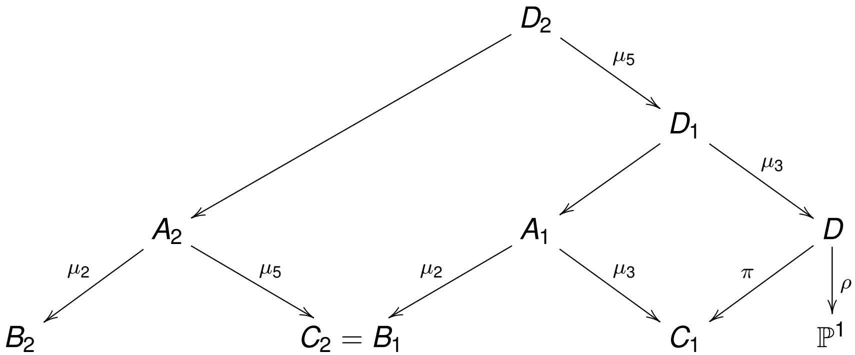
$$t^2 = h(z) = 30z^4 + 50z^3 + 44z^2 + 46z + 78.$$

Curves with a $\mu_5 \rtimes \mu_2$ action

C a genus two curve with $P_\infty - P_0$ of order 5 in J_C.
$A \to C$ associated unramified μ_5-cover.
The involution σ lifts to A. Set $B = A/\sigma$. Then $g_B = 2$.
The corresponding moduli space is rational.



Composing parameterizations



Other families of covers

1. $\mu_3 \rtimes \mu_2$ with $(r_s, r_t) = (6, 1)$
   B and C have genus 2. The map $B \to E$ is any degree 3 map with a triple pole. One for every non-Weierstrass point P on B. Family of parameterizations of B by genus two curves C_P, non-isotrivial. However, $J_{C_P}[3] \simeq J_B[3]$.
2. $\mu_3 \rtimes \mu_2$ with $(r_s, r_t) = (8, 1)$
   B and C have genus 3. The map $B \to E$ has degree 3 and a triple pole P, a Weierstrass point. C is hyperelliptic. Every genus 3 curve B with a Weierstrass point is parameterized by a genus 3 hyperelliptic curve.