Bisection for genus 2 curves in odd characteristic

By Josep M. Miret,*) Jordi Pujolàs*) and Anna Rio**)

(Communicated by Heisuke Hironaka, m.j.a., March 12, 2009)

Abstract: We show how to invert the multiplication-by-2 map in Jacobians of genus 2 curves C over finite fields $\mathbf{F}_q$ of odd characteristic. For any divisor $D \in \mathrm{Jac(C)}(\mathbf{F}_q)$ we provide a method to construct the coordinates of all divisors $D' \in \mathrm{Jac(C)}(\mathbf{F}_q)$ such that $2D' = D$.

Key words: Genus 2 curves; Jacobian; finite field.

1. Introduction. Let C be a genus two curve over a finite field $\mathbf{F}_q$ of odd characteristic, given by a model

$$\mathrm{C} : y^2 = f(x), \tag{1}$$

where $f(x) = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0 \in \mathbf{F}_q[x]$ has no double roots. If q is different from a power of 5, f_4 can be made 0 after a translation of x. In the following we assume $f_4 = 0$ everywhere except in section 5. The curves with a model like (1) have one (Weierstraß) point P_∞ at infinity, and the roots of $f(x)$ are the x-coordinates of the affine Weierstraß points of C.

The algorithms we present here work in the group of $\mathbf{F}_q$-points of the Jacobian Jac(C), in terms of the usual Mumford coordinates $(u(x), v(x))$ of weight one divisors $(u(x) = x - x_1,\ v(x) = y_1)$ and weight two divisors $(u(x) = x^2 + u_1x + u_0,\ v(x) = v_1x + v_0)$ ([4], page 307). Our aim in this paper is to efficiently construct $\frac{1}{2}D_2$, namely the set of pre-images

$$D_1 = (u_1(x), v_1(x)) \in \mathrm{Jac(C)}(\mathbf{F}_q)$$

of any given divisor $D_2 = (u_2(x), v_2(x)) \in \mathrm{Jac(C)}(\mathbf{F}_q)$ under the multiplication-by-two map

$$\begin{aligned}[2] : \mathrm{Jac(C)}(\mathbf{F}_q) &\longrightarrow \mathrm{Jac(C)}(\mathbf{F}_q)\\ D_1 &\longmapsto D_2 = 2D_1.\end{aligned}$$

We build on the ideas in [6], where a search for a linear polynomial $k_1x + k_0 \in \mathbf{F}_q[x]$ involved in the reduction part of the addition law, was successful to determine $\frac{1}{2}D_2$ for genus 2 curves over finite fields of even characteristic.

We expect our method to be of some significance for point counting techniques in genus 2, as the results we present here should help to find quickly the 2-power of the cardinal $\#\mathrm{Jac(C)}(\mathbf{F}_q)$, much as in the even characteristic case was done in [7]. Ours is a much specific approach to the 2-part of the cardinal only, but we expect that the natural adaptation of [7] to odd characteristic allows to compute the 2-part faster than the current algorithms (see [5]).

The structure of the rest of the paper is as follows: In section 2 we recall the role of the 2-torsion subgroup $\mathrm{Jac(C)}(\mathbf{F}_q)[2]$ in this problem, then we set a classification of the rank of the 2-torsion subgroup in terms of the factorization of $f(x)$, and finally we find $\frac{1}{2}D_2$ for some easy cases. In section 3 we provide a constructive method to find $\frac{1}{2}D_2$ for any given $D_2 \in \mathrm{Jac(C)}(\mathbf{F}_q)$ in terms of the roots of certain polynomials $p_{w_1}(x), p_{w_2}(x)$ of degree 16. In section 4 we describe the factorization of $p_{w_1}(x), p_{w_2}(x)$ in terms of the galois structure of the 2-torsion subgroup $\mathrm{Jac(C)}(\mathbf{F}_q)[2]$, in the same spirit as in the genus 1 paper [8], where the factorization of the ℓ-division polynomials was given. In the final section 5 we show some examples.

2. Two torsion. Since our base field's characteristic is odd, the 2-torsion subgroup $\mathrm{Jac(C)}(\mathbf{F}_q)[2]$ is either trivial, or isomorphic to $(\mathbf{Z}/2\mathbf{Z})^r$, $r = 1, 2, 3, 4$. In this section first we recall how the factorization of $f(x)$ as a polynomial in $\mathbf{F}_q[x]$ determines the rank of $\mathrm{Jac(C)}(\mathbf{F}_q)[2]$.

The Weierstraß $\mathbf{F}_q$-points W of C are fixed under the hyperelliptic involution $\iota : (x, y) \mapsto (x, -y)$. Hence $2W$ is the divisor of zeros of the function $x - x(W)$, and the degree zero divisor $2W - 2P_\infty$ is therefore identified with the neutral

2000 Mathematics Subject Classification. Primary 11G20, 14H40, 14H45.

*) Departament de Matemàtica, Universitat de Lleida, C/ Jaume II, 69, Lleida, Spain.
**) Departament de Matemàtica Aplicada II, Universitat Politècnica de Catalunya, C/ Jordi Girona 1-3, Barcelona, Spain.

doi: 10.3792/pjaa.85.55

element in $\mathrm{Jac(C)}(\mathbf{F}_q)$. Therefore all weight one divisors with an affine $\mathbf{F}_q$-rational Weierstraß point in the finite support have order 2, and they generate the $\mathbf{F}_q$-rational 2-torsion subgroup $\mathrm{Jac(C)}(\mathbf{F}_q)[2]$. Analogously, any irreducible quadratic factor of $f(x)$ provides the first coordinate $u(x)$ of a divisor in $\mathrm{Jac(C)}(\mathbf{F}_q)[2]$.

Proposition 1. *The rank of* $\mathrm{Jac(C)}(\mathbf{F}_q)[2]$ *depends on the* $\mathbf{F}_q$*-factorization of* $f(x)$ *as follows*:

factorization types of $f(x)$	2-rank
$[1,4]$, $[2,3]$	1
$[1,1,3]$, $[1,2,2]$	2
$[1,1,1,2]$	3
$[1,1,1,1,1]$	4

Proof. Let m be the number of irreducibles of degree 1 or 2 in the prime decomposition of $f(x)$ in $\mathbf{F}_q[x]$. Since the product of all the factors of $f(x)$ provides the divisor of zeros of a principal divisor, if $m = 0, 1, 2$ then the rank of $\mathrm{Jac(C)}(\mathbf{F}_q)[2]$ is clearly 0, 1 or 2 respectively, and if $m \geq 3$, then the rank of $\mathrm{Jac(C)}(\mathbf{F}_q)[2]$ is equal to $m-1$. □

Remark 1. *From now on we write all divisors in* $\mathrm{Jac(C)}(\overline{\mathbf{F}}_q)[2]$ *as* W*. Since* $2W$ *is principal for all* $W \in \mathrm{Jac(C)}(\mathbf{F}_q)[2]$*, it follows that*

$$\frac{1}{2}D_2 = \{D_1 + W \mid W \in \mathrm{Jac(C)}(\mathbf{F}_q)[2]\}.$$

We show $\frac{1}{2}D_2$ in an easy example first. Take $(x_0, y_0) \in \mathrm{C}(\mathbf{F}_q)$ with $y_0 \neq 0$ and consider the particular case of a divisor whose first Mumford coordinate is a square $u(x) = (x - x_0)^2$. From any such point on $\mathrm{C}(\mathbf{F}_q)$, working out the second Mumford coordinate $v(x)$ in $\mathrm{Jac(C)}(\mathbf{F}_q)$ one obtains the weight two divisor

$$D_2 = \left((x - x_0)^2, \frac{f'(x_0)}{2y_0}(x - x_0) + y_0)\right).$$

One checks that the weight one divisor

$$D_1 = (x - x_0, y_0)$$

trivially satisfies $[2]D_1 = D_2$ (use Cantor's algorithms [3]). With the coordinates of one element in $\frac{1}{2}D_2$, the rest are easily determined adding the 2-torsion divisors. In particular, one easily sees that for every root w of $f(x)$ in $\mathbf{F}_q$, the set $\frac{1}{2}D_2$ contains a divisor with first coordinate equal to $(x - x_0)(x - w)$.

For divisors D_2 with a nonsquare first coordinate, things are not as simple, since one does not have easy preimages D_1 at hand. Our goal in this paper is to provide a method to find $\frac{1}{2}D$ for a generic $D \in \mathrm{Jac(C)}(\mathbf{F}_q)$– one whose first coordinate is not a square. In Proposition 2 below, we show that for our purpose it is enough to determine the first coordinates of the elements in $\frac{1}{2}D$ for almost all divisors D.

Lemma 1. $D_1, -D_1 \in \frac{1}{2}D_2$ *if and only if* $Ord(D_2) = 2$.

Proof. Since $[2](-D_1) = -([2]D_1)$, then $[2]D_1 = -[2]D_1$, so $[4]D_1 = 0$, which is the same as $[2]D_2 = 0$. □

Proposition 2. *If* $Ord(D_2) \neq 2$*, then there do not exist* $D_1, D_1' \in \frac{1}{2}D_2$ *with equal first coordinate.*

Proof. We write P^ι for the image under the hyperelliptic involution ι of any point P of the curve. For any given divisor $D = P + Q - 2P_\infty$ there are at most 4 divisors in $\mathrm{Jac(C)}(\mathbf{F}_q)$ with the same first coordinate $u(x)$, namely

$$\begin{aligned} D &= P + Q - 2P_\infty, & -D &= P^\iota + Q^\iota - 2P_\infty, \\ \tilde{D} &= P^\iota + Q - 2P_\infty, & -\tilde{D} &= P + Q^\iota - 2P_\infty. \end{aligned}$$

Assume $[2]D = [2]\tilde{D} = D_2$. Then $0 = [2](D - \tilde{D}) = [2](Q - Q^\iota)$. The divisor $Q - Q^\iota$ is equivalent to $2Q - 2P_\infty$ since their difference is principal

$$\begin{aligned} (2Q - 2P_\infty) - (Q - Q^\iota) &= Q + Q^\iota - 2P_\infty \\ &= (x - x(Q)). \end{aligned}$$

But the divisor $2Q - 2P_\infty = 2(Q - P_\infty)$ cannot have order 2 since then $f(x)$ would have a double root. Hence D and $\tilde{D}$ are not allowed to be both in any set $\frac{1}{2}D_2$ for any D_2. Since $Ord(D_2) \neq 2$, by Lemma 1 above it is also forbidden for one divisor and its opposite to be in $\frac{1}{2}D_2$ at the same time. Therefore our claim follows. □

3. Bisection polynomials. In this section we show how to build up, for any given $D_2 \in \mathrm{Jac(C)}(\mathbf{F}_q)$, a degree 16 polynomial whose roots provide the first coordinate of all the divisors in $\frac{1}{2}D_2$.

The way we build such polynomial is to reverse the reduction part in Cantor's algorithm [4, pg. 308]. For a divisor with coordinates $(u(x), v(x))$, the reduction steps consist in the iteration of

`r1.` $u'(x) \leftarrow \frac{f(x) - v^2(x)}{u(x)}$, $\quad v'(x) \leftarrow -v(x) \bmod u'(x)$

`r2.` $u(x) \leftarrow u'(x)$, $\quad v(x) \leftarrow v'(x)$

until $\deg(u(x)) \leq 2$.

The method we follow, as shown in [6], is to run the steps `r1` and `r2` backwards once, starting

with the coordinates $(u_2(x), v_2(x))$ of D_2, and then to match the resulting "unreduced" coordinates with the "doubled" coordinates $(u_1'(x), v_1'(x)) = (u_1(x)^2, \ldots)$ from the composition part of doubling a potential divisor $D_1 = (u_1(x), v_1(x))$.

In the reversing of the reduction part of Cantor's algorithms, we use a linear polynomial $k(x) = k_1 x + k_0$ to find a representative of the class $-v_2(x)$ mod $u_2(x)$ of degree greater than 1. We summarize the steps of our method below:

1. $u_2'(x) \leftarrow u_2(x)$, $v_2'(x) \leftarrow v_2(x)$
2. find the unreduced coordinates $u_1'(x), v_1'(x)$ of a representative in the class of a potential D_1
   $u_1'(x) \leftarrow \frac{f(x)-v_1'(x)^2}{u_2'(x)}$, $v_1'(x) \leftarrow -v_2'(x) + u_2'(x)k(x)$
3. equate $u_1'(x)$ with $u_1(x)^2$.

In the next paragraphs we follow this sketch, and we obtain a pair of bivariate polynomials that our wanted k_0, k_1 have to satisfy in case D_1 exists. Then, instead of working with two bivariate polynomials, we turn them into a single univariate polynomial (of degree 16) in k_1. We show the computations explicitly when the input divisor D_2 has weight 2, the analogous applies in weight 1.

From the final reduction step in the duplication algorithm, using $k(x) = k_1 x + k_0$ and $u_2(x) = x^2 + u_{21}x + u_{20}$ one finds

$$\begin{aligned} v_1'(x) = {} & k_1 x^3 + (k_0 + k_1 u_{21})x^2 \\ & + (k_0 u_{21} + k_1 u_{20} - v_{21})x + k_0 u_{20} - v_{20}. \end{aligned}$$

It follows that

$$\begin{aligned} u_1(x)^2 = {} & x^4 + 2u_{11}x^3 + (2u_{10} + u_{11}^2)x^2 \\ & + 2u_{10}u_{11}x + u_{10}^2 \end{aligned}$$

must be equal to

$$\begin{aligned} u_1'(x) = {} & x^4 + \tfrac{1}{k_1^2}x^3(-1 + 2k_0k_1 + u_{21}k_1^2) \\ & + \tfrac{1}{k_1^2}x^2(k_0^2 + u_{20}k_1^2 + u_{21} + 2k_0u_{21}k_1 + 2v_{21}k_1) \\ & + \tfrac{1}{k_1^2}x(-f_3 + u_{20} + 2k_0u_{20}k_1 + k_0^2u_{21} - u_{21}^2 \\ & + 2v_{20}k_1 + 2k_0v_{21}) + \tfrac{1}{k_1^2}(-f_2 + k_0^2u_{20} + f_3u_{21} \\ & - 2u_{20}u_{21} + u_{21}^3 + 2k_0v_{20} + v_{21}^2). \end{aligned}$$

Equating u_{11} and u_{10} from the degree 3 and 2 terms respectively one obtains the coefficients

$$\begin{aligned} u_{11} = {} & \tfrac{1}{2k_1^2}(k_1^2u_{21} + 2k_0k_1 - 1) \\ u_{10} = {} & \tfrac{1}{8k_1^4}(-k_1^4(u_{21}^2 - 4u_{20}) + k_1^3(4k_0u_{21} - 8v_{21}) \\ & + 6k_1^2u_{21} + 4k_1k_0 - 1), \end{aligned}$$

and after substituting the values of u_{11} and u_{10} above into the degree 1 and 0 monomials, we find the multivariate polynomials

$$\begin{aligned} & p_1(k_0, k_1) \\ & = k_0^2(-8k_1^2) + k_0(-2k_1^5(u_{21}^2 - 4u_{20}) \\ & \quad - 12k_1^3u_{21} + 6k_1) + k_1^6u_{21}(u_{21}^2 - 4u_{20}) \\ & \quad + 8k_1^5(u_{21}v_{21} - 2v_{20}) + k_1^4(12u_{20} - 8f_3 - 15u_{21}^2) \\ & \quad - 8k_1^3v_{21} + 7k_1^2u_{21} - 1 \\ & p_2(k_0, k_1) \\ & = k_0^2(-16k_1^6(u_{21}^2 - 4u_{20}) - 32k_1^4u_{21} - 16k_1^2) \\ & \quad + k_0(8k_1^7u_{21}(u_{21}^2 - 4u_{20}) + 64k_1^6(u_{21}v_{21} - 2v_{20}) \\ & \quad + 8k_1^5(-4u_{20} - 5u_{21}^2) + 64k_1^4v_{21} - 40k_1^3u_{21} + 8k_1) + \\ & \quad - k_1^8(u_{21}^2 - 4u_{20})^2 - 16k_1^7v_{21}(u_{21}^2 - 4u_{20}) \\ & \quad + k_1^6(-64f_2 + 64f_3u_{21} - 176u_{20}u_{21} + 76u_{21}^3) \\ & \quad + 96k_1^5u_{21}v_{21} + 2k_1^4(4u_{20} - 19u_{21}^2) \\ & \quad - 16k_1^3v_{21} + 12k_1^2u_{21} - 1, \end{aligned}$$

of degrees $2, 6$ and $2, 8$ in k_0 and k_1 respectively. We consider the (degree 16) resultant

$$p_{w_2}(x) := Res_{k_0}(p_1(k_0, x), p_2(k_0, x))$$

of p_1 and p_2 w.r.t. k_0, which we show below:

$$\begin{aligned} & p_{w_2}(x) \\ & = x^{16}(u_{21}^2 - 4u_{20})^5 + 16\,x^{15}(u_{21}^2 - 4u_{20})^4v_{21} \\ & \quad + 8\,x^{14}(u_{21}^2 - 4u_{20})^3(8f_2 - 12f_3u_{21} \\ & \quad + 20u_{20}u_{21} - 15u_{21}^3) \\ & \quad + 16\,x^{13}(u_{21}^2 - 4u_{20})^2(32f_3v_{20} - 40u_{20}v_{20} \\ & \quad + 90u_{21}^2v_{20} - 16f_3u_{21}v_{21} - 20u_{20}u_{21}v_{21} - 35u_{21}^3v_{21}) \\ & \quad - 4\,x^{12}(u_{21}^2 - 4u_{20})(256f_3^2u_{20} - 768f_3u_{20}^2 + 576u_{20}^3 \\ & \quad + 1280f_2u_{20}u_{21} - 64f_3^2u_{21}^2 - 256f_3u_{20}u_{21}^2 \\ & \quad + 1648u_{20}^2u_{21}^2 - 320f_2u_{21}^3 + 112f_3u_{21}^4 - 932u_{20}u_{21}^4 \\ & \quad + 121u_{21}^6 + 2560u_{21}v_{20}^2 - 512u_{20}v_{20}v_{21} \\ & \quad - 2432u_{21}^2v_{20}v_{21} + 256u_{20}u_{21}v_{21}^2 + 576u_{21}^3v_{21}^2) \\ & \quad + 16\,x^{11}(1536f_2u_{20}v_{20} - 1024f_3u_{20}u_{21}v_{20} \\ & \quad + 2880u_{20}^2u_{21}v_{20} - 384f_2u_{21}^2v_{20} + 256f_3u_{21}^3v_{20} \\ & \quad - 160u_{20}u_{21}^3v_{20} - 140u_{21}^5v_{20} + 2048v_{20}^3 \\ & \quad + 256f_3u_{20}^2v_{21} - 448u_{20}^3v_{21} - 768f_2u_{20}u_{21}v_{21} \\ & \quad + 384f_3u_{20}u_{21}^2v_{21} - 2064u_{20}^2u_{21}^2v_{21} + 192f_2u_{21}^3v_{21} \\ & \quad - 112f_3u_{21}^4v_{21} + 476u_{20}u_{21}^4v_{21} + 17u_{21}^6v_{21} \\ & \quad - 3072u_{21}v_{20}^2v_{21} + 1536u_{21}^2v_{20}v_{21}^2 - 256u_{21}^3v_{21}^3) \\ & \quad + 8\,x^{10}(1024f_2f_3u_{20} - 1664f_2u_{20}^2 - 1536f_3^2u_{20}u_{21} \\ & \quad + 5056f_3u_{20}^2u_{21} - 4160u_{20}^3u_{21} - 256f_2f_3u_{21}^2 \\ & \quad + 192f_2u_{20}u_{21}^2 + 384f_3^2u_{21}^3 - 2848f_3u_{20}u_{21}^3 \end{aligned}$$

$$
\begin{aligned}
&+ 3600u_{20}^2u_{21}^3 + 56f_2u_{21}^4 + 396f_3u_{21}^5\\
&- 220u_{20}u_{21}^5 - 105u_{21}^7 + 2048f_3v_{20}^2 - 3072u_{20}v_{20}^2\\
&+ 5888u_{21}^2v_{20}^2 - 2048f_3u_{21}v_{20}v_{21} + 1024u_{20}^2v_{21}^2\\
&- 2048u_{20}u_{21}v_{20}v_{21} - 4608u_{21}^3v_{20}v_{21}\\
&+ 512f_3u_{21}^2v_{21}^2 + 1280u_{20}u_{21}^2v_{21}^2 + 896u_{21}^4v_{21}^2)\\
&- 16\,x^9(256f_3u_{20}v_{20} - 352u_{20}^2v_{20} + 1280f_2u_{21}v_{20}\\
&- 1984f_3u_{21}^2v_{20} + 3216u_{20}u_{21}^2v_{20} - 2382u_{21}^4v_{20}\\
&+ 256f_2u_{20}v_{21} + 1408f_3u_{20}u_{21}v_{21} - 1424u_{20}^2u_{21}v_{21}\\
&- 704f_2u_{21}^2v_{21} + 608f_3u_{21}^3v_{21}\\
&- 328u_{20}u_{21}^3v_{21} + 971u_{21}^5v_{21} + 1024v_{20}^2v_{21}\\
&- 1024u_{21}v_{20}v_{21}^2 + 256u_{21}^2v_{21}^3)\\
&+ 2\,x^8(2048f_2^2 - 1024f_3^2u_{20} + 3072f_3u_{20}^2 - 2240u_{20}^3\\
&- 6144f_2f_3u_{21} + 15360f_2u_{20}u_{21} + 4864f_3^2u_{21}^2\\
&- 16896f_3u_{20}u_{21}^2 + 18960u_{20}^2u_{21}^2 - 8960f_2u_{21}^3\\
&+ 11712f_3u_{21}^4 - 22660u_{20}u_{21}^4 + 7715u_{21}^6\\
&+ 5120u_{21}v_{20}^2 - 8192f_3v_{20}v_{21} + 10240u_{20}v_{20}v_{21}\\
&- 2560u_{21}^2v_{20}v_{21} + 4096f_3u_{21}v_{21}^2\\
&- 10240u_{20}u_{21}v_{21}^2 + 1280u_{21}^3v_{21}^2)\\
&+ 16\,x^7(128f_2v_{20} + 768f_3u_{21}v_{20} - 800u_{20}u_{21}v_{20}\\
&+ 440u_{21}^3v_{20} - 128f_3u_{20}v_{21} + 176u_{20}^2v_{21}\\
&- 704f_2u_{21}v_{21} + 608f_3u_{21}^2v_{21} - 1208u_{20}u_{21}^2v_{21}\\
&+ 971u_{21}^4v_{21} - 512v_{20}v_{21}^2 + 256u_{21}v_{21}^3)\\
&- 8\,x^6(256f_2f_3 - 416f_2u_{20} - 384f_3^2u_{21}\\
&+ 1264f_3u_{20}u_{21} - 1040u_{20}^2u_{21} - 56f_2u_{21}^2\\
&- 396f_3u_{21}^3 + 640u_{20}u_{21}^3 + 105u_{21}^5 - 256v_{20}^2\\
&- 1024u_{21}v_{20}v_{21} - 512f_3v_{21}^2 + 768u_{20}v_{21}^2\\
&- 896u_{21}^2v_{21}^2)\\
&+ 16\,x^5(32f_3v_{20} - 56u_{20}v_{20} - 106u_{21}^2v_{20}\\
&- 192f_2v_{21} + 112f_3u_{21}v_{21} - 332u_{20}u_{21}v_{21}\\
&- 17u_{21}^3v_{21} + 256v_{21}^3)\\
&+ 4\,x^4(64f_3^2 - 192f_3u_{20} + 144u_{20}^2 + 320f_2u_{21}\\
&- 112f_3u_{21}^2 + 448u_{20}u_{21}^2 - 121u_{21}^4 - 128v_{20}v_{21}\\
&- 576u_{21}v_{21}^2)\\
&+ 16\,x^3(20u_{21}v_{20} + 16f_3v_{21} - 20u_{20}v_{21} + 35u_{21}^2v_{21})\\
&+ 8\,x^2(8f_2 - 12f_3u_{21} + 20u_{20}u_{21} - 15u_{21}^3)\\
&+ 16\,x(2v_{20} - u_{21}v_{21}) + (u_{21}^2 - 4u_{20}).
\end{aligned}
$$

Remark 2. *Since $u_2(x)$ is not a square, $p_{w_2}(x)$ has* 16 *roots in $\overline{\mathbf{F}}_q$, none of which is* 0.

Remark 3. *The values of k_1 for which $p_1(x,k_1)$ and $p_2(x,k_1)$ are proportional are roots of the degree* 8 *polynomial*

$$
\begin{aligned}
\beta(k_1) = {}& k_1^8(u_{21}^2 - 4u_{20})^2 - 10k_1^6u_{21}(u_{21}^2 - 4u_{20})\\
&+ 16k_1^5(u_{21}v_{21} - 2v_{20}) + 16k_1^3v_{21}\\
&- 10k_1^2u_{21} - 1.
\end{aligned}
$$

Theorem 1. *Let $D_2 = (u_2(x), v_2(x))$ be a weight* 2 *divisor of* $\mathrm{Jac(C)}(\mathbf{F}_q)$ *such that $u_2(x)$ is not a square and let $p_1(k_0,k_1), p_2(k_0,k_1)$ be as above. Then the coefficients of the first coordinate $u_1(x)$ of every $\mathbf{F}_q$-rational divisor $D_1 = (u_1(x), v_1(x)) \in \frac{1}{2}D_2$ are*

$$
\begin{aligned}
u_{11} &= \tfrac{1}{2k_1^2}(k_1^2u_{21} + 2k_0k_1 - 1)\\
u_{10} &= \tfrac{1}{8k_1^4}(-k_1^4(u_{21}^2 - 4u_{20}) + k_1^3(4k_0u_{21} - 8v_{21})\\
&\quad + 6k_1^2u_{21} + 4k_1k_0 - 1),
\end{aligned}
$$

where $k_1 \in \mathbf{F}_q$ is a root of $p_{w_2}(x)$, and $k_0 = \alpha(k_1)/(k_1\beta(k_1))$ with $\beta(k_1)$ as above and

$$
\begin{aligned}
\alpha(k_1) = {}& 2k_1^{10}u_{21}(u_{21}^2 - 4u_{20})^2 - 16k_1^9(24u_{20}u_{21}v_{21}\\
&+ 8u_{20}v_{20} + u_{21}^3v_{21} - 2u_{21}^2v_{20}) - k_1^8(80u_{20}^2\\
&+ 120u_{20}u_{21}^2 + 64u_{20}f_3 - 25u_{21}^4 - 16u_{21}^2f_3)\\
&+ 32k_1^7u_{21}(u_{21}v_{21} - 2v_{20}) + 8k_1^6(20u_{20}u_{21}\\
&- 15u_{21}^3 - 12u_{21}f_3 + 8f_2) - 16k_1^5(7u_{21}v_{21}\\
&- 2v_{20}) + 2k_1^4(12u_{20} + 17u_{21}^2 - 8f_3 - u_{21}) - 1
\end{aligned}
$$

whenever $\beta(k_1) \neq 0$, and k_0 equals any of the two roots of $p_1(x,k_1)$ otherwise.

Proof. Since $u_2(x)$ is not a square, $k_1 = 0$ is not a root of $p_{w_2}(x)$ because the independent term is nonzero. The formulas for u_{11}, u_{10} follow from the construction of $p_{w_2}(x)$. By definition, if k_1 is a root of $p_{w_2}(x)$ then the quadratic polynomials $p_1(x,k_1)$ and $p_2(x,k_1)$ share at least one root. If the root k_1 satisfies also $\beta(k_1) = 0$, then $p_1(x,k_1)$ and $p_2(x,k_1)$ are the same quadratic polynomial, and with the two roots of it one obtains 2 divisors in $\frac{1}{2}D_2$. If $\beta(k_1) \neq 0$, there is only one k_0 and the formula $k_0 = \alpha(k_1)/(k_1\beta(k_1))$ follows at once. □

Corollary 1. *The multiplicity of the roots of $p_{w_2}(x)$ is at most* 2*, and the double roots satisfy $\beta(k_1) = 0$.*

Proof. For every root k_1 of $p_{w_2}(x)$, there are at most 2 values k_0 which are roots of $p_1(x,k_1)$ and $p_2(x,k_1)$ at the same time. The number of shared roots to be 2 implies that k_1 is a root of $p_{w_2}(x)$ of multiplicity $m > 1$. Since k_1 counts for at most 2 different divisors and (over $\overline{\mathbf{F}}_q$) the cardinal of $\frac{1}{2}D_2$ equals $\deg(p_{w_2}(x))$, necessarily $m \leq 2$. If k_1 is double then p_1 and p_2 are proportional and $\beta(k_1) = 0$. □

The same procedure yelds a bisection polynomial for weight 1 divisors with the same properties.

4. Factorizations of the bisection polynomials. In this section we relate the possible factorizations of $p_{w_1}(x)$ and $p_{w_2}(x)$ with the possible factorizations of $f(x)$.

Theorem 2. *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*:

$f(x)$	$p_{w_i}(x), i = 1, 2$
$[1,1,1,1,1]$	$[1,\dots,1]$, $[1,\dots,1,2,2,2,2]$, $[1,1,1,1,2,\dots,2]$, $[1,1,2,\dots,2]$, $[2,\dots,2]$
$[1,1,1,2]$	$[1,\dots,1,2,2,2,2]$, $[1,1,1,1,2,\dots,2]$, $[1,1,2,\dots,2]$, $[2,\dots,2]$, $[4,4,4,4]$
$[1,1,3]$	$[1,1,1,1,3,3,3,3]$, $[1,1,2,6,6]$, $[1,1,1,1,6,6]$, $[2,2,6,6]$
$[1,2,2]$	$[1,1,1,1,2,\dots,2]$, $[1,1,1,1,6,6]$, $[4,4,4,4]$
$[2,3]$	$[1,1,2,3,3,6]$, $[4,12]$, $[1,1,1,1,3,3,6]$
$[1,4]$	$[1,1,2,4,4,4]$, $[8,8]$, $[1,1,1,1,4,4,4]$

Proof. Since the Frobenius automorphism π commutes with the multiplication-by-two map [2], the Galois action in the preimage $[2]^{-1}(D_2)$ is given by addition of the elements in $\mathrm{Jac(C)}(\overline{\mathbf{F}}_q)[2]$. In order to factor $p_{w_2}(x)$ and $p_{w_1}(x)$, the goal is to find Galois orbits in $[2]^{-1}(D_2)$. There is a bijection between the Galois orbits and the factors of $p_{w_2}(x)$ and $p_{w_1}(x)$, except for those double $\mathbf{F}_q$-roots k_1 such that $p_1(x,k_1)$ and $p_2(x,k_1)$ are quadratic irreducible proportional polynomials.

We fix a natural set of basis in $\mathrm{Jac(C)}(\overline{\mathbf{F}}_q)[2]$ (one for every factorization type of $f(x)$), w.r.t. which the Frobenius action is represented as follows:

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

and their orders are 1, 2, 3, 2, 6, 4 respectively.

We show the details for the case $[2,3]$, the other are completely analogous. The basis of $\mathrm{Jac(C)}(\overline{\mathbf{F}}_q)[2]$ established with our criterion consists of two divisors $W_1, W_2 = W_1^\pi$ defined over the quadratic extension and two divisors $W_3, W_4 = W_3^\pi$ over the cubic extension.

Take $D_1 \in \mathrm{Jac(C)}(\overline{\mathbf{F}}_q)$ such that $2D_1 = D_2$. If $D_1 \in \mathrm{Jac(C)}(\mathbf{F}_q)$ then clearly we also have $D_1 + W_1 + W_2 \in \mathrm{Jac(C)}(\mathbf{F}_q)$. This exhausts the single-element orbits. By the shape the matrix, the only 2-element orbit is

$$\{D_1 + W_1, D_1 + W_2\},$$

the two 3-element orbits are

$$\{D_1 + W_3, D_1 + W_4, D_1 + W_1 + W_2 + W_3 + W_4\}$$
$$\{D_1 + W_1 + W_2 + W_3, D_1 + W_1 + W_2 + W_4, D_1 + W_3 + W_4\},$$

and the only 6-element orbit is

$$\{D_1 + W_1 + W_3, D_1 + W_2 + W_4, D_1 + W_1 + W_2 + W_4, D_1 + W_3 + W_4, D_1 + W_1 + W_2 + W_3, D_1 + W_1 + W_2 + W_4\}.$$

If D_1 is not defined over the base field $\mathbf{F}_q$, then the Frobenius action adds a binary combination of the basis W_i to D_1. The length of the orbit containing D_1 depends on the image D_1^π of D_1 under Frobenius. Writing

$$D_1^\pi = D_1 + m_1W_1 + m_2W_2 + m_3W_3 + m_4W_4$$

with $m_i \in \{0,1\}$ for $i = 1,2,3,4$, then one sees

$$D_1^{\pi^2} = D_1 + (m_1 + m_2 + m_4)W_1 + (m_1 + m_2 + m_4)W_2 + (m_3 + m_4)W_3 + m_3W_4.$$

From this, the only $\mathbf{F}_q$-orbit of order 2 containing D_1 is obtained with $m_1 = m_2 = 1$, $m_3 = m_4 = 0$, namely $D_1^\pi = D_1 + W_1 + W_2$.

Similarly,

$$D_1^{\pi^3} = D_1 + (m_2 + m_3 + m_4)W_1 + (m_1 + m_3 + m_4)W_2$$

and the only possibilities for orbits of order 3 containing D_1 arise if D_1 under Frobenius is one of

$$D_1 + W_1 + W_2 + W_3, D_1 + W_1 + W_2 + W_4,$$
$$D_1 + W_3 + W_4.$$

The remaining D_1^π for orbits with D_1 are

order 4	order 12
$D_1 + W_1$	$D_1 + W_1 + W_3$
$D_1 + W_2$	$D_1 + W_1 + W_4$
order 6	$D_1 + W_3 + W_4$
$D_1 + W_1 + W_2 + W_3 + W_4$	$D_1 + W_2 + W_3$
$D_1 + W_3$	$D_1 + W_2 + W_4$
$D_1 + W_4$	$D_1 + W_2 + W_3 + W_4$.

With these, the remaining factors of $p_{w_1}(x), p_{w_2}(x)$ follow at once. The full factor structure is $[1, 1, 2, 3, 3, 6]$ when D_1 belongs to an orbit of order 1, 2, 3, 6 and $[4, 12]$ otherwise. □

5. Examples. We gather in this final section some examples worked out with MAGMA [2]. We provide the coefficients of the Mumford coordinates of several sets $\frac{1}{2}D$. We use the notation $(1, u_1, u_0, v_1, v_0)$ for the divisor $(x^2 + u_1x + u_0, v_1x + v_0)$ and $(0, 1, u_0, 0, v_0)$ for $(x + u_0, v_0)$. We include an example over a lengthy 60-bit prime field, an example in weight 1, and an example in characteristic 5, which requires the presence of the annoying f_4 terms in the curve's equations (which makes the bisection polynomials look quite larger than the ones we showed above).

Since the most expensive step is to extract a root of a (degree 16) polynomial over $\mathbf{F}_q$, Cantor and Zassenhaus' modification of Berlekamp's algorithm (see [1, Th. 7.4.6]) predicts an expected running time of $O(\log^3 q)$ bit operations. We checked the timings needed to find $\frac{1}{2}D$ for fields of cryptographic size in genus 2. For prime fields of around 100 bits these were not higher than 1 second.

5.1. Rank 1. Consider

$$y^2 = x^5 + 315x^3 + 311x^2 + 314x + 311$$

over $\mathbf{F}_{10007}$, and the weight 1 divisor $D_2 = (0, 1, -18, 0, 5199)$. We obtain

$$\begin{aligned} p_{w_1}(x) &= (x + 7531)(x + 8008)(x^2 + 4475x + 4678) \\ &\quad \times (x^3 + 1522x^2 + 1784x + 105) \\ &\quad \times (x^3 + 2953x^2 + 4868x + 2792) \\ &\quad \times (x^6 + 5532x^5 + 3811x^4 + 2637x^3 \\ &\qquad + 2230x^2 + 9108x + 6048), \\ \tfrac{1}{2}D_2 &= \{(1, 8412, 253, 7202, 6736), \\ &\qquad (1, 6870, 7683, 4792, 8061)\} \end{aligned}$$

with $k_1 \in \{1999, 2476\}$ and $k_0 \in \{2587, 7975\}$.

5.2. Rank 2 in characteristic 5. Consider

$$y^2 = x^5 + 2x^4 + 3x^3 + 3x^2 + 4x + 2$$

over $\mathbf{F}_{25}$ with generator ξ over $\mathbf{F}_5$, and $D_2 = (1, 2, 0, 0, \xi^3)$. We find that $p_{w_2}(x)$ splits as [1,1,1,1,3,3,3,3] with $k_1 \in \{\xi^{20}, 3, \xi^{16}, 2\}$ and $k_0 \in \{\xi^5, \xi^{22}, \xi^{13}, \xi^2\}$ and

$$\begin{aligned} \tfrac{1}{2}D_2 = \{&(1, \xi^{21}, \xi^{15}, \xi^{22}, \xi^{13}), (1, \xi^8, \xi^2, \xi^{17}, \xi^7) \\ &(1, \xi^9, \xi^3, \xi^2, \xi^5), (1, \xi^{16}, \xi^{10}, \xi, \xi^{23})\}. \end{aligned}$$

5.3. Rank 2 over a big prime field. Take

$$y^2 = x^5 + 2x^3 + 19x^2 + x + 19$$

over the 60-bit prime field $\mathbf{F}_{1152921504606847009}$, and

$$\begin{aligned} D_2 = (&1, 487047376486907768, 887399657010377162, \\ &107397106367603060, 1046421023729122909). \end{aligned}$$

We find that $p_{w_2}(x)$ splits as $[1, 1, 1, 1, 3, 3, 3, 3]$ with

$$\begin{aligned} k_1 \in \{&1073327960591131715, 312451317570481688, \\ &173493032620927706, 125392561284629917\}, \\ k_0 \in \{&57867538720497893, 585543712742483770, \\ &397309658395539060, 786413003132741577\}, \end{aligned}$$

and one of the 4 divisors in $\frac{1}{2}D_2$ is

$$\begin{aligned} (&1, 889060526864891673, 1130483776820005303, \\ &1152033329783565100, 271691093272385826). \end{aligned}$$

Acknowledgements. The authors are partially supported by grants MTM2007-66842-C02-02, MTM2006-15038-C02-01 and 2005SGR 00443.

References

[1] E. Bach and J. Shallit, *Algorithmic number theory. Vol.* 1, MIT Press, Cambridge, 1996.

[2] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265.

[3] D. G. Cantor, Computing in the Jacobian of a hyperelliptic curve, Math. Comp. **48** (1987), no. 177, 95–101.

[4] H. Cohen *et al.*, *Handbook of elliptic and hyperelliptic curve cryptography*, Chapman & Hall/CRC, Boca Raton, 2006.

[5] P. Gaudry and É. Schost, Construction of secure random curves of genus 2 over prime fields, in *Advances in cryptology—EUROCRYPT*, LNCS, 3027, Springer, Berlin 2004, pp. 239–256.

[6] I. Kitamura, M. Katagi and T. Takagi, A complete divisor class halving algorithm for hyperelliptic curve cryptosystems of genus two, in *Information Security and Privacy*, LNCS, 3574, Springer-Verlag, 2005, pp. 146–157.

[7] J. Miret, R. Moreno, J. Pujolàs and A. Rio, Halving for the 2-Sylow subgroup of genus 2 curves over binary fields, (2008). (Submitted).

[8] H. Verdure, Factorisation patterns of division polynomials, Proc. Japan Acad. Ser. A Math. Sci. **80** (2004), no. 5, 79–82.