Finite Fields and Their Applications 36 (2015) 170–188

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Bisection and squares in genus 2 ☆

Josep M. Miret [a], Jordi Pujolàs [a,*], Nicolas Thériault [b]

[a] Departament de Matemàtica, Universitat de Lleida, Lleida, Spain
[b] Departamento de Matemática, Universidad del Bío-Bío, Concepción, Chile

A R T I C L E   I N F O

Article history:
Received 16 July 2014
Received in revised form 8 August 2015
Accepted 10 August 2015
Available online 29 August 2015
Communicated by Igor Shparlinski

MSC:
11G20
11T71
14G50
14H40
14H45

Keywords:
Hyperelliptic curves
Genus 2
Divisor class
Bisection
Efficient computation

A B S T R A C T

We show how to compute the pre-images of multiplication-by-2 in Jacobians of genus 2 curves $C : y^2 = f(x)$ over $\mathbb{F}_q$ with q odd. We characterize $D = [u(x), v(x)] \in 2\mathrm{Jac}(C)(\mathbb{F}_q)$ in terms of the quadratic character of $u(x)$ at the roots of $f(x)$ in imaginary models, and in terms of the quadratic character of the quotients of $u(x)$ at pairs of roots of $f(x)$ in real models. Our method reduces the problem to the computation of at most 5 square roots over the splitting field of $f(x)$ plus the solution of a system of linear equations.

☆ Research of the authors was supported in part by grants MTM2013-46949-P (Spanish Ministerio de Ciencia e Innovación), 2014SGR-1666 (Generalitat de Catalunya) and FONDECYT 1151326 (Chile).

* Corresponding author.
E-mail addresses: miret@matematica.udl.cat (J.M. Miret), jpujolas@matematica.udl.cat (J. Pujolàs), ntheriau@ubiobio.cl (N. Thériault).

http://dx.doi.org/10.1016/j.ffa.2015.08.001
1071-5797/

1. Introduction

We work with divisors D in the Jacobian $\mathrm{Jac}(\mathrm{C})(\mathbb{F}_q)$ of a genus 2 curve $\mathrm{C} : y^2 = f(x)$ over a finite field $\mathbb{F}_q$ of odd characteristic by means of their usual Mumford representation, this is a pair of polynomials $[u(x), v(x)]$ such that $f(x) \equiv v(x)^2$ modulo $u(x)$, with $u(x)$ monic and $\deg(v(x)) < \deg(u(x)) \leq 2$ (see [3]) except if $\deg(f(x)) = 6$ and the support of D contains some of the points at infinity, in which case $\deg(u(x)) = 0, 1$ and $\deg(v(x)) = 3$ (see [11,5]).

Given $D_2 = [u_2(x), v_2(x)] = [x^2 + u_{21}x + u_{20}, v_{21}x + v_{20}] \in \mathrm{Jac}(\mathrm{C})(\mathbb{F}_q)$ and θ a root of $f(x)$, we prove an equivalence between the values $u_2(\theta)$ being squares and the existence of $D_1 = [u_1(x), v_1(x)] = [x^2 + u_{11}x + u_{10}, v_{11}x + v_{10}] \in \mathrm{Jac}(\mathrm{C})(\mathbb{F}_q)$ such that $2D_1 = D_2$. We provide computational details not covered in [3]. Our contribution shows how to compute the bisections D_1 from $\sqrt{u_2(\theta)}$ (see Theorems 2.5, 2.7, 4.7 and 4.8).

As a consequence of the final modular reduction in Cantor's divisor class reduction algorithm (see [2] or [4, p. 308]), if D_1 is a weight 2 bisection of D_2, both defined over $\mathbb{F}_q$, then there exists a linear polynomial $k(x) = k_1x + k_0 \in \mathbb{F}_q[x]$ such that $u_1^2(x)$ and the monic associate of the quotient

$$\frac{f(x) - ((k_1x + k_0)u_2(x) - v_2(x))^2}{u_2(x)} \tag{1}$$

are equal (see [7–9]). This means that for every $D_2 \in 2\mathrm{Jac}(\mathrm{C})(\mathbb{F}_q)$ there exists a coefficient $c = c(k_1, k_0, f_0, \ldots, f_6, u_{21}, u_{20}, v_{21}, v_{20}) \in \mathbb{F}_q$ such that

$$\frac{f(x) - ((k_1x + k_0)u_2(x) - v_2(x))^2}{u_2(x)} = c \cdot u_1^2(x). \tag{2}$$

For (2) to hold we need $D_1 \notin \Theta = \{D \in \mathrm{Jac}(\mathrm{C})(\mathbb{F}_q) \mid \deg(u_D) \leq 1\}$. Given a bisectee D_2, from (2) we obtain the bisections D_1 away from Θ. Any D_1 is fully defined by $u_1(x)$ and $k(x)$ since

$$v_1(x) \equiv k(x)u_2(x) - v_2(x) \bmod u_1(x). \tag{3}$$

Because of the imbalance in degrees that would occur otherwise, $D_1 \notin \Theta$ implies $k_1 \neq 0$ if $f(x)$ has degree 5 and $k_1 \neq \pm\sqrt{f_6}$ if $f(x)$ has degree 6. Bisections $D_1 \in \Theta$ are out of reach with our method. They correspond to the values $k_1 = 0, \pm\sqrt{f_6}$ and they lie at infinity. However, one finds them at almost no cost by other means (see [7,8] for example). Our method does not apply for bisectees $D_2 = \pm(\infty_1 - \infty_2)$ either, but again their bisections are found differently.

As an analogy, let $E : y^2 = g(x)$ be an elliptic curve over $\mathbb{F}_q$ and let $Q \in E(\mathbb{F}_q) \setminus E(\mathbb{F}_q)[2]$. If $P \in E(\mathbb{F}_q)$ is such that $2P = Q$, then (2) is

$$\frac{(k_0(x - x_Q) - y_Q)^2 - g(x)}{(x_Q - x)} = (x - x_P)^2,$$