Bisection for genus 2 curves with a real model *

Josep M. Miret Jordi Pujolàs Nicolas Thériault

Abstract

Integer multiplication in Jacobians of genus 2 curves over a finite field $\mathbb{F}_q$ is a fundamental operation for hyperelliptic curve cryptography. Algorithmically, the result of this operation is given by the very well known algorithms of Cantor. One method to reverse duplication in these cases consists in associating, to every preimage of the desired doubled divisor defined over $\mathbb{F}_q$, a root in $\mathbb{F}_q$ of the so called bisection polynomial. We generalize this approach to genus 2 curves with two points at infinity, both in even and odd characteristics. We attach a bisection polynomial to each possible type of Mumford coordinate, we show the factorization of these in terms of Galois orbits in the set of bisections, and we compare the efficiency of our approach versus brute-force adaptations of the existing methods to our setting.

1 Introduction

The state of the art for reversing the multiplication-by-two map in the group of points $\mathrm{Jac}(C)(\mathbb{F}_q)$ of Jacobians of genus 2 curves over finite fields can be found in [10]. In there the very particular properties that multiplication-by-2 acquires in the Kummer surface of C are exploited to find preimages by essentially computing 4 square roots (with a few other basic field operations). This is the most efficient algorithm currently available. Previously methods (see [9] for example) consisted in finding the roots of certain degree 16 polynomial obtained after a Gröbner basis computation.

*Research of the authors was supported in part by grants MTM2013-46949-P (Spanish Ministerio de Ciencia e Innovación), 2014SGR-1666 (Generalitat de Catalunya), FONDECYT 1110578 and Anillo ACT56 (Chile)

Received by the editors in May 2014.

Communicated by M. Van den Bergh.

2010 *Mathematics Subject Classification :* 11Y40, 11G20, 14H45, 11T71, 14G50.

Key words and phrases : Halving algorithm, genus 2 curves, real model, finite fields.

In this paper we extend the works [13, 14] (see also [2, 3]) on curves of genus 2 with an imaginary model, to curves of genus 2 with a real model over a finite field $\mathbb{F}_q$ of any characteristic. In them it is shown how to reverse the multiplication-by-two map by finding the roots of an explicit polynomial of degree 16 (thus avoiding the Gröbner computations). The main advantage of this approach is its potential generalization to find preimages of multiplication-by-n for other (small) values of n.

Certainly, if a curve in the real model admits an imaginary model then our purpose can be accomplished with [13, 14]. However, only hyperelliptic curves with at least one rational Weierstrass point admit imaginary models over the same base field. Our work in the present paper covers the cases without a rational Weierstrass point over the base field. Without our approach, the only alternative left would be to lift the curve to an extension of the base field where an isomorphism to an imaginary model exists (it is sufficient to take an extension of degree 2, 3 or 6), and perform the halving computations there. The same applies when using the Kummer surface, although in this case the field extension must contain all the Weierstrass points. Nevertheless, the increased computational complexity due to the lifting makes this alternative more costly than ours. We provide evidence of the efficiency gain of our method with two examples over fields of sizes 100 and 400 bits.

The plan of the paper is the following. We first survey how to represent divisors in Jacobians of curves with a real model, including those for which the standard Mumford representation is not available. In Section 3 we explain how to construct the *bisection polynomials* that reverse multiplication-by-2. In Section 4 we show how these polynomials factor, using the Frobenius endomorphism. In Section 5 we show some examples, and in the last section we illustrate the efficiency gains of using our polynomials compared to the obvious adaptation of those in [14].

2 Generalities

For us C is a genus 2 curve over a finite field $\mathbb{F}_q$ split at infinity. Therefore C has two different points ∞_1, ∞_2 above the infinity point of the singular model, both defined over $\mathbb{F}_q$ or else quadratic-conjugate, which are permuted by the hyperelliptic involution. Under this assumption, C has a *real* model

$$\mathrm{C} : y^2 + h(x)y = f(x),$$

where $f(x) = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0 \in \mathbb{F}_q[x]$ is a separable sextic and $h(x) = 0$ if q is odd, and where $\deg(f) \leq 6$ and $h(x) = x^3 + h_2x^2 + h_1x + h_0 \in \mathbb{F}_q[x]$ if q is even. The points at infinity are defined over $\mathbb{F}_q$ when f_6 is a square a^2 in odd characteristic or it is of the form $a^2 + a, a \in \mathbb{F}_q$, in even characteristic. We choose the root a to be associated to ∞_1. Then ∞_2 will be associated to the root $-a$ in odd characteristic or $a + 1$ in even characteristic.

We now recall the coordinates $(u(x), v(x))$ of a degree 0 divisor class in the Jacobian of a genus 2 curve with a real model both in odd and even characteristics. More details can be found in [7, 8, 12, 15]. We follow the representation by

Galbraith, Harrison and Mireles [8] since it is the one used in Magma [4, Handbook, Section "Points on the Jacobian"], which we use for our practical examples. The only difference is that Magma specifies the weight of the divisor while we do not need to. In particular, we can assume that efficient group addition operations are readily available. Also, following the divisor representation in [8], divisors of weight 2 are always balanced at infinity for us, in the sense that their non-affine support is $\infty_2 + \infty_1$.

Consider first the cases with the two points at infinity are defined over $\mathbb{F}_q$. It is well known that the points at infinity are represented using the Puiseux series in x^{-1} of y (see [11] for example), where the leading term (in x) corresponds to the root associated to either ∞_1 or ∞_2. In odd characteristic ∞_1 is represented by $ax^3 + \frac{f_5}{2a}x^2 + \sum_{i=-1}^{\infty} a_i x^{-i}$ and in even characteristic by $ax^3 + (ah_2 + f_5)x^2 + \sum_{i=-1}^{\infty} a_i x^{-i}$.

Since all affine-reduced divisors can be written as the sum of a balanced affine-reduced divisor with a number of copies of the divisor $\infty_2 - \infty_1$, we can restrict ourselves to working with divisors of the following forms:

- Balanced affine-supported divisors of weight two $P_1 + P_2 - (\infty_1 + \infty_2)$ are given the Mumford representation $(x^2 + u_1 x + u_0, v_1 x + v_0)$.
- Affine-supported divisors of weight one $P_1 - \infty_1$ (resp. $P_1 - \infty_2$) are given the representation $(x - x_1, ax^3 + v_0)$ with $v_0 = y_1 - ax_1^3$ (resp. replace a with $-a$).
- Infinity-supported divisors $\infty_2 - \infty_1$ and $\infty_1 - \infty_2$ (from now on "weight zero divisors") are represented in odd characteristic by

$$(1, \pm(ax^3 + \frac{f_5}{2a}x^2))$$

  and in even characteristic by

$$(1, ax^3 + (f_5 + ah_2)x^2),\ (1, (a+1)x^3 + (f_5 + (a+1)h_2)x^2).$$

When the points at infinity are not defined over $\mathbb{F}_q$, they are Galois conjugates, and therefore only balanced divisors can be $\mathbb{F}_q$-rational. In terms of reduced divisors, this means that all non-zero reduced divisors are balanced, affine-supported of weight 2, so of the form $P_1 + P_2 - (\infty_1 + \infty_2)$, and therefore all divisors are given the Mumford representation.

Since our halving algorithm takes balanced, affine-reduced divisors or $\pm(\infty_2 - \infty_1)$, and returns divisors of these same types, for us unbalanced divisors are not a problem. On the other hand, the 2-torsion divisors are of the form $P_i + P_j - (\infty_1 + \infty_2)$ where $\{P_i, P_j\}$ is a pair of Weierstrass points fixed (as a pair) under the Frobenius. It is well known [14, pg. 56, Prop. 1] that the rank of $\mathrm{Jac}(C)(\mathbb{F}_q)[2^\infty]$ depends on the $\mathbb{F}_q$-factorisation of the hyperelliptic polynomials as shown in Table 1 (we indicate the degrees of the irreducible factors, and use exponents for the repeated factors in even characteristic).

We see that the 2-rank of curves without an imaginary model is at most 2 in odd characteristic, and always 0 in even characteristic.

Table 1: 2-ranks for curves with a real model.

odd characteristic	
factorisation types of $f(x)$	2-rank
$[6],\ [1,5],\ [3,3]$	0
$[2,4],\ [1,2,3],\ [1,1,4]$	1
$[2,2,2],\ [1,1,2,2],\ [1,1,1,3]$	2
$[1,1,1,1,2]$	3
$[1,1,1,1,1,1]$	4

even characteristic	
factorisation types of $h(x)$	2-rank
$[3],\ [1^3]$	0
$[1,2],\ [1,1^2]$	1
$[1,1,1]$	2

3 Bisection in real models

For the rest of the paper, we use the notation

$$\frac{1}{2}D_2 := \{D_1 \in \mathrm{Jac(C)}(\mathbb{F}_q) \mid 2D_1 = D_2\}$$

and $D_i = (x^2 + u_{i1}x + u_{i0}, v_{i1}x + v_{i0})$, $D_i = (x + u_{i0}, v_{i0})$, etc. for $i = 1, 2$. We call the D_1's in $\frac{1}{2}D_2$ the *bisections* of the given D_2, and the divisor D_2 to bisect the *bisectee*. It is clear that two different bisections of the same bisectee differ by a divisor of order 2. Our goal is to provide an algorithm to find the bisections of generic bisectees for genus 2 curves with a real model.

3.1 Bisections of weight 1 and bisections of weight 0

We consider the generic case of weight 2 bisections in the next section. Here we show that if any given bisectee D_2 of any weight 0, 1 or 2 has a weight 1 bisection or a weight 0 bisection, then such bisections are found by extracting a square root.

Assume first that D_2 has weight 1 or 2, and that $\infty_1 - \infty_2$ exists – otherwise there are no weight 1 divisors at all in $\mathrm{Jac}(C)(\mathbb{F}_q)$. If $2D_1 = D_2$ with $D_1 = P_1 - \infty_1$ (the same argument works if we take $D_1 = P_1 - \infty_2$), and say $P_1 = (x_1, y_1) \in \mathrm{C}(\mathbb{F}_q)$, then $D_2 = 2P_1 - 2\infty_1$. Therefore, since D_2 is not $\infty_2 - \infty_1$, then

$$D_2 + (\infty_1 - \infty_2) = 2P_1 - (\infty_1 + \infty_2)$$

is a non-zero divisor in the balanced representation form. In this case, $P_1 - \infty_1 = (x - x_1, ax^3 + (y_1 - ax_1^3))$ belongs to $\frac{1}{2}D_2$, and from the algorithmic point of view, such bisections are easy to find: since the doubling algorithm squares the first coordinate $x - x_1$ [6, pg. 319], one only needs to check whether the first coordinate of $D_2 \pm (\infty_1 - \infty_2)$ is a square or not. If it is, then the first coordinate of D_1 is the

square root and we are done (the other bisections are obtained by adding the divisors of order 2). If $D_2 - (\infty_1 - \infty_2) = 2P_1 - (\infty_1 + \infty_2)$, then $P_1 - \infty_2 \in \frac{1}{2}D_2$ and the argument works symmetrically.

For weight 1 bisections of weight 0 bisectees we have the following result.

Proposition 1. *Let* $P_i \in \mathrm{C}(\mathbb{F}_q)$. *Then* $P_i - \infty_1 \in \frac{1}{2}(\infty_2 - \infty_1)$ *and* $P_i - \infty_2 \in \frac{1}{2}(\infty_1 - \infty_2)$ *if and only if* P_i *is a Weierstrass point of* C.

Proof. Put $x_i = x(P_i)$. For $P_i - \infty_1$ we have

$$2(P_i - \infty_1) = (2P_i - \infty_1 - \infty_2) + (\infty_2 - \infty_1),$$

and this is equal to $\infty_2 - \infty_1$ if and only if

$$2P_i - \infty_1 - \infty_2 = div(x - x_i),$$

which is true if and only if P_i is a Weierstrass point. The same holds for $P_i - \infty_2$. ∎

In chasing weight 0 bisections, the situation is even more straightforward. Checking whether $D_2 = \pm 2(\infty_1 - \infty_2)$ is naturally done as above: if one of $D_2 \pm (\infty_1 - \infty_2)$ is $\mp(\infty_1 - \infty_2)$ (with the sign reversed), then D_2 admits $\mp(\infty_1 - \infty_2)$ as a bisection, and all other bisections are obtained by adding the divisors of order 2.

3.2 Weight two bisections

In this section we show how to attach, to any given bisectee $D_2 \in \mathrm{Jac}(\mathrm{C})(\mathbb{F}_q)$, a polynomial

$$p_{D_2}(x) = \sum_{i=0}^{\#\mathrm{Jac}(\mathrm{C})(\mathbb{F}_q)[2]} c_i x^i \in \mathbb{F}_q[x],$$

whose roots allow to build up the first coordinate of the weight 2 bisections in $\frac{1}{2}D_2$. We call this polynomial the *bisection polynomial* of D_2.

The coefficients c_i are functions $c_i(f_6, \ldots, f_0, h_2, \ldots, h_0, u_{21}, u_{20}, v_{21}, v_{20})$ of the coefficients of the curve and of the coordinates of the bisectee D_2, and give values in the base field $\mathbb{F}_q$. They are different if the weight of the bisectee D_2 is 2, 1 or 0. We reflect the structure of the support of the bisectee in the bisection polynomial by writing $p_{w_2}(x)$, $p_{w_1}(x)$, $p_{w_0}(x)$ accordingly.

Although completely analogous to the case of genus 2 curves with an imaginary model (see [14]), we recall the general method. In order to obtain the bisection polynomial, the idea is to "reverse" the reduction step in Cantor's addition algorithm [5] (see also [6, pg. 308]). In the reduction part of this algorithm, the transformation of the "unreduced coordinates" $(u_2'(x), v_2'(x))$ into a *reduced* divisor $D_2 = (u_2(x), v_2(x))$ consists in the operations

$$u_2(x) = \frac{f(x) - v_2'(x)h(x) - v_2'(x)^2}{u_2'(x)}, \quad v_2(x) = -(h(x) + v_2'(x)) \bmod u_2(x).$$

We say "to dereduce" for describing the use of an auxiliary polynomial $k(x) = k_1 x + k_0$ (as first appeared in [13]) to equate the dashed coordinates in the reduction equalities above:

$$v_2'(x) = -(h(x) + v_2(x)) + k(x)u_2(x), \quad u_2'(x) = \frac{f(x) - v_2'(x)h(x) - v_2'(x)^2}{u_2(x)}.$$

In the next paragraphs we refer to a *dereduced* divisor of a given divisor D to mean "a divisor D' in the same divisor class of D, dereduced with $k(x)$". Our goal is to find a particular $k(x)$ that fits the reversion of the multiply-by-2 map.

From the doubling algorithm [6, pg. 319], we see that $2D_1 = D_2$ clearly implies the equality between the first coordinate $u_2'(x)$ of the dereduced divisor of the bisectee D_2, and the square of the first coordinate $u_1(x)$ of D_1:

$$u_1(x)^2 = u_2'(x). \tag{1}$$

Since we are searching for weight 2 bisections, in the remaining the left hand side of (1) is of the form

$$u_1(x)^2 = x^4 + 2u_{11}x^3 + (2u_{10} + u_{11}^2)x^2 + 2u_{10}u_{11}x + u_{10}^2,$$

and the right hand side is the quotient of a sextic by a quadratic polynomial. The actual quotient depends on the different possibilities for the polynomials that define the coordinates of the bisectee D_2, which we surveyed in Section 2. The equality (1) is obtained by making the resulting quartic monic.

Equating u_{11} and u_{10} from the terms of degree 3 and 2 in $u_2'(x)$ respectively one obtains expressions in terms of k_0 and k_1. Replacing these expressions for u_{11} and u_{10} into the monomials of degree 1 and 0 and eliminating the denominators, we find two bivariate polynomials $s_1(k_0, k_1), s_2(k_0, k_1)$ which share a non-constant factor. The resultant of s_1 and s_2 with respect to k_0,

$$p_{w_2}(x) = Res_{k_0}(s_1(k_0, x), s_2(k_0, x)),$$

is a degree 16 univariate polynomial whose $\mathbb{F}_q$-rational roots are the values of k_1 we are searching for. This is how some coefficients c_i of $p_{w_2}(x)$ look like for bisectees of weight 2 and curves with $f_5 = f_3 = 0$:

$$\begin{aligned}
c_0 &= -65536(4u_{20} - u_{21}^2)^6, \\
c_1 &= 1048576(4u_{20} - u_{21}^2)^5 v_{21}, \\
c_2 &= -524288(4u_{20} - u_{21}^2)^4(8f_2 - 8f_4u_{20} + 14f_4u_{21}^2 - 30u_{20}u_{21}^2 + 15u_{21}^4), \\
&\vdots
\end{aligned}$$

$$
\begin{aligned}
c_{16} = & -268435456\left(-4f_2+(f_4-u_{20})(f_4+3u_{20})+4v_{21}^2\right)v_{21}^4-49807360(8f_4-51u_{20})u_{21}^{10}\\
&+536870912(f_4-3u_{20})v_{20}v_{21}^3u_{21}+8388608(717u_{20}-263f_4)v_{21}^2u_{21}^6\\
&+134217728\left((f_4-3u_{20})(-15f_2+4f_4^2+6f_4u_{20}-9u_{20}^2)+2(10f_4-33u_{20})v_{21}^2\right)v_{21}^2u_{21}^2\\
&+134217728\left(-27\left(f_2+u_{20}(-2f_4+3u_{20})\right)+32v_{21}^2\right)v_{20}v_{21}u_{21}^3-4152360960v_{20}v_{21}u_{21}^7\\
&-8388608\left((8f_4-51u_{20})(9f_2-4f_4^2+6f_4u_{20}-9u_{20}^2)+270v_{20}^2\right)u_{21}^6-591462400u_{21}^{12}\\
&-3145728(570f_2-232f_4^2+108f_4u_{20}+297u_{20}^2-60v_{21}^2)u_{21}^8\\
&-16777216\left(81f_2^2+16f_4^4-48f_4^3u_{20}+81(u_{20}^4-4u_{20}v_{20}^2)+1134u_{20}^2v_{21}^2-88v_{21}^4\right)u_{21}^4\\
&-301989888\left((14f_4-51u_{20})v_{20}v_{21}u_{21}-f_4(6u_{20}^3-6v_{20}^2+37u_{20}v_{21}^2)\right)u_{21}^4\\
&+16777216\left(6f_2(12f_4^2-18f_4u_{20}+27u_{20}^2+8v_{21}^2)-4f_4^2(27u_{20}^2+28v_{21}^2)\right)u_{21}^4
\end{aligned}
$$

The procedure is completely analogous for obtaining $p_{w_1}(x)$ (of degree 16) and $p_{w_0}(x)$ (of degree 10). It is noticeable that none of the bisection polynomials depend on the coefficients f_1, f_0.

In even characteristic the maximum number of bisections of a given bisectee is 4. Since $u_1(x)^2 = x^4 + u_{11}^2x^2 + u_{10}^2$, equating the linear and cubic terms with $u_2'(x)$ one readily obtains a closed formula for k_0 in terms of k_1, and for k_1 the analogous $p_{w_2}(x)$, $p_{w_1}(x)$ (of degree 4), and $p_{w_0}(x)$ (linear). This is how they look:

$$
\begin{aligned}
p_{w_2}(x) = & \, u_{21}^3x^4+u_{21}(h_1+h_2^2)x^2+(h_0+h_1h_2)x+(h_2+u_{21})v_{21}+v_{20}\\
&+f_3+f_4u_{21}+f_5(h_1+u_{20}+u_{21}(f_5+u_{21}))\\
&+f_6u_{21}(h_1+(f_6+1)u_{21}^2),
\end{aligned}
$$

$$
\begin{aligned}
p_{w_1}(x) = & \, x^4+(h_1+h_2^2)x^2+(h_0+h_1h_2)x+au_{20}(h_0+h_1h_2+h_2u_{20}^2)\\
&+a^2u_{20}^2(h_1+h_2^2)+(h_0+h_1h_2)v_{20}+f_2+f_3u_{20}\\
&+f_4(f_4+h_1+u_{20}^2)+f_5u_{20}(f_5u_{20}+h_1+u_{20}^2)+f_6h_1(h_1+u_{20}^2),
\end{aligned}
$$

$$
p_{w_0}(x) = x-\Big(\frac{f_1+h_1(f_3+ah_0+f_5h_1+ah_1h_2)}{h_1h_2+h_0}\Big).
$$

4 Factorization of the bisection polynomials

In this section we relate the possible factorisations of $p_{w_1}(x)$, $p_{w_2}(x)$ and $p_{w_0}(x)$ with the factorisations of $f(x)$ and $h(x)$. We are able to factor the bisection polynomials because of the correspondence between factors of $p_{w_i}(x)$ defined over the base field and Galois orbits of bisections.

4.1 Odd characteristic

By construction, whenever our method finds a pair of values (k_0, k_1), we have a bisection. For instance, if $p_{w_i}(x)$ has a linear simple factor $x - k_1$, then k_0 is a root of a degree 1 factor of $\gcd(s_1(x, k_1), s_2(x, k_1))$. Therefore multiplicity 1 linear factors of $p_{w_i}(x)$ have always a corresponding bisection, and we say we have a *successful* factorisation of $p_{w_i}(x)$.

However, there is not always a bijection between the roots of $p_{w_i}(x)$ and the set of bisections. Indeed, the bijection fails for certain multiple roots of $p_{w_i}(x)$. By definition of resultant, the degree of $\gcd(s_1(x, k_1), s_2(x, k_1))$ is in fact the multiplicity of k_1 as a root of $p_{w_i}(x)$. It can therefore happen that $p_{w_i}(x)$ contains some factors with multiplicity $2, 3$ or 4. This corresponds to $\gcd(s_1(x, k_1), s_2(x, k_1))$ of degree $2, 3$ or 4. When such a gcd has 2, 3 or 4 roots in $\mathbb{F}_q$, we have 2, 3 or 4 different sets of pairs (k_0, k_1), and the corresponding set of bisections. In these cases we say we have a *successful* factorisation of $p_{w_i}(x)$ as well. On the contrary, even if $p_{w_i}(x)$ does actually have a root over $\mathbb{F}_q$, if $\gcd(s_1(x, k_1), s_2(x, k_1))$ does not have a linear factor we consider the factorisation of $p_{w_i}(x)$ to be *unsuccessful*.

The case of pairs (k_1, k_0) of multiplicity greater than 1 as a pair do have a geometric interpretation: they correspond to the divisors of order 4.

For simplicity, in Theorem 1 below we consider the factorisation of $p_{w_i}(x)$ to be that of the full factorisation for pairs (k_0, k_1). For instance, a double $\mathbb{F}_q$-rational root k_1 that gives rise to an irreducible gcd of degree 2, will be considered a degree 2 irreducible factorisation of $p_{w_i}(x)$ over $\mathbb{F}_q$, and labeled as "unsuccessful factorisation" in the table of Theorem 1. Also, in accordance to this, a double $\mathbb{F}_q$-rational root k_1 which gives rise to a gcd that factors into 2 distinct linear factors, we will label as a successful factorisation of type $[1, 1]$ and not $[1^2]$. This notation aims to distinguish between the roots of $p_{w_i}(x)$ that lead to bisections (over $\mathbb{F}_q$) from those that do not (unless we go to an extension of $\mathbb{F}_q$).

Factors that appear multiple times in the factorisation of $p_{w_i}(x)$ can then be equivalent to $[1, 1]$ or $[2]$ (for a factor of $p_{w_i}(x)$ of type $[1^2]$), $[1, 1, 1]$, $[1, 2]$ or $[3]$ (for a factor of $p_{w_i}(x)$ of type $[1^3]$), $[1, 1, 1, 1]$, $[1, 1, 2]$, $[1, 3]$, $[2, 2]$, or $[4]$ (for a factor of $p_{w_i}(x)$ of type $[1^4]$), $[2, 2]$ or $[4]$ (for a factor of $p_{w_i}(x)$ of type $[2^2]$), $[2, 2, 2]$, $[2, 4]$ or $[6]$ (for a factor of $p_{w_i}(x)$ of type $[2^3]$) etc., depending on the factorisation of the gcd polynomial for k_0.

Theorem 1. *The degrees of the irreducible factors of $p_{w_1}(x)$ and $p_{w_2}(x)$ depend on the degrees of the irreducible factors of $f(x)$ as follows:*

$f(x)$	$p_{w_i}(x), i = 1, 2$ *successful factorisations*	*unsuccessful factorisations*
$[2,2,2]$	$[1,1,1,1,2,...,2]$	$[4,4,4,4]$
$[2,4]$	$[1,1,2,4,4,4]$	$[8,8]$
$[3,3]$	$[1,3,3,3,3,3]$	
$[6]$	$[1,3,6,6]$	
$[1,1,1,1,1,1]$	$[1,1,...,1]$	$[2,...,2]$
$[1,1,1,1,2]$	$[1,...,1,2,2,2,2]$	$[2,...,2], [4,4,4,4]$
$[1,1,1,3]$	$[1,1,1,1,3,3,3,3]$	$[2,2,6,6]$
$[1,1,2,2]$	$[1,1,1,1,2,...,2]$	$[4,4,4,4]$
$[1,2,3]$	$[1,1,2,3,3,6]$	$[4,12]$
$[1,1,4]$	$[1,1,2,4,4,4]$	$[8,8]$
$[1,5]$	$[1,5,5,5]$	

Proof. The curves for which there exists an isomorphic imaginary model are dealt with in [14] (we include them for completeness). It remains to deal with the first four factorisation types of $f(x)$. Since the Frobenius automorphism π commutes with the multiplication-by-two map, the Galois action in the preimage $\frac{1}{2}D_2$ is given by addition of the elements in $\mathrm{Jac(C)}(\overline{\mathbb{F}}_q)[2]$. In order to factor $p_{w_2}(x)$ and $p_{w_1}(x)$, the goal is to find Galois orbits in $\frac{1}{2}D_2$. There is a bijection between the Galois orbits and the factors of $p_{w_2}(x)$ and $p_{w_1}(x)$.

The full 2-torsion group of the curve C (over $\overline{\mathbb{F}}_q$) is given by the set of 15 pairs of Weierstrass points $\{P_i, P_j\}$ (which is associated to the divisor $P_i + P_j - (\infty_1 + \infty_2)$) with the divisor 0. Note that when computing sums of divisors of order 2, one must keep in mind that the sum of the 6 Weierstrass points $-3(\infty_1 + \infty_2)$ is a divisor in the class 0. Given a specific set of Weierstrass points, we define a basis for $\mathrm{Jac(C)}(\overline{\mathbb{F}}_q)[2]$ that keeps the matrix representing the effect of the Frobenius as "simple" as possible.

Table 2: Basis of the 2-torsion group depending on the factorization of $f(x)$.

$f(x)$	Weierstrass points	W_1	W_2	W_3	W_4
$[2,2,2]$	$\{P, P^\pi, Q, Q^\pi, R, R^\pi\}$	$\{P, P^\pi\}$	$\{Q, Q^\pi\}$	$\{P, Q\}$	$\{P, R\}$
$[2,4]$	$\{P, P^\pi, Q, Q^\pi, Q^{\pi^2}, Q^{\pi^3}\}$	$\{P, P^\pi\}$	$\{Q, Q^{\pi^2}\}$	$\{Q, Q^\pi\}$	$\{P, Q\}$
$[3,3]$	$\{P, P^\pi, P^{\pi^2}, Q, Q^\pi, Q^{\pi^2}\}$	$\{P, P^\pi\}$	$\{P^\pi, P^{\pi^2}\}$	$\{Q, Q^\pi\}$	$\{Q^\pi, Q^{\pi^2}\}$
$[6]$	$\{P, P^\pi, P^{\pi^2}, P^{\pi^3}, P^{\pi^4}, P^{\pi^5}\}$	$\{P, P^{\pi^3}\}$	$\{P^\pi, P^{\pi^4}\}$	$\{P, P^\pi\}$	$\{P^\pi, P^{\pi^2}\}$
$[1,1,1,1,1,1]$	$\{P, Q, R, S, T, U\}$	$\{P, Q\}$	$\{P, R\}$	$\{P, S\}$	$\{P, T\}$
$[1,1,1,1,2]$	$\{P, Q, R, S, T, T^\pi\}$	$\{P, Q\}$	$\{P, R\}$	$\{P, S\}$	$\{P, T\}$
$[1,1,1,3]$	$\{P, Q, R, S, S^\pi, S^{\pi^2}\}$	$\{P, Q\}$	$\{P, R\}$	$\{S, S^\pi\}$	$\{S^\pi, S^{\pi^2}\}$
$[1,1,2,2]$	$\{P, Q, R, R^\pi, S, S^\pi\}$	$\{R, R^\pi\}$	$\{P, R\}$	$\{S, S^\pi\}$	$\{P, S\}$
$[1,2,3]$	$\{P, Q, Q^\pi, R, R^\pi, R^{\pi^2}\}$	$\{Q, Q^\pi\}$	$\{P, Q\}$	$\{R, R^\pi\}$	$\{R^\pi, R^{\pi^2}\}$
$[1,1,4]$	$\{P, Q, R, R^\pi, R^{\pi^2}, R^{\pi^3}\}$	$\{P, Q\}$	$\{R, R^{\pi^2}\}$	$\{R, R^\pi\}$	$\{P, R\}$
$[1,5]$	$\{P, Q, Q^\pi, Q^{\pi^2}, Q^{\pi^3}, Q^{\pi^4}\}$	$\{P, Q\}$	$\{P, Q^\pi\}$	$\{P, Q^{\pi^2}\}$	$\{P, Q^{\pi^3}\}$

Table 2 contains the basis used for each factorisation type. The matrices representing the effect on the Frobenius are then given below.

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$
[2,2,2] [2,4] [3,3] [6]

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$
[1,1,1,1,1,1] [1,1,1,1,2] [1,1,1,3] [1,1,2,2]

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$
[1,2,3] [1,1,4] [1,5]

Given a basis $\{W_1, W_2, W_3, W_4\}$ and the associated matrix M for the effect of the Frobenius π on the 2-torsion group, we now consider the effect of the π on the set of bisections of D_2. Given a specific bisection D_1, the set $\mathcal{S}$ is given by D_1, $D_1 + W_i$, $1 \leq i \leq 4$, $D_1 + W_i + W_j$, $i \neq j$, $1 \leq i, j \leq 4$, $D_1 + W_i + W_j + W_h$, $i \neq j$, $i \neq h$, $j \neq h$, $1 \leq i, j, h \leq 4$, $D_1 + W_1 + W_2 + W_3 + W_4$, where π acts as a permutation on $\mathcal{S}$. If we divide this permutation into disjoint cycles, then the length of each cycle corresponds to the degree of an irreducible factor of $p_{w_i}(x)$, with singletons corresponding to roots in $\mathbb{F}_q$ (i.e. bisections defined over $\mathbb{F}$). Note that the cycle decomposition is completely fixed once we have the image of D_1 under π.

To work out all the possible factorisations of $p_{w_i}(x)$, we work our way through each of the 16 possible images $\pi(D_1)$, computing the cycle decomposition of the permutation $\pi|_{(D_1, \pi(D_1))}$. For example, for $f(x)$ of type [6], with $\pi(D_1) = D_1$, we find the cycles

$$\begin{aligned} &\{D_1\}, \\ &\{D_1 + W_1, D_1 + W_2, D_1 + W_1 + W_2\}, \\ &\{D_1 + W_3,\ D_1 + W_4,\ D_1 + W_1 + W_3 + W_4,\ D_1 + W_1 + W_2 + W_3, \\ &\quad D_1 + W_1 + W_4,\ D_1 + W_1 + W_2 + W_3 + W_4\}, \\ &\{D_1 + W_3 + W_4,\ D_1 + W_1 + W_3,\ D_1 + W_2 + W_4, \\ &\quad D_1 + W_2 + W_3 + W_4,\ D_1 + W_2 + W_3,\ D_1 + W_1 + W_2 + W_4\}, \end{aligned}$$

which corresponds to the decomposition $[1, 3, 6, 6]$. ■

Since the Galois–orbit structure of $\frac{1}{2}D_2$ is independent of the weight of the bisectee D_2, and taking into account Proposition 1, we deduce that the polynomial $p_{w_0}(x) \cdot f(x)$ (as a degree 16 polynomial) follows the same factorisation types as $p_{w_1}(x)$ and $p_{w_2}(x)$.

4.2 Even characteristic

We see that there is a one to one correspondence between bisections and the roots of the quartic $p_{w_i}(x)$. We may say that the roots k_1 over $\mathbb{F}_q$ of $p_{w_i}(x)$ have now a direct geometric interpretation.

Theorem 2. *The degrees of the irreducible factors of $p_{w_i}(x)$ depend on the degrees of the irreducible factors of $h(x)$ as follows:*

$h(x)$	$p_{w_i}(x), i = 1, 2$	
	successful factorisations	*unsuccessful factorisations*
$[1,1,1]$	$[1,1,1,1]$	$[2,2]$
$[1,1^2]$	$[1^2,2]$	$[2^2]$
$[1^3]$	$[1^4]$	
$[1,2]$	$[1,1,2]$	$[4]$
$[3]$	$[1,3]$	

Proof. From $h(x)$, we define the polynomial $H(x) = x^4 + c_2x^2 + c_1x = x \cdot h(x + h_2)$. Since we are in characteristic two, $H(x)$ acts as a linear operator on $\mathbb{F}_q$ and its algebraic extensions. Furthermore, $p_{w_1}(x)$ and $u_{21}p_{w_2}(\frac{x}{u_{21}})$ are of the form $H(x) + c_0$. The factorisation of $p_{w_i}(x)$ can therefore be obtained from the factorisation of $H(x) + c_0$.

Let $x + \gamma_1$ and $x + \gamma_2$ be two factors of $H(x) + c_0$. Since $H(x)$ is a linear operator, $\gamma_1 + \gamma_2$ must be a root of $H(x) = x \cdot h(x + h_2)$. If $h(x)$ is separable, then $c_1 \neq 0$ (since $x^3 + c_2x = h(x + h_2) = x(x + \sqrt{c_2})^2$), so $p_{w_i}(x)$ has four distinct roots (over the closure of $\mathbb{F}_q$). The factorisation form of $p_{w_i}(x)$ is also obtained from that of $h(x)$. If $h(x)$ is $[1^2, 1]$, then $c_1 = 0$ and $c_2 \neq 0$, so $H(W) = W^2(W + \sqrt{c_2})^2$, so each root of $p_{w_i}(x)$ (whether $\mathbb{F}_q$-rational or $\mathbb{F}_{q^2}$-rational) is a double root. If $h(x)$ is $[1^3]$, then $c_1 = c_2 = 0$ and $H(W) = W^4$, so $p_{w_i}(x)$ has a quadruple $\mathbb{F}_q$-rational root. ∎

Note that the polynomial $p_{w_0}(x) \cdot h(x)$ (as a degree 4 polynomial) follows the same factorisation types as $p_{w_i}(x)$.

5 Examples

In this section we illustrate the results above. We show examples of our method to compute bisections over fields of even and odd characteristic. We leave large characteristics for the next section, where we discuss the efficiency of our algorithm.

Example 1. Consider the curve $y^2 = x^6 + 5x^4 + 3x^2 + 1$ over $\mathbb{F}_{19}$. Our method for the random bisectee $D_2 = (x^2 + 14x + 1, 12)$ finds $v_2'(x) = k_1x^3 + (k_0 + 14k_1)x^2 + (14k_0 + k_1)x + k_0 - 12$, so that $u_2'(x)$ equals

$$x^4 + \frac{(14k_1^2 + 2k_0k_1 + 14)}{k_1^2 - 1}x^3 + \frac{(k_0^2 + k_1^2 + 9k_0k_1 + 9)}{k_1^2 - 1}x^2 + \frac{(14k_0^2 + 14k_1 + 2k_0k_1 + 12)}{k_1^2 - 1}x + \frac{(k_0^2 + 14k_0 + 10)}{k_1^2 - 1}.$$

Equating this against $u_1(x)^2 = x^4 + 2u_{11}x^3 + (2u_{10} + u_{11}^2)x^2 + 2u_{10}u_{11}x + u_{10}^2$, in

the terms of degree 3 and 2 one obtains the formulas

$$u_{11} = \tfrac{1}{(k_1^2-1)}(7k_1^2 + k_0k_1 + 7),$$
$$u_{10} = \tfrac{1}{(k_1^2-1)^2}\big(16k_1^4 + 8k_1^3k_0 + 11k_1^2 + 14k_1k_0 + 13k_0^2 + 13\big).$$

Substituting these in the terms of lower degree and taking the resultant w.r.t. k_0 we obtain the following polynomial satisfied by k_1:

$$p_{w_2}(x) = (x-3)(x+2)(x^2+6x+15)(x^4+4x^3+3x^2+16x+6)$$
$$(x^4+13x^3+15x^2+4x+4)(x^4+16x^3+11x^2+2x+1).$$

With the choice $k_1 = 3$, then $s_1(x,3) = 5x^3+8x^2+17x$, $s_2(x,3) = 3x^4+8x^3+9x^2+7x$ and k_0 is the root of $\gcd(s_1(x,3), s_2(x,3)) = x$. The formulas for u_{10}, u_{11} yield $u_1(x) = x^2+4x+5$, and with the right choice of the second coordinate one finds that a bisection of D_2 is

$$D_1 = (x^2+4x+5, x+9) \in \frac{1}{2}D_2.$$

Note that this curve has 2-rank 1, and the bisection corresponding to $k_1 = -2$ is $D_1 + (x^2+14, 0) = (x^2+17x, 15x+18)$.
For the bisectee $D_2 = (x^2+16, 14)$ our method finds that

$$p_{w_2}(x) = x^4(x^4+7x^2+15)(x^4+3x^3+5x^2+6x+10)$$
$$(x^4+16x^3+5x^2+13x+10).$$

With the quadruple root $k_1 = 0$ of $p_{w_2}(x)$ we find $s_1(x,0) = 0$ and $s_2(x,0) = 3x^4+11x^2+6x+1 = 3(x+15)(x+16)(x^2+7x+9)$. Since there are two roots k_0 over $\mathbb{F}_{19}$ of s_2, we say that the factorisation type of $p_{w_2}(x)$ is not $[1^4,4,4,4]$ but $[1,1,2,4,4,4]$. The formulas for u_{10}, u_{11} at the values $\{k_0,k_1\} = \{3,0\}$ and $\{k_0,k_1\} = \{4,0\}$ yield that the two bisections of D_2 are $(x^2+9,7)$, $(x^2+15,9)$, whose difference is again $(x^2+14,0)$.

Example 2. Take the curve $y^2 + (x^3+x^2+\alpha^{17})y = \alpha x^6 + x + \alpha^5$ over $\mathbb{F}_{2^7}$. Here $\alpha = f_6$ is a generator of $\mathbb{F}_{2^7}$ that satisfies $\alpha^7+\alpha+1 = 0$, and the values a such that $a^2+a = \alpha$ are $\alpha^{16}, \alpha^{112}$. For the infinity-supported bisectee $D_2 = (1, \alpha^{112}x^3 + \alpha^{112}x^2)$, we obtain $k_1 = \alpha^{110}$, $k_0 = \alpha^{12}$, $u_{11} = \alpha^{50}$, $u_{10} = \alpha^{87}$, so that

$$D_1 = (x^2+\alpha^{50}x+\alpha^{87}, \alpha^{45}x+\alpha^{60}) \in \frac{1}{2}D_2.$$

Note that since $h(x)$ factors as $(x+\alpha^{16})(x^2+\ldots)$ this curve has 2-rank 1, and D_2 has a second weight 1 bisection $(x+\alpha^{16}, \alpha^{112}x^3+\alpha^{84})$.

6 Efficiency

At this point a natural question arises: what is the benefit of using tailored bisection polynomials for real models, when most curves with a real model admit an

imaginary model (after perhaps an extension of the base field), and when bisection polynomials are already available for them (see [13, 14])? The answer, apart from the completeness issue alluded to in the introduction, is clear: efficiency. Indeed, given polynomials of fixed degree and assuming the Extended Riemann Hypothesis, and using efficient factorisation algorithms (for example, Cantor and Zassenhaus' modification of Berlekamp's algorithm, see [1]), the running time of our halving algorithm is between $O^{\sim}(\log^2 q)$ and $O(\log^3 q)$. However, depending on the polynomial $f(x)$ defining the model of C, one may need to cope with an extension of the base field of degree up to 6 to find an imaginary model where to use the bisection polynomials in [14]. In this worst case scenario, the penalty constant involved for a degree 6 extension is (a priori) between 6^2 and 6^3.

However, another issue complicates the cost estimate: going to an extension of $\mathbb{F}_q$ where some of the Weierstrass points of the curve are defined also implies an increase in the 2-rank of the the curve. This results in an increase in the number of linear factors of the bisection polynomial (which is what the algorithm is looking for). Not only some of the roots found will not correspond to bisections defined over $\mathbb{F}_q$ (and must be eliminated), but they will increase the cost of finding all linear factors. For example, when $f(x)$ is a degree 6 irreducible, we go from having a single linear factor (corresponding to the bisection) to having 16 linear factors, 15 of which correspond to bisections in $\mathbb{F}_{q^6}$ but not in $\mathbb{F}_q$. The increase in cost will then be by a factor significantly higher than 6^2.

The next example shows that in practice our predictions are realistic. The size of the primes we chose for this example is larger, around 100 bits and 400 bits.

Example 3. Consider the prime $p = 2^{100} + 277$ and the curve over $\mathbb{F}_p$

$$\mathrm{C} : y^2 = x^6 + 2x^3 + 3x^2 + 17x + 31.$$

Over $\mathbb{F}_{p^6}$, C admits an imaginary model C′. Using a machine with 4 Intel(R) Xeon(R) CPU's X5460 @ 3.16GHz, and a total of 16GiB System Memory, we found that the average time for a halving computation in $\mathrm{Jac}(\mathrm{C}')$ over $\mathbb{F}_{p^6}$ with the bisection polynomials appeared in [14] is around 290 times slower than an average halving in $\mathrm{Jac}(\mathrm{C})$ over $\mathbb{F}_p$ with our polynomials.
Using the same machine, with the 400 bit prime $p = 2^{400} + 181$ and

$$\mathrm{C} : y^2 = x^6 + 4x^4 + 3x^2 + 17x + 31$$

over $\mathbb{F}_p$, an average halving with [14] in the imaginary model over $\mathbb{F}_{p^6}$ is around 460 times slower than an average halving with our method over $\mathbb{F}_p$.

References

[1] Bach, E., Shallit, J.: *Algorithmic Number Theory*, pg. 167. MIT Press, Cambridge, MA (1996).

[2] Birkner, P.: Efficient divisor class halving on genus two curves, *Selected Areas in Cryptography 2006*, LNCS **4356**, 317–326 (2007).

[3] Birkner, P., Thériault, N.: Faster halvings in genus 2, *Selected Areas in Cryptography 2008*, LNCS **5381**, 1–17 (2008).

[4] Canon, J., Bosma, W., Playoust, C.: The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24**, 235–265 (1997).

[5] Cantor, D.: Computing in the Jacobian of a Hyperelliptic Curve, *Math. Comp.* **48**, 95–101 (1987).

[6] Cohen, H., Frey, G., Avanzi R., Doche, C., Lange, T., Nguyen, K., Vercauteren, F.: *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Math. and its Applications. Chapman & Hall/CRC, Boca Raton (2005).

[7] S. Erikson, S., Jacobson, M.J., Shang, N., Shen, S., Stein, A: Explicit formulas for Real Hyperelliptic Curves of Genus 2 in Affine Representation, *WAIFI 2007*, LNCS **4547**, 202–218 (2007).

[8] Galbraith, S., Harrison, M., Mireles D.J.: Efficient Hyperelliptic Arithmetic Using Balanced Representation for Divisors, in A. J. van der Poorten and A. Stein (eds.), *ANTS-VIII*, LNCS **5011**, 342–356 (2008).

[9] Gaudry, P., Schost, É.: Construction of secure random curves of genus 2 over prime fields, in C. Cachin and J. Camenisch (eds.), *EUROCRYPT 2004*, LNCS **3027**, 239–256 (2004).

[10] Gaudry, P., Schost, É.: Genus 2 point counting over prime fields, *J. Symbolic Comput.* **47**, 368–400 (2012).

[11] Griffiths, D.: Series expansions of algebraic functions, in W. Bosma and A. J. van der Poorten (eds.), *Computational algebra and number theory*, Kluwer, 267–277 (1995).

[12] Jacobson, M., Scheidler, R., Stein, A.: Cryptographic protocols on real hyperelliptic curves, *Adv. in Math. of Communications* **1** no. 2, 197–221 (2007).

[13] Kitamura, I., Katagi, M., Takagi, T.: A complete divisor class halving algorithm for hyperelliptic curve cryptosystems of genus two, LNCS **3574**, 146–157 (2005).

[14] Miret, J., Pujolàs, J., Rio, A.: Bisection for genus 2 curves in odd characteristic, *Proc. of the Japan Academy– Series A* **85**, 55–61 (2009).

[15] Paulus S., Rück, and H.-G.: Real and imaginary quadratic representations of hyperelliptic function fields, *Math. Comp.* **68** no. 227, 1233–1241 (1999).

Dept. de Matemàtica, Universitat de Lleida, Spain
email :{miret, jpujolas}@matematica.udl.cat

Departamento de Matemática y Ciencia de la Computación
Universidad de Santiago de Chile
Santiago, Chile
email: nicolas.theriault@usach.cl