The geometry of some parameterizations and encodings

Jean-Marc Couveignes, Reynald Lercier

THE GEOMETRY OF SOME PARAMETERIZATIONS AND ENCODINGS

JEAN-MARC COUVEIGNES AND REYNALD LERCIER

ABSTRACT. We explore parameterizations by radicals of low genera algebraic curves. We prove that for q a prime power that is large enough and prime to 6, a fixed positive proportion of all genus 2 curves over the field with q elements can be parameterized by 3-radicals. This results in the existence of a deterministic encoding into these curves when q is congruent to 2 modulo 3. We extend this construction to parameterizations by ℓ-radicals for small odd integers ℓ, and make it explicit for $\ell = 5$.

1. INTRODUCTION

Let $\mathbb{F}_q$ be a finite field, let $C/\mathbb{F}_q$ be an algebraic curve, we propose in this paper new algorithms for computing in deterministic polynomial time a point in $C(\mathbb{F}_q)$. This is usefull in numerous situations, for instance in discrete logarithm cryptography [2]. To be more precise, we consider this question for low genus curves with an emphasis on the genus 2 case.

The mathematical underlying problem is to compute radical expressions for solutions of a system of algebraic equations. Galois theory provides nice answers, both in theory and practice, for sets of dimension 0 and degree less than 5. Explicit results are known in dimension 1 too. A famous theorem of Zariski states that a generic curve of genus at least 7 cannot be parameterized by radicals. Conversely, a complex curve of genus less than 7 can be parameterized by radicals over the field of rational fractions [10, 9].

In this work we restrict the degree of radicals involved in the parameterizations. Typically, for C a curve over the field with q elements, we only allow radicals of degrees l prime to $q(q-1)$. The reason is that for such l, we can compute l-th roots of elements in $\mathbb{F}_q$ in deterministic polynomial time in $\log(q)$. Especially, for odd q, we do not allow square roots. We will be mainly concerned with genus 2 curves.

Shallue and Woestijne came in 2006 to a first practical deterministic algorithm for constructing points on genus 1 curves over any finite field [18]. In 2009, Icart proposed a deterministic encoding with quasi-quadratic complexity in $\log q$ for elliptic curves over a finite field when q is congruent to 2 modulo 3 [11]. To this end, he constructed a parameterization by 3-radicals for every elliptic curve over a field with characteristic prime to 6. Couveignes and Kammerer recently proved that there exists an infinity of such parameterizations [5], corresponding to rational curves on a K3 surface associated with the elliptic curve.

Nevertheless, in genus 2, only partial results are known. Ulas attempted to generalize Shallue and Woestijne results [20]. Tibouchi and Fouque designed encodings for curves with automorphism group containing the dihedral group with 8 elements [8]. Each of these two constructions reaches a family of dimension 1 inside the dimension 3 moduli space of the genus 2 curves. So the proportion of target curves for such parameterizations tends to zero when q tends to infinity. At the same time,

Date: February 16, 2021.

Research supported by the "Direction Générale de l'Armement" and by the French National Research Agency (ANR) through the project PEACE (ANR-12-BS01-0010-01) and the Investments for the future Programme IdEx Bordeaux (ANR-10-IDEX-03-02).

Kammerer, Lercier and Renault [13] published encodings for a dimension 2 family of genus 2 curves. In particular their curves have no non-hyperelliptic involution. However these curves still represent a negligible proportion of all genus 2 curves when q tends to infinity.

In this paper we construct a parameterization by 3-radicals for a genus 2 curve C over a field K with characteristic p prime to 6 under the unique restriction that C has two K-rational points whose difference has order 3 in the Jacobian variety. This is a dimension 3 family. In particular, we parameterize all genus 2 curves when K is algebraically closed. When K is a finite field with characteristic prime to 6 we parameterize this way a positive proportion of all curves.

Our construction extends the ones by Farashahi [7] for genus 1 curves and Kammerer, Lercier and Renault [13] for genus 2 curves. Our starting point is the observation that the role played by Tartaglia-Cardan formulae in these parameterizations can be formalized and generalized using the theory of torsors under resoluble finite group schemes. This leads us to a systematic exploration and combination of possibilities offered by the action of small resoluble group schemes over curves of low genus.

The principles of our method are presented in Section 2. We first recall the basics of parameterizations of curves by radicals and encodings, then we explain how to produce such parameterizations using the action of resoluble group schemes on algebraic curves. Section 3 provides a first illustration of this general method in the case of genus 1 curves. This offers a new insight on previous work by Farashahi, and Kammerer, Lercier, Renault. We present a parameterization of a large (3-dimensional) family of genus 2 curves in Section 4. Variations on this theme are presented in Section 5. Section 6 presents detailed computations for one of these families. We parameterize Jacobians of dimension 2 with one 5-torsion point. We finish with a few questions and prospects.

We thank Jean Gillibert, Qinq Liu, and Jilong Tong for useful discussions.

2. Definitions and generalities

In this section we recall a few definitions an present the principles of our method. Sections 2.1 and 2.2 recall elementary results about radicals. Section 2.3 recalls the definition of a parameterization. Section 2.4 gives elementary definitions about torsors. Basic properties of encodings are recalled in Section 2.5. Section 2.6 presents Tartaglia-Cardan formulae in the natural language of torsors. Our strategy for finding new parameterizations is presented in Sections 2.7 and 2.8.

2.1. Radical extensions.

The following classical lemma [14, Chapter VI, Theorem 9.1] gives necessary and sufficient conditions for a binomial to be irreducible.

Lemma 1. *Let K be a field, let $d \geq 1$ be a positive integer, and let $a \in K^*$. The polynomial $x^d - a$ is irreducible in $K[x]$ if and only if the two following conditions hold true*

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

Let K be a field with characteristic p. Let S be a set of rational primes such that $p \notin S$. Let $M \supset K$ be a finite separable K-algebra, and $L \subset M$ a K-subalgebra of M. The extension $L \subset M$ is said to be *S-radical* if M is isomorphic, as an L-algebra, to $L[x]/(x^l - a)$ for some $l \in S$ and some $a \in L^*$. When S contains all primes but p, we speak of *radical extensions*.

An extension $M \supset L$ is said to be *S-multiradical* if their exists a finite sequence of K-algebras

$$K \subset L = L_0 \subset L_1 \subset \cdots \subset L_n = M$$

such that every intermediate extension L_{i+1}/L_i for $0 \leq i \leq n-1$ is S-radical.

2.2. **Radical morphisms.** Let K be a field with characteristic p. Let $\bar{K} \supset K$ be an algebraic closure.

Let $f : C \to D$ an epimorphism of (projective, smooth, absolutely integral) curves over K. We say that f is a *radical morphism* if the associated function field extension $K(D) \subset K(C)$ is radical. We define similarly multiradical morphisms, S-radical morphisms, S-multiradical morphisms. If f is a radical morphism then $K(C) = K(D, b)$ where $b^l = a$ and a is a non-constant function on D and $l \neq p$ is a prime integer. Call γ_b the map

$$\begin{aligned} \gamma_b : \qquad & C \longrightarrow D \times \mathbb{P}^1 \\ & P \longmapsto (f(P), b(P)). \end{aligned}$$

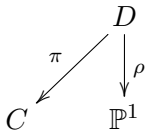
Let $X \subset C$ be the ramification locus of f, and let $Y = f(X) \subset D$ be the branch locus. A geometric point Q on D is branched if and only if a has a zero or a pole at Q with multiplicity prime to l. We ask if γ_b induces an injection on $C(\bar{K})$. Equivalently we ask if b separates points in every fiber of f. First, there is a unique ramification point above each branched point. Then, if a has neither a zero nor a pole at Q, then b separates the points in the fiber of f above Q. Finally, if a has a zero or a pole at Q with multiplicity divisible by l, then b (and γ_b) fail to separate the points in the fiber of f above Q. However, there exists a finite covering $(U_i)_i$ of C by affine open subsets, and functions $b_i \in \mathcal{O}(U_i - X)^*$ such that $b_i/b \in K(D)^* \subset K(C)^*$. We set $\mathbf{b} = (b_i)_{1 \leq i \leq I}$ and define a map

$$\begin{aligned} \gamma_{\mathbf{b}} : \qquad & C \longrightarrow D \times \left(\mathbb{P}^1\right)^I \\ & P \longmapsto (f(P), b_1(P), \ldots, b_I(P)). \end{aligned}$$

This map induces an injection on $C(\bar{K})$. So every point $P \in C(\bar{K})$ can be characterized by its image $f(P)$ on D and the value of the b_i at P.

2.3. **Parameterizations.** An *S-parameterization* of a projective, absolutely integral, smooth curve C over K is a triple (D, ρ, π) where D is another projective, absolutely integral, smooth curve over K, and ρ is an S-multiradical map from D/K onto $\mathbb{P}^1/K$, and π is an epimorphism from D/K onto C/K. In this situation one says that C/K is *parameterizable* by S-radicals.

(1)



2.4. **Γ-groups.** Let K be a field with characteristic p. Let K_s be a separable closure of K. Let Γ be the Galois group of K_s/K. Let A be a finite set acted on continuously by Γ. We say that A is a finite Γ-set. We associate to it the separable K-algebra

$$\mathrm{Alg}(A) = \mathrm{Hom}_\Gamma(A, K_s)$$

of Γ-equivariant maps from A to K_s. If G is a finite Γ-set and has a group structure compatible with the Γ-action we say that G is a finite Γ-group, or a finite étale group scheme over K. Now let A be a finite Γ-set acted on by a finite Γ-group G. If the action of G on A is compatible with the actions of Γ on G and A, then we say that A is a finite G-set. The quotient A/G is then a finite Γ-set. If further G acts freely on A we say that A is a free finite G-set. A simply transitive G-set is called a G-torsor. The left action of G on itself defines a G-torsor called the trivial torsor. The set of isomorphism classes of G-torsors is isomorphic, as a pointed set, to $H^1(\Gamma, G)$. See [16, Chapter I §2].

Let $l \neq p$ be a prime and let A be a free finite μ_l-set. Let $B = A/\mu_l$. According to Kummer theory, the inclusion $\mathrm{Alg}(B) \subset \mathrm{Alg}(A)$ is a radical extension of separable K-algebras. It has degree l.

Let S be a finite set of primes. Assume that the characteristic p of K does not belong to S. A finite Γ-group G is said to be *S-resoluble* if there exists a sequence of Γ-subgroups $1 = G_0 \subset G_1 \subset \cdots \subset G_I = G$ such that for every i such that $0 \leq i \leq I-1$, the group G_i is normal in G_{i+1}, and the quotient G_{i+1}/G_i is isomorphic, as a finite Γ-group, to μ_{l_i} for some l_i in S.

Let G be a finite Γ-group. Assume that G is *S-resoluble*. Let A be a free finite G-set. Let $B = A/G$. The inclusion $\mathrm{Alg}(B) \subset \mathrm{Alg}(A)$ is an S-multiradical extension of separable K-algebras. It has degree $\#G$.

2.5. **Encodings.** We assume that K is a finite field with characteristic p and cardinality q. Let S be a set of prime integers. We assume that $p \notin S$ and S is disjoint from the support of $q-1$. Let $f : C \to D$ be a radical morphism of degree $l \in S$. Let $X \subset C$ be the ramification locus of f, and let $Y = f(X) \subset D$ be the branch locus. Let $F : C(K) \to D(K)$ the induced map on K-rational points. We prove that F is a bijection.

A branched point Q in $D(K)$ is totally ramified, so has a unique preimage P in $C(K)$. Let $Q \in D(K) - Y(K)$ be a non-branched point. The fiber $f^{(-1)}(Q)$ is a μ_l-torsor. Since $H^1(K, \mu_l) = K^*/(K^*)^l$ is trivial, this torsor is isomorphic to μ_l with the left action. Since $H^0(K, \mu_l) = \mu_l(K)$ is trivial also, $f^{(-1)}(Q)$ contains a unique K-rational point. Therefore F is a bijection.

Lemma 2. *Let K be a finite field with q elements. Let S be a finite set of prime integers. We assume that $p \notin S$ and S is disjoint from the support of $q-1$. Let $f : C \to D$ be an S-multiradical morphism between two smooth, projective, absolutely irreducible curves over K. The induced map $F : C(K) \to D(K)$ on K-rational points is a bijection.*

The reciprocal map $F^{(-1)} : D(K) \to C(K)$ can be evaluated in deterministic polynomial time by computing successive l-th roots for various $l \in S$.

We assume now that we are in the situation of the diagram (1). Let $R : D(K) \to \mathbb{P}^1(K)$ be the map induced by ρ and let $\Pi : D(K) \to C(K)$ be the map induced by π. The composition $\Pi \circ R^{(-1)}$ is called an *encoding*.

2.6. **Tartaglia-Cardan formulae.** Let K be a field with characteristic prime to 6. Let K_s be an algebraic closure of K. Let Γ be the Galois group of K_s/K. Let $\mu_3 \subset K_s$ be the finite Γ-set consisting of the three roots of unity. Let $\mathrm{Sym}(\mu_3)$ be the full permutation group on μ_3. The Galois group acts on μ_3. So we have a group homomorphism $\Gamma \to \mathrm{Sym}(\mu_3)$ and Γ acts on $\mathrm{Sym}(\mu_3)$ by conjugation. This action turns $\mathrm{Sym}(\mu_3)$ into a group scheme over K. Because μ_3 acts on itself by translation, we have an inclusion of group schemes $\mu_3 \subset \mathrm{Sym}(\mu_3)$ and μ_3 is a normal subgroup of $\mathrm{Sym}(\mu_3)$. The stabilizer of $1 \in \mu_3$ is a subgroup scheme of $\mathrm{Sym}(\mu_3)$. It is not normal in $\mathrm{Sym}(\mu_3)$. It is isomorphic to μ_2. So $\mathrm{Sym}(\mu_3)$ is the semidirect product $\mu_3 \rtimes \mu_2$.

Let $\zeta_3 \in K_s$ be a primitive third root of unity. We set $\sqrt{-3} = 2\zeta_3 + 1$. Let

$$h(x) = x^3 - s_1 x^2 + s_2 x - s_3$$

be a degree 3 separable polynomial in $K[x]$. Let

$$R = \mathrm{Roots}(h)$$

be the set of roots of $h(x)$ in K_s. This is a finite Γ-set with cardinality 3. Let

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

be the set of bijections from R to μ_3. For $\gamma \in \Gamma$ and $f \in A$ we set ${}^{\gamma}f = \gamma \circ f \circ \gamma^{-1}$. This turns A into a finite Γ-set of cardinality 6. The action of $\mathrm{Sym}(\mu_3)$ on the left turns it into a $\mathrm{Sym}(\mu_3)$-torsor. We call

$$C = A/\mu_3$$

the quotient of A by the normal Γ-subgroup $\mu_3 \subset \mathrm{Sym}(\mu_3)$ of order 3. This is a μ_2-torsor. We call

$$B = A/\mu_2$$

the quotient of A by the stabilizer of 1 in $\mathrm{Sym}(\mu_3)$. This a finite Γ-set of cardinality 3, naturally isomorphic to $\mathrm{Roots}(h)$. Indeed a function ξ in $\mathrm{Alg}(B) \subset \mathrm{Alg}(A)$ is defined by

$$\begin{aligned} \xi : \qquad & A \longrightarrow K_s \\ & f \longmapsto f^{(-1)}(1). \end{aligned}$$

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 construct functions in the algebra $\mathrm{Alg}(A)$ of the $\mathrm{Sym}(\mu_3)$-torsor A. These functions can be constructed with radicals because $\mathrm{Sym}(\mu_3) = \mu_3 \rtimes \mu_2$ is $\{2,3\}$-resoluble. A first function δ in $\mathrm{Alg}(C) \subset \mathrm{Alg}(A)$ is defined by

$$\begin{aligned} \delta : \qquad & A \longrightarrow K_s \\ & f \longmapsto \sqrt{-3}\big(f^{(-1)}(\zeta)-f^{(-1)}(1)\big)\big(f^{(-1)}(\zeta^2)-f^{(-1)}(\zeta)\big)\big(f^{(-1)}(1)-f^{(-1)}(\zeta^2)\big). \end{aligned}$$

Note that the $\sqrt{-3}$ is necessary to balance 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 discriminant Δ of $h(x)$ multiplied by -3. We say that -3Δ is the *twisted discriminant*. A natural function ρ in $\mathrm{Alg}(A)$ is defined as

$$\begin{aligned} \rho : \qquad & A \longrightarrow K_s \\ & f \longrightarrow \textstyle\sum_{r\in R} r \times f(r) = \sum_{\zeta\in\mu_3} \zeta \times f^{(-1)}(\zeta). \end{aligned}$$

It is clear that ρ^3 is invariant by $\mu_3 \subset \mathrm{Sym}(\mu_3)$ or equivalently belongs to $\mathrm{Alg}(C)$. So it can be expressed as a combination of 1 and δ. Indeed a simple calculation shows that

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

A variant of ρ is

$$\begin{aligned} \rho' : \qquad & A \longrightarrow K_s \\ & f \longrightarrow \textstyle\sum_{r\in R} r \times f(r)^{-1}. \end{aligned}$$

One has

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

and

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

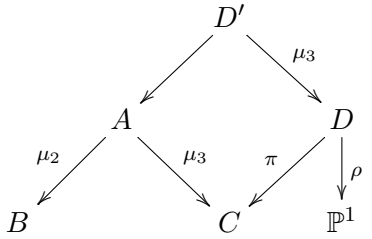
Finally, the root ξ of $h(x)$ can be expressed in terms of ρ and ρ' as

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

Note that the algebra $\mathrm{Alg}(A)$ is not the Galois closure of $K[x]/h(x)$. If we wanted to construct a Galois closure we would rather consider the $\mathrm{Sym}(\{1,2,3\})$-torsor $\mathrm{Bij}(R, \{1,2,3\})$ of indexations of the roots. We are not interested in this torsor however. This is because $\mu_3 \rtimes \mu_2$ is resoluble while $C_3 \rtimes C_2$ is not, in general. The algebra constructed by Tartaglia and Cardan contains the initial cubic extension, because the quotient of $\mathrm{Bij}(\mathrm{Roots}(h), \mu_3)$ by the stabilizer of 1 in $\mathrm{Sym}(\mu_3)$ is isomorphic to the quotient of $\mathrm{Bij}(R, \{1,2,3\})$ by the stabilizer of 1 in $\mathrm{Sym}(\{1,2,3\})$, that is $\mathrm{Roots}(h)$. On the other hand, the quotient of $\mathrm{Bij}(R, \{1,2,3\})$ by the 3-cycle $(123) \in \mathrm{Sym}(\{1,2,3\})$ is associated with the algebra $K[x]/(x^2 - \Delta)$ while the quotient of $\mathrm{Bij}(R, \mu_3)$ by the 3-cycle $(1\zeta\zeta^2) \in \mathrm{Sym}(\mu_3)$ is associated with the algebra $K[x]/(x^2 + 3\Delta)$.

2.7. **Curves with a $\mu_3 \rtimes \mu_2$ action.** We still assume that the characteristic of K is prime to 6. Let A be a projective, absolutely integral, smooth curve over K. We assume that the automorphism group $\mathrm{Aut}(A \otimes_K K_s)$ contains a finite étale K-group-scheme isomorphic to $\mu_3 \rtimes \mu_2$. The quotients $B = A/\mu_2$, and $C = A/\mu_3$ are projective, absolutely integral, smooth curves over K. In this situation, we say that C is the *resolvent* of B. By abuse of language we may say also that we have constructed a parameterization of B by C.

Assume now that C admits a parameterization by S-radical as in diagram (1). We call D' the normalization of the fiber product of A and D above C. We assume that D' is absolutely integral.



We set $S' = S \cup \{3\}$. We let ρ' be the composite map

$$\rho' : D' \xrightarrow{\mu_3} D \xrightarrow{\rho} \mathbb{P}^1,$$

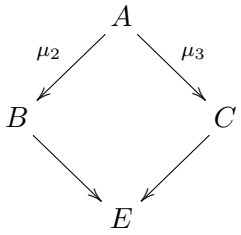
and π' the composite map

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

Then (D', ρ', π') is an S'-parameterization of B. The mild condition that D' be absolutely integral is granted in the following cases:

(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 point P of C, and π is not branched at P. Indeed the two coverings are linearly disjoint in that case. We note that 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, because $A \to C$ and π are linearly disjoint then. Note that the resulting parameterization π' has degree prime to 3 also. We can iterate in that case.

2.8. **Selecting curves.** We still assume that the characteristic of K is prime to 6. We now look for interesting examples of curves with a $\mu_3 \rtimes \mu_2$ action. We keep the notation introduced in Section 2.7. We set $E = A/(\mu_3 \rtimes \mu_2)$.



The curve C is the one we already know how to parameterize. The curve B is the one we want to parameterize. It should be as generic as possible. In particular, we will assume that $E = \mathbb{P}^1$. Otherwise, the Jacobian of B would contain a subvariety isogenous to the Jacobian of E. It would not be so generic then.

Assuming now that $E = \mathbb{P}^1$ we denote by r the number of branched points of the cover $B \to E$. Let r_s be the number of branched points with ramification type $2, 1$. These are called simple branched points. Let r_t the number of branched points with ramification type 3. These are totally branched points. We have $r = r_s + r_t$. According to the Hurwitz Genus Formula [19, III.4.12, III.5.1] the genus of B is

$$g_B = \frac{r_s}{2} + r_t - 2.$$

We note that every simple branched point of the cover $B \to E$ gives rise to a branched point of type $2, 2, 2$ of the cover $A \to E$ and to a (necessarily simple) branched point of $C \to E$. And every totally branched point of the cover $B \to E$ gives rise to a branched point of type $3, 3$ of the cover $A \to E$ and to a non-branched point of $C \to E$. So

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

We set

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

and call it the *modular dimension*. It is the dimension of the family of covers obtained by letting the r branched points move along $E = \mathbb{P}^1$. The -3 stands for the action of $\mathrm{Aut}(\mathbb{P}^1) = \mathrm{PGL}_2$. If we aim at all curves of genus g_B we should have m greater than or equal to the dimension of the moduli space of curves of genus g_B. We deduce the *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 $n \geq 2$. This is a necessary condition.

The first case to consider is when C has genus 0 (because we know how to parameterize genus 0 curves). So we first take $r_s = 2$. So $g_B = r_t - 1$ and the genericity condition reads $r_t \leq 2$. Only $r_t = 2$ is of interest. We shall see in Section 3 that we find a parameterization similar to those by Farashahi and Kammerer, Lercier, Renault in this case.

Assuming we know how to parameterize some genus 1 curves, we may consider the case when C itself has genus 1. We have $r_s = 4$ in that case. And $g_B = r_t$. The genericity assumption reads $r_t \leq 2$. The case $r_t = 2$ will be studied in detail in Section 4.

3. Curves of genus 1

Let K be a field of characteristic prime to 6. Let B/K be a projective, smooth, absolutely integral curve of genus 1. This is the curve we want to parameterize, following the strategy presented in Sections 2.7 and 2.8. Since $r_s = r_t = 2$ in this case, we look for a map $B \to \mathbb{P}^1$ of degree 3 with two fully branched points and two simply branched points. Such a map has two totally ramified points. They may be either K-rational or conjugated over K. We will assume that they are K-rational. We call them P_0 and P_∞. The two divisors $3P_0$ and $3P_\infty$ are linearly equivalent because they both are fibers of the same degree three map to $\mathbb{P}^1$. So the difference $P_\infty - P_0$ has order 3 in the Jacobian of B. Our starting point will thus be a genus 1 curve B/K and two points P_0, P_∞ in $B(K)$ such that $P_\infty - P_0$ has order 3 in the Jacobian.

Let $z \in K(B)$ be a function with divisor $3(P_0 - P_\infty)$. There is a unique hyperelliptic involution $\sigma : B \to B$ sending P_0 onto P_∞. It is defined over K. There exists a scalar $a_{0,0} \in K^*$ such that $\sigma(z) \times z = a_{0,0}$. Let x be a degree 2 function, invariant by σ, with polar divisor $(x)_\infty = P_0 + P_\infty$. Associated to the inclusion $K(x) \subset K(x,z)$ there is a map $B \to \mathbb{P}^1$ of degree 2. 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 $x = \infty$. So $z + a_{0,0}/z$ is a polynomial of degree 3 in x. Multiplying z by a scalar, and adding a scalar to x, we may assume that

$$z + \frac{a_{0,0}}{z} = x^3 + a_{1,1}x + a_{0,1}. \tag{2}$$

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

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

This is a curve $B^\star \subset \mathbb{P}^1 \times \mathbb{P}^1$ with arithmetic genus 2. Since B has geometric genus 1, we deduce that $B^\star$ has one ordinary double point (with finite x and z coordinates). Let $(x,z) = (j,k)$ be this singular point. We find

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

The plane affine model $B^\star$ has equation

$$z^2 + k^2 = z\left(x^3 - 3j^2 x + 2(k + j^3)\right). \tag{3}$$

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

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

We can parameterize B with cubic radicals. We first parameterize the conic C with equation

$$v^2 = h(z) \tag{4}$$

using the rational point $(z,v) = (0,k)$. Applying Tartaglia-Cardan formulae to the cubic Equation (3) we deduce a parameterization of B with one cubic radical. In order to relate Equation (3) to a Weierstrass model, we simply sort in z and find the degree 2 equation in z,

$$z^2 - (x^3 - 3j^2 x + 2k + 2j^3)z + k^2 = 0$$

with discriminant

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

A Weierstrass model for B is then $u^2 = (x + 2j)(x^3 - 3j^2 x + 4k + 2j^3)$. Replacing j by λj and k by $\lambda^3 k$ for some non-zero λ in K we obtain an isomorphic curve. So we may assume that $j \in \{0, 1\}$ without loss of generality. This construction is not substantially different from the ones

given by Farashahi [7] and Kammerer, Lercier, Renault [13]. Starting from any genus 1 curve B and two points P_0 and P_∞ such that $P_\infty - P_0$ has order 3 in the Jacobian, we can construct a model of B as in Equation (3) and a parameterization of B.

Example. Let us consider an elliptic curve given in Weierstrass form $Y^2 = X^3 + a\,X + b$, for example the curve $Y^2 = X^3 + 3\,X - 11$ over $\mathbb{R}$, together with a 3-torsion point $(x_0, y_0) = (3, -5)$.

Define the scalars α and β by

$$\alpha = -\frac{3\,{x_0}^2 + a}{2\,y_0} \text{ and } \beta = -y_0 - \alpha\,x_0.$$

The functions $x = \alpha/3 + (Y + y_0)/(X - x_0)$ and $z = Y + \alpha\,X + \beta$ have divisors with zeros and poles as prescribed. On our particular curve, these functions are

$$x = \frac{Y - 5}{X - 3} + 1 \text{ and } z = Y + 3\,X - 4\,. \tag{5}$$

The functions x and z are related by Equation (2) where

$$a_{0,0} = 4\,y_0^2 = 100\,,\ a_{1,1} = -4\,x_0 = -12\,,\ a_{0,1} = -4\,\frac{4\,a^3 + 27\,b^2}{27\,{y_0}^3} = 4\,.$$

So

$$z + \frac{100}{z} = x^3 - 12\,x + 4\,.$$

The double point on the latter is $(x, z) = (j, k)$ with

$$j = \frac{-2\alpha}{3} = -2 \text{ and } k = -2\,y_0 = 10\,.$$

A parameterization of the conic C given by Equation (4) that reaches the point $(z, v) = (0, k)$ at $t = \infty$ is

$$z = 2\,\frac{kt - k - 2\,j^3}{t^2 - 1} = 4\,\frac{5\,t + 3}{t^2 - 1}\,,\ v = k - tz = \frac{(2k + 4j^3)t - kt^2 - k}{t^2 - 1}\,.$$

and using Tartaglia-Cardan formulae we find $x = \rho/3 + 3j^2/\rho$ with

$$\rho = 3j^2 \times \sqrt[3]{\frac{2(t+1)}{(2\,j^3 - kt + k)\,(1 - t)}}\,.$$

It remains to invert Eq. (5) in order to express X and Y as functions of x and y, *i.e.* as functions of the parameter t. For $t = 0$, we obtain in this way the point

$$(X, Y) = (2\,(\sqrt[3]{3})^2 + 4\,\sqrt[3]{3} + 3,\ -6\,(\sqrt[3]{3})^2 - 12\,\sqrt[3]{3} - 17)\,.$$

4. Curves of genus 2

We look for parameterizations of genus 2 curves. We will follow the strategy of Sections 2.7 and 2.8. We take $r_s = 4$ and $r_t = 2$ this time. Given a genus 2 curve B, we look for a degree three map $B \to \mathbb{P}^1$ having 4 simply branched points and 2 totally branched points. Such a map has two totally ramified points. We will assume that they are K-rational. We call them P_0 and P_∞. The difference $P_\infty - P_0$ has order 3 in the Jacobian of B. Our starting point will thus be a genus 2 curve B/K and two points P_0, P_∞ in $B(K)$ such that $P_\infty - P_0$ has order 3 in the Jacobian. The calculations will be slightly different depending on whether the set $\{P_0, P_\infty\}$ is stable under the action of the hyperelliptic involution of B or not. These two cases will be treated in Sections 4.2 and 4.3

respectively. Section 4.1 recalls simple facts about genus 2 curves. Explicit calculations are detailed in Sections 4.4 and 4.5.

4.1. **Generalities.** Let K be a field of odd characteristic. Let $\bar{K}$ be an algebraic closure of K. Let B/K be a projective, smooth, absolutely integral curve of genus 2. Take two non-proportional holomorphic differential forms and let x be their quotient. This is a function on B of degree 2. Any degree 2 function y on B belongs to the field $K(x) \subset K(B)$. Otherwise the image of $x \times y : B \to \mathbb{P}^1 \times \mathbb{P}^1$ would be a curve birationally equivalent to B with arithmetic genus $(2-1) \times (2-1) = 1$. A contradiction. So every degree two function on B has the form $(ix+j)/(kx+l)$ with i, j, k and l in K. And B has a unique hyperelliptic involution σ. This is the non-trivial automorphism of the Galois extension $K(x) \subset K(B)$. From Hurwitz genus formula, this extension is ramified at exactly 6 geometric points $(P_i)_{1 \leq i \leq 6}$ in $B(\bar{K})$. If $\#K > 5$ we can assume that the unique pole of x is not one of the P_i. Set $F(x) = \prod_i (x - x(P_i)) \in K[x]$. According to Kummer theory, there exists a scalar $F_0 \in K^*$ such that $F_0 F$ has a square root y in $K(B)$. We set $f = F_0 F$ and obtain an affine model for B with equation

$$y^2 = f(x)$$

and two $\bar{K}$-points O and $\sigma(O)$ at infinity. Every function c in $K(B)$ can be written as

$$c = a(x) + yb(x)$$

with a and b in $K(x)$. If $P = (x_P, y_P)$ is a $\bar{K}$-point on B we denote by v_P the associated valuation of $\bar{K}(B)$. If P is one of the $(P_i)_{1 \leq i \leq 6}$ then

$$v_P(c) = \min(2v_{x_P}(a), 2v_{x_P}(b) + 1), \tag{6}$$

where $x_P = x(P) \in \bar{K}$ and v_{x_P} is the valuation of $\bar{K}(x)$ at $x = x_P$. If P is a finite point which is not fixed by σ then

$$\min(v_P(c), v_{\sigma(P)}(c)) = \min(v_{x_P}(a), v_{x_P}(b)). \tag{7}$$

Finally

$$\min(v_O(c), v_{\sigma(O)}(c)) = \min(-\deg(a), -\deg(b) - 3). \tag{8}$$

Let J be the Jacobian of B. A point x in J can be represented by a divisor in the corresponding linear equivalence class. We may fix a degree 2 divisor Ω and associate to x a degree 2 effective divisor D_x such that $D_x - \Omega$ belongs to the linear equivalence class associated with x. This D_x is generically unique. Indeed the only special effective divisors of degree 2 are the fibers of the map $B \to \mathbb{P}^1$. We may also represent linear equivalence classes by divisors of the form $P - Q$ where P and Q are points on B. There usually are two such representations as the map

$$B^2 \longrightarrow \mathrm{Jac}(B)$$

$$(P, Q) \longmapsto P - Q,$$

is surjective and its restriction to the open set defined by

$$P \neq Q, P \neq \sigma(Q)$$

is finite étale of degree 2.

4.2. **A 2-dimensional family.** Let K be a field of characteristic prime to 6. In this paragraph we study genus 2 curves B/K satisfying the condition that there exists a point P in $B(K)$ such that the class of $\sigma(P) - P$ has order 3 in the Picard group. In particular P is not fixed by σ. We let x and y be functions as in Section 4.1. We can assume that $x(P) = \infty$. Let z be a function with divisor $3(\sigma(P) - P)$. There exists a scalar $w \in K^*$ such that $\sigma(z) \times z = w$. We write

$$z = a(x) + yb(x)$$

with a and b in $K(x)$. We deduce from Equations (6), (7), (8), that a and b are polynomials and $\deg(a) \leq 3$ and $\deg(b) \leq 0$. From $z\sigma(z) = a^2 - b^2 f = w \in K^*$ we deduce that $\deg(b) = 0$ and $\deg(a) = 3$. We may divide z by a scalar in K^* and assume that a is unitary. Replacing x by $x + \beta$ for some β in K, we may even assume that $a(x) = x^3 + kx + l$ with k and l in K. Replacing y by by we may assume that $b = 1$ so

$$z = y + x^3 + kx + l.$$

An affine plane model for B has thus equation

$$z^2 - 2a(x)z + w = 0$$

that is

$$x^3 + kx + l = \frac{z + wz^{-1}}{2}. \tag{9}$$

This a degree 3 equation in x with coefficients $s_1 = 0$, $s_2 = k$, $s_3 = (z + wz^{-1})/2 - l$, and twisted discriminant $81/4$ times

$$h(z) = z^2 + w^2 z^{-2} - 4l(z + wz^{-1}) + 2w + 4l^2 + \frac{16k^3}{27}.$$

We can parameterize B with cubic radicals. We first parameterize the elliptic curve C with equation $v^2 = h(z)$ with one cubic radical, using e.g. Icart's method [11]. We deduce a parameterization of B applying Tartaglia-Cardan formulae to the cubic Equation (9). This introduces another cubic radical. This is essentially the construction given by Kammerer, Lercier and Renault [13]. Note that this family of genus 2 curves has dimension 2: when K is algebraically closed we may assume that $w = 1$ without loss of generality.

4.3. **The complementary 3-dimensional family.** We still assume that K has prime to 6 characteristic. We consider a genus 2 curve B and two points P_0 and P_∞ in $B(K)$ such that the difference $P_0 - P_\infty$ has order 3 in the Picard group. This time we assume that $P_\infty \neq \sigma(P_0)$. There exists a degree 2 function x having a zero at P_0 and a pole at P_∞. Let z be a function with divisor $3(P_0 - P_\infty)$. The image of $x \times z : B \to \mathbb{P}^1 \times \mathbb{P}^1$ has equation

$$\sum_{\substack{0 \leqslant i \leqslant 3 \\ 0 \leqslant j \leqslant 2}} a_{i,j} X_1^i X_0^{3-i} Z_1^j Z_0^{2-j} = 0. \tag{10}$$

The function z takes the value ∞ at a single point, and x has a pole at this point. So if we set $Z_0 = 0$ in Equation (10) the form we find must be proportional to $Z_1^2 X_0^3$. We deduce that

$$a_{3,2} = a_{2,2} = a_{1,2} = 0$$

and

$$a_{0,2} \neq 0.$$

The function z takes value 0 at a single point, and x has a zero at this point. So if we set $Z_1 = 0$ in Equation (10) the form we find must be proportional to $Z_0^2 X_1^3$. We deduce that

$$a_{2,0} = a_{1,0} = a_{0,0} = 0$$

and

$$a_{3,0} \neq 0.$$

Equation (10) now reads

$$(a_{3,0}Z_0 + a_{3,1}Z_1)Z_0X_1^3 + (a_{1,1}X_0 + a_{2,1}X_1)Z_0Z_1X_0X_1 + (a_{0,1}Z_0 + a_{0,2}Z_1)Z_1X_0^3 = 0.$$

This is a curve of arithmetic genus 2 in $\mathbb{P}^1 \times \mathbb{P}^1$. It must be smooth because it has geometric genus 2. The corresponding plane affine model has equation

$$(a_{3,0} + a_{3,1}z)x^3 + (a_{1,1} + a_{2,1}x)zx + (a_{0,1} + a_{0,2}z)z = 0. \tag{11}$$

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

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

We can parameterize B with cubic radicals. We first parameterize the elliptic curve with equation $v^2 = h(z)$ with one cubic radical, using Icart's method. We deduce a parameterization of B applying Tartaglia-Cardan formulae to the cubic Equation (11). This introduces another cubic radical.

In order to relate Equation (11) to an hyperelliptic model, we simply sort in z and find the degree 2 equation in z,

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

with discriminant

$$m(x) = (a_{3,1}x^3 + a_{2,1}x^2 + a_{1,1}x + a_{0,1})^2 - 4a_{0,2}a_{3,0}x^3. \tag{12}$$

An hyperelliptic model for B is then

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

The construction will succeed for every genus 2 curve having a rational 3-torsion point in its Jacobian that splits in the sense that it can be represented as a difference between two K-rational points on B.

4.4. **Rational 3-torsion points in genus 2 Jacobians.** In this section we start from an hyperelliptic curve

$$\mathbf{y}^2 = \mathbf{m}(\mathbf{x}),$$

where $\mathbf{m}(\mathbf{x})$ is a degree 6 polynomial. We look for a parameterization of it, following Sections 4.2 or 4.3. To this end we need a model as in Equations (11) and (12). Such a model is obtained by writing $\mathbf{m}(\mathbf{x})$ as a difference $\mathbf{m}_3(\mathbf{x})^2 - \mathbf{m}_2(\mathbf{x})^3$ where $\mathbf{m}_3$ is a degree ≤ 3 polynomial and $\mathbf{m}_2$ is a degree ≤ 2 polynomial with rational roots. We now are very close to investigations by Clebsh [4] and Elkies [6]. Three-torsion points in the Jacobian of the curve $\mathbf{y}^2 = \mathbf{m}(\mathbf{x})$ correspond to expressions of $\mathbf{m}$ as a difference between a square and a cube. When the base field K is finite, we may first compute the Zeta function of the curve, deduce the cardinality of the Picard group and obtain elements of order 3 in it by multiplying random elements in the Picard group by the prime to three part of its order. For

a general base field K, we can look for solutions to $\mathbf{m}(\mathbf{x}) = \mathbf{m}_3(\mathbf{x})^2 - \mathbf{m}_2(\mathbf{x})^3$ by a direct Gröbner basis computation. Our experiments with the computer algebra softwares MAPLE or MAGMA show that this approach is efficient enough when K is a finite field of reasonable (say cryptographic) size. When K is the field $\mathbb{Q}$ of rationals, this direct approach becomes quite slow.

In this section we explain how to accelerate the computation using invariant theory. Our method takes as input, instead of $\mathbf{m}(\mathbf{x})$, the standard homogeneous invariants for the action of GL_2 evaluated at $\mathbf{m}(\mathbf{X}_1, \mathbf{X}_0)$, the degree 6 projective form associated with $\mathbf{m}(\mathbf{x})$. Classical invariant theory results [1, 4] show that the orbit under GL_2 of a degree 6 non-singular form $\mathbf{m}(\mathbf{X}_1, \mathbf{X}_0)$ is characterized by 5 homogeneous invariants I_2, I_4, I_6, I_{10}, I_{15}, of respective degrees 2, 4, 6, 10, and 15. There is a degree 30 algebraic relation between the I_i (see [12]).

The action of GL_2 on pairs $(\mathbf{m}_2(\mathbf{X}_1, \mathbf{X}_0), \mathbf{m}_3(\mathbf{X}_1, \mathbf{X}_0))$ consisting of a quadric and a cubic gives rise to well known invariants also: ι_2 (the discriminant of m_2), ι_4 (the discriminant of m_6) and 3 joint invariants ι_3, ι_5 and ι_7, of respective degrees 2, 4, 3, 5 and 7. There is a degree 14 algebraic relation between the ι_i [17, p.187-189]. Since the map $(\mathbf{m}_2, \mathbf{m}_3) \mapsto \mathbf{m} = \mathbf{m}_3^2 - \mathbf{m}_2^3$ is GL_2-equivariant we can describe its fibers in terms of the invariants on each side. We easily obtain the I_i's as functions of the ι_i's,

$$
\begin{aligned}
2^2\, I_2 &= 120\,\iota_5 + 4\,\iota_4 - 12\,\iota_3\,\iota_2 + 3\,{\iota_2}^3\,,\\
2^7\, I_4 &= 2640\,{\iota_5}^2 + 96\,\iota_5\,\iota_4 - 768\,\iota_5\,\iota_3\,\iota_2 + 240\,\iota_5\,{\iota_2}^3 - 24\,\iota_4\,\iota_3\,\iota_2 + 8\,\iota_4\,{\iota_2}^3\\
&\quad -8\,{\iota_3}^3 + 48\,{\iota_3}^2{\iota_2}^2 - 24\,\iota_3\,{\iota_2}^4 + 3\,{\iota_2}^6\,,\\
2^{10}\, I_6 &= -5120\,{\iota_5}^3 - 192\,{\iota_5}^2\iota_4 - 2304\,{\iota_5}^2\iota_3\,\iota_2 + 3504\,{\iota_5}^2{\iota_2}^3 - 96\,\iota_5\,\iota_4\,\iota_3\,\iota_2\\
&\quad +240\,\iota_5\,\iota_4\,{\iota_2}^3 - 288\,\iota_5\,{\iota_3}^3 + 1008\,\iota_5\,{\iota_3}^2{\iota_2}^2 - 768\,\iota_5\,\iota_3\,{\iota_2}^4 + 120\,\iota_5\,{\iota_2}^6\\
&\quad +4\,{\iota_4}^2{\iota_2}^3 + 24\,\iota_4\,{\iota_3}^2{\iota_2}^2 - 24\,\iota_4\,\iota_3\,{\iota_2}^4 + 4\,\iota_4\,{\iota_2}^6 + 36\,{\iota_3}^4\iota_2\\
&\quad -72\,{\iota_3}^3{\iota_2}^3 + 48\,{\iota_3}^2{\iota_2}^5 - 12\,\iota_3\,{\iota_2}^7 + {\iota_2}^9\,,\\
2^{12}\, I_{10} &= 46656\,{\iota_5}^5 + 3456\,{\iota_5}^4\iota_4 - 3888\,{\iota_5}^4\iota_3\,\iota_2 + 729\,{\iota_5}^4{\iota_2}^3 + 64\,{\iota_5}^3{\iota_4}^2\\
&\quad -144\,{\iota_5}^3\iota_4\,\iota_3\,\iota_2 + 27\,{\iota_5}^3\iota_4\,{\iota_2}^3 + 128\,{\iota_5}^3{\iota_3}^3 - 27\,{\iota_5}^3{\iota_3}^2{\iota_2}^2\,.
\end{aligned}
\tag{13}
$$

Given the I_i's evaluated at $\mathbf{m}(\mathbf{X}_1, \mathbf{X}_0)$, the generic change of variable $\lambda = {\iota_2}^3$ and $\mu = \iota_2 \times \iota_3$ turns these equations into a system of 4 equations of total degrees 1, 3, 4 and 6 in the 4 variables λ, μ, ι_4 and ι_5. A Gröbner basis can be easily computed for the lexicographic order (note that the first equation is linear). This yields a degree 40 polynomial in λ. If none of the roots of this polynomial are squares, we can abort the calculation because we need $\mathbf{m}_2(\mathbf{x})$ to have rational roots in order to parameterize the curve $\mathbf{y}^2 = \mathbf{m}(\mathbf{x})$.

Considering Equation (12) of Section 4.3 it is natural to look for a form m in the GL_2-orbite of $\mathbf{m}$ such that $m = m_3^2 - m_2^3$ for some $m_2(x) = e\,x$ and $m_3(x) = a\,x^3 + b\,x^2 + c\,x + d$, where $e^3 = 4a_{0,2}a_{3,0}$, $a = a_{3,1}$, $b = a_{2,1}$, $c = a_{1,1}$, $d = a_{0,1}$. The invariants of (m_2, m_3) are

$$
\begin{aligned}
&\iota_2 = e^2\,,\ \iota_3 = -e(9\,ad - bc)\,, \qquad \iota_5 = -e^3ad\,,\ \iota_7 = e^3(ac^3 - b^3d)\,,\\
&\qquad\qquad \iota_4 = -27\,a^2d^2 + 18\,abcd - 4\,ac^3 - 4\,b^3d + b^2c^2\,.
\end{aligned}
\tag{14}
$$

So for each candidate $(\iota_2, \iota_3, \iota_4, \iota_5)$ issued from Equations (13), we invert Eq. (14). A Groebner basis for the lexicographic order d, c, b, a, e yields generically a 1-dimensional system the last two equations of which are

$$
\begin{aligned}
0 &= e^2 - \iota_2\,,\\
0 &= {\iota_2}^3\iota_5\,b^6 - \iota_2\,({\iota_2}^3\iota_4 - {\iota_2}^2{\iota_3}^2 + 36\,\iota_2\,\iota_3\,\iota_5 - 216\,{\iota_5}^2)\,e\,a\,b^3 - 4\,(\iota_2\,\iota_3 - 9\,\iota_5)^3\,a^2\,.
\end{aligned}
$$

We keep solutions $m_2(x)$ and $m_3(x)$ that yield a polynomial $m(x) = m_3(x)^2 - m_2(x)^3$ which is GL_2-equivalent to $\mathbf{m}(\mathbf{x})$ over the base field (see [15] for efficient algorithms). Applying the isomorphism to $m_2(x)$ and $m_3(x)$ gives $\mathbf{m}_2(\mathbf{x})$ and $\mathbf{m}_3(\mathbf{x})$.

4.5. **An example.** Let K be a field with 83 elements. We start from the genus 2 curve with affine equation $\mathbf{y}^2 = \mathbf{m}(\mathbf{x})$ with $\mathbf{m}(\mathbf{x}) = \mathbf{x}^6 + 39\mathbf{x}^5 + 64\mathbf{x}^4 + 7\mathbf{x}^3 + \mathbf{x}^2 + 19\mathbf{x} + 36$. In order to find $\mathbf{m}_3(\mathbf{x})$ and $\mathbf{m}_2(\mathbf{x})$ such that $\mathbf{m}(\mathbf{x}) = \mathbf{m}_3(\mathbf{x})^2 - \mathbf{m}_2(\mathbf{x})^3$, we first compute the invariants of the degree six form $\mathbf{m}$

$$(I_2, I_4, I_6, I_{10}) = (23, 9, 38, 53, 59)\,.$$

A Groebner basis for the relations between λ, μ and ι_4 is

$$\begin{aligned}
\iota_4 &= 27\,\lambda^{39} + 58\,\lambda^{38} + 3\,\lambda^{37} + 18\,\lambda^{36} + 42\,\lambda^{35} + 26\,\lambda^{34} + 52\,\lambda^{33} + 60\,\lambda^{32} + 78\,\lambda^{31} + 17\,\lambda^{30} \\
&\quad +50\,\lambda^{29} + 12\,\lambda^{28} + 75\,\lambda^{27} + 20\,\lambda^{26} + 75\,\lambda^{25} + 38\,\lambda^{24} + 19\,\lambda^{23} + 21\,\lambda^{22} + 35\,\lambda^{21} \\
&\quad +31\,\lambda^{20} + 27\,\lambda^{19} + 49\,\lambda^{18} + 44\,\lambda^{17} + 30\,\lambda^{16} + 38\,\lambda^{15} + 55\,\lambda^{14} + 59\,\lambda^{13} + 6\,\lambda^{12} + 2\,\lambda^{11} \\
&\quad +36\,\lambda^{10} + 18\,\lambda^9 + 2\,\lambda^8 + 41\,\lambda^7 + 62\,\lambda^6 + 3\,\lambda^5 + 49\,\lambda^4 + \lambda^3 + 33\,\lambda^2 + 36\,\lambda + 69\,, \\
\mu &= 62\,\lambda^{40} + 46\,\lambda^{39} + 11\,\lambda^{38} + 33\,\lambda^{37} + 75\,\lambda^{36} + 19\,\lambda^{35} + 53\,\lambda^{34} + 10\,\lambda^{33} + 48\,\lambda^{32} + 47\,\lambda^{31} \\
&\quad +77\,\lambda^{30} + 14\,\lambda^{29} + 49\,\lambda^{28} + 47\,\lambda^{27} + 38\,\lambda^{26} + 19\,\lambda^{25} + 25\,\lambda^{24} + 44\,\lambda^{23} + 68\,\lambda^{22} \\
&\quad +15\,\lambda^{21} + 36\,\lambda^{20} + 9\,\lambda^{19} + 73\,\lambda^{18} + 13\,\lambda^{17} + 64\,\lambda^{16} + 5\,\lambda^{15} + 67\,\lambda^{14} + 82\,\lambda^{13} + 69\,\lambda^{12} \\
&\quad +9\,\lambda^{11} + 69\,\lambda^{10} + 35\,\lambda^9 + 57\,\lambda^8 + 57\,\lambda^7 + 7\,\lambda^6 + 11\,\lambda^5 + 37\,\lambda^4 + 78\,\lambda^3 + 10\,\lambda^2 + 73\,\lambda\,, \\
0 &= \lambda^{40} + 48\,\lambda^{39} + 67\,\lambda^{38} + 35\,\lambda^{37} + 50\,\lambda^{36} + 23\,\lambda^{35} + 4\,\lambda^{34} + 12\,\lambda^{33} + 37\,\lambda^{32} + 49\,\lambda^{31} + \\
&\quad 40\,\lambda^{30} + 71\,\lambda^{29} + 60\,\lambda^{28} + 79\,\lambda^{27} + 19\,\lambda^{26} + 81\,\lambda^{25} + 82\,\lambda^{24} + 26\,\lambda^{23} + 9\,\lambda^{22} + 19\,\lambda^{21} \\
&\quad +82\,\lambda^{20} + 40\,\lambda^{19} + 50\,\lambda^{18} + 67\,\lambda^{17} + 80\,\lambda^{16} + 29\,\lambda^{15} + 73\,\lambda^{14} + 38\,\lambda^{13} + 81\,\lambda^{12} \\
&\quad +73\,\lambda^{11} + 5\,\lambda^{10} + 14\,\lambda^9 + 82\,\lambda^8 + 46\,\lambda^7 + 62\,\lambda^6 + 32\,\lambda^5 + 17\,\lambda^4 + 74\,\lambda^3 \\
&\quad +15\,\lambda^2 + 30\,\lambda + 43\,.
\end{aligned}$$

Here, we only have two rational candidates for (λ, μ, ι_4), the first one gives

$$(\iota_2, \iota_3, \iota_4, \iota_5) = (17, 51, 35, 55)\,.$$

Now, inverting Eq. (14) yields 4 possibilities, all parameterized by a:

(1) $\{\, d + 74\,c^3 = 0, c\,b + 45 = 0, c\,a + 63\,b^2 = 0, b^3 + 23\,a = 0, e + 73 = 0 \,\}$,
(2) or $\{\, d + 65\,c^3 = 0, c\,b + 45 = 0, c\,a + 73\,b^2 = 0, b^3 + 46\,a = 0, e + 73 = 0 \,\}$,
(3) or $\{\, d + 18\,c^3 = 0, c\,b + 38 = 0, c\,a + 73\,b^2 = 0, b^3 + 37\,a = 0, e + 10 = 0 \,\}$,
(4) or $\{\, d + 9\,c^3 = 0, c\,b + 38 = 0, c\,a + 63\,b^2 = 0, b^3 + 60\,a = 0, e + 10 = 0 \,\}$.

A solution to the first set of equations is, for $a = 1$,

$$m_3(x) = x^3 + 46\,x^2 + 73\,x + 47 \text{ and } m_2(x) = 10\,x,$$

and the polynomial

$$m(x) = m_3(x)^2 - m_2(x)^3$$

is GL_2-equivalent to $\mathbf{m}(x)$. Indeed

$$m(\frac{76\mathbf{x} + 70}{36\mathbf{x} + 43}) \times (36\mathbf{x} + 43)^6 = \mathbf{m}(\mathbf{x}).$$

So we set

$$\mathbf{m}_3(\mathbf{x}) = m_3(\frac{76\mathbf{x} + 70}{36\mathbf{x} + 43}) \times (36\mathbf{x} + 43)^3 = 15\mathbf{x}^3 + 30\mathbf{x}^2 + 46\mathbf{x} + 7$$

and

$$\mathbf{m}_2(\mathbf{x}) = m_2(\frac{76\mathbf{x}+70}{36\mathbf{x}+43}) \times (36\mathbf{x}+43)^2 = 53\mathbf{x}^2 + 29\mathbf{x} + 54$$

and we check that $\mathbf{m} = \mathbf{m}_3^2 - \mathbf{m}_2^3$.

Parameterization. The curve with equation $\mathbf{y}^2 = \mathbf{m}(\mathbf{x})$ over the field with 83 elements is isomorphic to the curve with equation

$$y^2 = (ax^3 + b\,x^2 + c\,x + d)^2 - (e\,x)^3 = (x^3 + 46\,x^2 + 73\,x + 47)^2 - (10\,x)^3$$

through the change of variables

$$x = \frac{76\mathbf{x}+70}{36\mathbf{x}+43}, \text{ and } y = \frac{\mathbf{y}}{(36\mathbf{x}+43)^3}. \tag{15}$$

With the notation in Section 4.3 we have $a = a_{3,1} = 1$, $b = a_{2,1} = 46$, $c = a_{1,1} = 73$, $d = a_{0,1} = 47$, $e = 10$, $a_{0,2} = -1/2$, $a_{3,0} = -e^3/2$. Let P_0 be the point with coordinates $x = 0$ and $y = -47$. Let P_∞ be the point where x has a pole and $y/x^3 = 1$. The functions x has a zero at P_0 and a pole at P_∞. The function $z = y + a\,x^3 + b\,x^2 + c\,x + d$ has divisor $3(P_0 - P_\infty)$. These two functions are related by the equation

$$(-e^3/2 + az)x^3 + (bx + c)zx + (d - z/2)z = 0, \tag{16}$$

that is $(z + 81)x^3 + (46\,x + 73)zx + (47 + 41\,z)z = 0$. The resolvent elliptic curve has equation $v^2 = h(z)$ with

$$h(z) = 41\,z^4 + 15\,z^3 + 38\,z^2 + 46\,z + 7\,.$$

It is birationally isomorphic to the Weierstrass curve with equation $Y^2 = X^3 + 37\,X + 60$, whose Icart's parameterization in t is

$$X = \kappa/6 + t^2/3\,,\ Y = (t^3 + t\,\kappa + 28/t)/6$$

where

$$\kappa = \sqrt[3]{81\,t^6 + 79\,t^2 + 71 + \frac{56}{t^2}}\,.$$

After a birational change of variable, we obtain

$$z = \frac{10\,Y + 16\,X + 72}{74\,X^2 + 79\,X + 49}\,,\ v = \frac{(47\,X^2 + 8\,X + 64)Y + 51\,X^4 + 5\,X^3 + 20\,X^2 + 20\,X + 18}{81\,X^4 + 72\,X^3 + 47\,X^2 + 23\,X + 77}\,.$$

We then apply Tartaglia-Cardan formulae to Eq. (16) in order to obtain x and $y = z - m_3(x)$ as functions of t. Inverting the change of variables in Equation (15) gives a point $(\mathbf{x}, \mathbf{y})$ on the initial curve.

4.6. **The density of target curves.** We prove that the construction in Section 4.3 provides a parameterization for a fixed positive proportion of genus 2 curves over $\mathbb{F}_q$ when q is prime to 6 and large enough. We call $\mathcal{S}$ the set of non-degenerate sextic binary forms with coefficients in $\mathbb{F}_q$. Scalar multiplication

$$(\lambda, m(X_1, X_0)) \mapsto \lambda m(X_1, X_0)$$

defines an action of the multiplicative group $\mathbb{F}_q^*$ on $\mathcal{S}$. The linear group $\mathrm{GL}_2(\mathbb{F}_q)$ also acts on $\mathcal{S}$. Call G the subgroup of $\mathrm{GL}_2(\mathbb{F}_q) \times \mathbb{F}_q^*$ consisting of pairs (γ, λ) where λ is a square. To every non-degenerate sextic binary form $m(X_1, X_0)$ with coefficients in $\mathbb{F}_q$ we associate the $\mathbb{F}_q$-isomorphism class of the curve with equation $y^2 = m(x, 1)$. This defines a surjective map ν from $\mathcal{S}$ onto the set $\mathcal{I}$ of $\mathbb{F}_q$-isomorphism classes of genus 2 curves over $\mathbb{F}_q$. The fibers of ν are the orbites for the action of

G on $\mathcal{S}$. When q tends to infinity, the proportion of forms in $\mathcal{S}$ with non-trivial stabilizer in G tends to zero. So it is equivalent to count isomorphism classes of curves in $\mathcal{I}$ or to count forms in $\mathcal{S}$.

We call $\mathcal{P}$ the set of pairs (m_2, m_3) consisting of a split quadratic form

$$m_2(X_1, X_0) = (aX_1 - bX_0)(cX_1 - dX_0)$$

and a cubic form m_3, such that $m_3^2 - m_2^3$ is a non-degenerate sextic form. The cardinality of $\mathcal{P}$ is $q^7 \times (1/2 + o(1))$ when q tends to infinity. Let $\chi : \mathcal{P} \to \mathcal{S}$ be the map that sends (m_2, m_3) onto $m_3^2 - m_2^3$. According to work by Clebsh [4] and Elkies [6, Theorem 3], fibers of χ have no more than 240 elements. So the image of χ has cardinality at least $q^7 \times (1/480 + o(1))$ and density at least $1/480 + o(1)$.

Theorem 1. *Let q be a prime power that is prime to 6. The proportion of all genus 2 curves over the field with q elements that can be parameterized by 3-radicals is at least $1/480 + \epsilon(q)$ where ϵ tends to zero when q tends to infinity.*

5. Other families of covers

In Sections 3 and 4 we have studied two families of $\mu_3 \rtimes \mu_2$ covers corresponding to $(r_s, r_t) = (2, 2)$ and $(r_s, r_t) = (4, 2)$ respectively. In this section we quickly review a few other possibilities. We also present an interesting family of $\mu_5 \rtimes \mu_2$ covers.

5.1. **The case $(r_s, r_t) = (4, 1)$.** Both B and C have genus 1. The map $B \to E$ is any degree three map having a triple pole. If B is given by a Weierstrass model, then for every scalar t, the function $y + tx$ will do. So we obtain a one parameter family of parameterization of B by elliptic curves C_t. The resolvents C_t form a non-isotrivial family. However, we observed that the 3-torsion group scheme $C_t[3]$ is isomorphic to $B[3]$ for every value of t.

5.2. **The case $(r_s, r_t) = (6, 1)$.** Both B and C have genus 2. The map $B \to E$ is any degree three map having a triple pole. There is one such map for every non-Weierstrass point P on B. We obtain a one parameter family of parameterization of B by genus 2 curves C_P. The resolvents C_P form a non-isotrivial family. However, we observed that the 3-torsion group scheme $J_{C_P}[3]$ is isomorphic to $J_B[3]$ for every $P \in B$.

5.3. **The case $(r_s, r_t) = (8, 1)$.** Both B and C have genus 3. The map $B \to E$ is a degree three map having a triple pole P. This pole is a rational Weierstrass point. The curve C is hyperelliptic. For every genus 3 curve B having a rational Weierstrass point, we thus obtain a parameterization of B by an hyperelliptic curve of genus 2. Conversely, for every hyperelliptic curve of genus 3 which we can parameterize, we obtain a parameterization for a 1-dimensional family of non-hyperelliptic genus 3 curves.

5.4. **Curves with a $\mu_5 \rtimes \mu_2$ action.** This time we assume that the characteristic of K is prime to 10. Let $\zeta_5 \subset \bar{K}$ be a primitive 5-th root of unity. We denote by $\mu_5 \rtimes \mu_2$ the subgroup scheme of $\mathrm{Sym}(\mu_5)$ generated by $x \mapsto x^{-1}$ and $x \mapsto \zeta_5 x$. Let A be a projective, absolutely integral, smooth curve over K. We assume that $\mathrm{Aut}(C \otimes_K \bar{K})$ contains the finite étale K-group scheme $\mu_5 \rtimes \mu_2$. We set $B = A/\mu_2$, and $C = A/\mu_5$. If C admits a parameterization by S-radical as in Equation (1), and if the normalization D' of the fiber product of A and D above C is absolutely integral, then we can construct an $S \cup \{5\}$-parameterization of B just as in Section 2.7. We assume that $E = A/(\mu_5 \rtimes \mu_2)$ has genus 0. Let r_d be the number of branched points with ramification type $2, 2, 1$. Let r_t the number

of branched points with ramification type 5. According to the Hurwitz Genus Formula [19, III.4.12, III.5.1] the genus of B is

$$g_B = r_d + 2r_t - 4.$$

Every branched point of type $2, 2, 1$ of the cover $B \to E$ gives rise to a branched point of type $2, 2, 2, 2, 2$ of the cover $A \to E$ and to a simple branched point of $C \to E$. And every totally branched point of the cover $B \to E$ gives rise to a branched point of type $5, 5$ of the cover $A \to E$ and to a non-branched point of $C \to E$. So

$$g_A = \frac{5r_d}{2} + 4r_t - 9, \quad \text{and} \quad g_C = \frac{r_d}{2} - 1.$$

We still call

$$m = a + b - 3$$

the *modular dimension*. The genericity condition is

$$2r_d + 5r_t \leq 12 - 2\epsilon(r_d + 2r_t - 4),$$

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

An interesting case is when $r_d = 6$ and $r_t = 0$. Then both B and C have genus 2. The map $B \to E$ is a $\mu_5 \rtimes \mu_2$-cover. The cover $A \to C$ is unramified. It is a quotient by μ_5. Associated to it, there is a C_5 inside J_C. So we are just dealing with a genus 2 curve C having a 5-torsion point in its Jacobian. We provide explicit equations for this situation in Section 6.

6. Genus 2 curves with a 5-torsion divisor

We assume that K has characteristic prime to 10. Let C be a genus 2 curve having a K-rational point of order 5 in its Jacobian. We assume that this point is the class of $P_\infty - P_0$ where P_∞ and P_0 are two K-rational points on C. We give explicit equations for C, P_0 and P_∞ depending on rational parameters. In Sections 6.1, 6.2, and 6.3, we distinguish three cases depending on the action of the hyperelliptic involution σ on P_0 and P_∞. We note that these two points cannot be both Weierstrass points. We finally give in Section 6.4 an example of how to combine this construction and the previous ones in order to parameterize more genus 2 curves.

6.1. **A first special case.** We first assume that P_0 is a Weierstrass point. So P_∞ is not. Let x be a degree 2 function having a pole at P_∞ and a zero at P_0. Let y be a function as in Section (4.1). We have $y^2 = f(x)$ for some degree 6 polynomial in $K[x]$. Let $z \in K(C)$ be a function with divisor $5(P_0 - P_\infty)$. We write

$$z = a(x) + yb(x)$$

with $a(x)$ and $b(x)$ in $K(x)$. We deduce from Equations (6), (7), (8), that a and b are polynomials and $\deg(a) \leq 5$ and $\deg(b) \leq 2$. Since z has a pole of order 5 at P_∞ and has valuation 0 at $\sigma(P_\infty)$ we actually know that $\deg(a) = 5$ and $\deg(b) = 2$. Also b is divisible by x exactly twice, and a is divisible by x at least thrice. Multiplying z by a scalar we may ensure that a is unitary. Multiplying y by a scalar we may ensure that $b = x^2$. And $a(x) = x^3(x^2 + kx + l)$ for some k and some l in K. There exists a scalar $w \in K^*$ such that

$$z \times \sigma(z) = wx^5 = x^4(x^2(x^2 + kx + l)^2 - f(x)).$$

So $f(x) = x^2(x^2 + kx + l)^2 - wx$. The curve C has affine equation

$$y^2 = x^2(x^2 + kx + l)^2 - wx,$$

P_∞ is one of the two points at infinity, and P_0 is the point $(0, 0)$. This is essentially the model given by Boxall, Grant and Leprévost [3].

6.2. **Another special case.** We assume now that $\sigma(P_0) = P_\infty$. Let x be a degree two function having poles at P_0 and P_∞. Let y and $f(x)$ be as in Section 4.1. Let z be a function with divisor $5(P_0 - P_\infty)$. We write $z = a(x) + yb(x)$ where a and b are polynomials in x with degrees 5 and 2. Multiplying z by a constant in K we may assume that a is unitary. Multiplying y by a constant in K we may assume that b is unitary. Adding a constant to x we may assume that

$$b(x) = x^2 - k$$

for some $k \in K$. There is a scalar $w \in K^*$ such that

$$z \times \sigma(z) = w = a^2 - fb^2.$$

So w is a square in the algebra $K[x]/b(x)$. This leaves two possibilities. Either $w = W^2$ for some $W \in K^*$ and $a(x) = W \bmod b(x)$, or $w = W^2 k$ for some $W \in K^*$ and $a(x) = Wx \bmod b(x)$. We study these two subcases successively.

6.2.1. *If $w = W^2$ and $a(x) = W \bmod b(x)$.* We check that

$$a(x) = W \bmod b(x)^2$$

indeed. Since a is unitary, there exists a scalar $j \in K$ such that $a = W + (x + j)b^2$. We deduce expressions for a, b and f in the parameters k, W, and j. The actual dimension of the family is 2 because we may multiply x by a scalar.

6.2.2. *If $w = W^2 k$ and $a(x) = Wx \bmod b(x)$.* In particular k is not 0. We check that $a(x) = Wx + a_1(x)b(x) \bmod b(x)^2$ with $a_1(x) = -Wx/(2k)$. So there exist a scalar $j \in K$ such that

$$a = Wx - Wxb(x)/(2k) + (x + j)b(x)^2.$$

We deduce expressions for a, b and f in the parameters k, W, and j. The actual dimension of the family is 2 again.

6.3. **Generic case.** We assume that none of P_0 and P_∞ is a Weierstrass point and $\sigma(P_0) \neq P_\infty$. Let x be a degree 2 function having a zero at P_0 and a pole at P_∞. Let y be a function as in Section 4.1. We have $y^2 = f(x)$ where $f \in K[x]$ is a degree 6 polynomial. Both $f(0)$ and the leading coefficient of f are squares in K. Let $z \in K(C)$ be a function with divisor $5(P_0 - P_\infty)$. We write

$$z = a(x) + yb(x)$$

with $a(x)$ and $b(x)$ in $K(x)$. We deduce from Equations (6), (7), (8), that a and b are polynomials and $\deg(a) \leq 5$ and $\deg(b) \leq 2$. Since z has a pole of order 5 at P_∞ and has valuation 0 at $\sigma(P_\infty)$ we actually know that $\deg(a) = 5$ and $\deg(b) = 2$. Multiplying z by a scalar, we may ensure that a is unitary. Multiplying y by a scalar, we may ensure that b is unitary. Since z has a zero of order 5 at P_0 and has valuation 0 at $\sigma(P_0)$ we know that $a(0) \neq 0$ and $b(0) \neq 0$.

The three polynomials $a(x)$, $b(x)$, and $f(x)$ are related by the equation

$$a^2 - fb^2 = wx^5$$

for some $w \in K^*$. In particular, wx is a square modulo $b(x)$. We can easily deduce that

$$b(x) = x^2 + (2k - wl^2)x + k^2$$

for some k and l in K^*. A square root of wx modulo $b(x)$ is then $(k + x)/l$. A square root of wx^5 modulo b is then

$$a_0(x) = \frac{(k^2 - 3kwl^2 + w^2l^4)x + (k - wl^2)k^2}{l}.$$

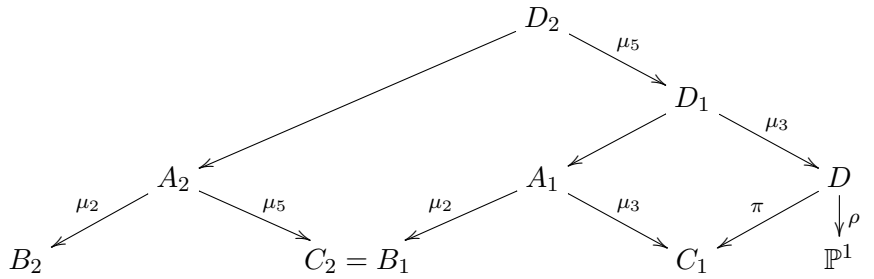


FIGURE 1. Composing parameterizations.

Using Hensel's lemma we deduce that a is the square root of wx^5 modulo b^2 of the form $a_0 + a_1 b$ with

$$a_1(x) = \frac{k^2 - 2wkl^2 + 2w^2l^4 + x(wl^2 + k)}{2wl^3}.$$

So there exists $j \in K$ such that $a = a_0 + a_1 b + a_2 b^2$ with

$$a_2(x) = x + j.$$

We deduce the expressions for a, b and $f = (a^2 - x^5)/b^2$ in the parameters j, k, l, w.

6.4. **An example.** Let K be a field with 83 elements. We set $w = 1$, $j = 2$, $k = 3$, $l = 14$ and find $a(x) = x^5 + 37x^4 + 78x^3 + 18x^2 + 26x + 29$ and $b(x) = x^2 + 59x + 9$, and

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

The curve C with equation $y^2 = f(x)$ has genus 2. Its Jacobian has $3.5.7.71$ points over K. We set $z = a(x) + yb(x)$ and define a cyclic unramified covering A of C by setting $t^5 = z$. We lift the action of the hyperelliptic involution σ onto A by setting $\sigma(t) = x/t$. The function $u = t + x/t$ is invariant by σ. The field $K(u, x)$ is the function field of the quotient curve $B = A/\sigma$. A singular plane model for B is given by the equation

$$u^5 + 78xu^3 + 5x^2u = 2a(x) = 2(x^5 + 37x^4 + 78x^3 + 18x^2 + 26x + 29).$$

Note the Tchebychev polynomial on the left hand side. The Jacobian of B has 5.37^2 points over K. In particular, its 3-torsion is trivial. However we can parameterize the curve B using the parameterization of C constructed in Section 4.5. Note that C appears in Section 4.5 under the name B.

6.5. **Composing parameterizations.** In Section 6.4 we parameterize a genus 2 curve (call it B_2) by another genus 2 curve (call it C_2), using a $\mu_5 \rtimes \mu_2$ action on some curve A_2. In Section 4.5 we had constructed a parameterization of $C_2 = B_1$ by a genus one curve (call it C_1) using a $\mu_3 \rtimes \mu_2$ action on some curve A_1. This C_1 can be parameterized e.g. using Icart's parameterization. Composing the three parameterizations we obtain a parameterization of B_2 by $\mathbb{P}^1$.

This situation is represented on Figure (6.5). The curve D_1 is the fiber product of D and A_1 over C_1. The curve D_2 is the fiber product of D_1 and A_2 over C_2. We can prove that D_1 and D_2 are absolutely irreducible by observing that all down left arrows have degree a power of two, while all down right arrows are Galois of odd degree. The interest of this construction is that, the Jacobian of B_2 having trivial 3-torsion, we reach a curve that was inaccessible before. We may compose again and again e.g. with parameterizations as in Section 5.2. It is natural to ask if we can reach that way all genus 2 curves over a large enough finite field or cardinality q when q is prime to 30. Answering

this question requires to study some morphisms from a moduli space of covers to the moduli space of genus 2 curves : proving in particular that the morphism is surjective and that the geometric fibers are absolutely irreducible.

REFERENCES

[1] O. Bolza. On Binary Sextics with Linear Transformations into Themselves. *Amer. J. Math.*, 10(1):47–70, 1887.

[2] D. Boneh and M. Franklin. Identity-Based Encryption from the Weil Pairing. In Joe Kilian, editor, *Advances in Cryptology – CRYPTO ' 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer-Verlag, Berlin Germany, 2001.

[3] J. Boxall, D. Grant, and F. Leprévost. 5-torsion points on curves of genus 2. *J. London Math. Soc. (2)*, 64(1):29–43, 2001.

[4] A. Clebsch. Zur theorie der binären formen sechster ordnung und zur dreitheilung a der hyperelliptischen funktionen. *Abh. der k. Ges. Wiss. zu Göttingen*, 14:17–75, 1869.

[5] J.-M. Couveignes and J.-G. Kammerer. The geometry of flex tangents to a cubic curve and its parameterizations. *J. Symb. Comput.*, 47(3):266–281, 2012.

[6] N. Elkies. The identification of three moduli spaces, 1999.

[7] R. R. Farashahi. Hashing into Hessian Curves. In *AFRICACRYPT*, pages 278–289, 2011.

[8] P.-A. Fouque and M. Tibouchi. Deterministic Encoding and Hashing to Odd Hyperelliptic Curves. In Marc Joye, Atsuko Miyaji, and Akira Otsuka, editors, *Pairing-Based Cryptography - Pairing 2010 - 4th International Conference, Yamanaka Hot Spring, Japan, December 2010. Proceedings*, volume 6487 of *Lecture Notes in Computer Science*, pages 265–277. Springer, 2010.

[9] M. Fried. Combinatorial computation of moduli dimension of Nielsen classes of covers. Graphs and algorithms, Proc. Conf., Boulder/CO 1987, Contemp. Math. 89, 61-79, 1989.

[10] M. Harrison. Explicit solution by radicals, gonal maps and plane models of algebraic curves of genus 5 or 6. *Journal of Symbolic Computation*, 51:3–21, April 2013.

[11] T. Icart. How to Hash into Elliptic Curves. In *CRYPTO*, pages 303–316, 2009.

[12] J.-I. Igusa. Arithmetic variety of moduli for genus two. *Ann. of Math. (2)*, 72:612–649, 1960.

[13] J.-G. Kammerer, R. Lercier, and G. Renault. Encoding Points on Hyperelliptic Curves over Finite Fields in Deterministic Polynomial Time. In *Pairing*, pages 278–297, 2010.

[14] S. Lang. *Algebra*. Springer, 2002.

[15] R. Lercier, C. Ritzenthaler, and J. Sijsling. Fast computation of isomorphisms of hyperelliptic curves and explicit descent. In E. W. Howe and K. S. Kedlaya, editors, *ANTS X — Proceedings of the Tenth Algorithmic Number Theory Symposium*, volume 1 of *The Open Book Series*, pages 463–486. Mathematical Sciences Publishers, 2013.

[16] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften (Fundamental Principles of Mathematical Sciences)*. Springer-Verlag, Berlin, 2000.

[17] G. Salmon. Lessons introductory to the modern higher algebra, 1885.

[18] A. Shallue and C. 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.

[19] H. Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[20] M. Ulas. Rational points on certain hyperelliptic curves over finite fields. *Bull. Polish Acad. Sci. Math.*, 55(2):97–104, 2007.

JEAN-MARC COUVEIGNES, UNIV. BORDEAUX, IMB, UMR 5251, F-33400 TALENCE, FRANCE.

JEAN-MARC COUVEIGNES, CNRS, IMB, UMR 5251, F-33400 TALENCE, FRANCE.

JEAN-MARC COUVEIGNES, INRIA, F-33400 TALENCE, FRANCE.
Email address: Jean-Marc.Couveignes@math.u-bordeaux1.fr

REYNALD LERCIER, DGA MI, LA ROCHE MARGUERITE, 35174 BRUZ, FRANCE.

REYNALD LERCIER, INSTITUT DE RECHERCHE MATHÉMATIQUE DE RENNES, UNIVERSITÉ DE RENNES 1, CAMPUS DE BEAULIEU, 35042 RENNES, FRANCE.
Email address: reynald.lercier@m4x.org