Discrete Logarithm based PKS

Ernesto Reinaldo Barreiro

Discrete Logarithm based PKS

Ernesto Reinaldo Barreiro

December 15, 2000

Contents

1 Introduction

This are some draft notes intended to support the lectures given by the author at CIMPA's School on Algebraic Geometry and its Applications to Coding Theory an Crytography.

1.1 Jacobian varieties

Let C be a complete non singular curve defined over a field $\mathbb{F}$. A divisor D on C is an element of the free abelian group generated by the set of $\overline{\mathbb{F}}$-points of C, i.e. a formal finite sum of $\overline{\mathbb{F}}$-points $D = \sum m_i P_i$. For $\mathbb{K}$ an algebraic extension of $\mathbb{F}$, we say that the divisor D is defined over $\mathbb{K}$ if for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{K})$ we have $D^\sigma = D$, where $D^\sigma = \sum m_i P_i^\sigma$ and P^σ is nothing but letting act σ in the coordinates of P. For a fixed $\mathbb{K}$, let $\mathbb{D}$ denote the additive group of divisors defined over $\mathbb{K}$, and let $\mathbb{D}^0$ be the subgroup composed by the divisors of degree 0 (the degree of D is defined as the integer $\sum m_i$). Given a $\mathbb{K}$-defined rational function f, by $\mathbb{K}$-defined we mean $f^\sigma = f$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{K})$, it has associated a degree zero divisor (f) (the divisor of zeroes and poles of f). We call such a divisor a principal divisor and denote by $\mathbb{P}$ the subgroup of $\mathbb{D}$ composed of all principal ($\mathbb{K}$-defined) divisors. The quotient $J(C) = \mathbb{D}^0/\mathbb{P}$ is called the jacobian of the curve C.

Let g denote the genus of the curve C and suppose our curve has a point $P_\heartsuit \in C(\mathbb{F})$. Let D be a divisor on $\mathbb{D}^0$, then there exists points $P_1, \ldots, P_g$ and a rational function f such that $D - (\sum_{i=1}^g P_i - gP_\heartsuit) = (f)$. This follows almost directly from Riemann-Roch theorem. Note that it may be possible that some of the points P_i are equal to each other or equal to the point $P_\heartsuit$. From this it follows that any element g of $J(C)$ has a representative, called the reduced representation of g, of the form $\sum_i^s P_s - P_\heartsuit$, with $s \leq g$ and $P_i \neq P_\heartsuit$. Mind that this reduced representation don't has to be (necessarily) unique.

Problem 1.1 *Given $g_1, g_2 \in J(C)$, with reduced representations $D_1 = \sum_{i=1}^{s_1} P_{1i} - s_1 P_\heartsuit$ and $D_2 = \sum_{i=1}^{s_2} P_{2i} - s_2 P_\heartsuit$, $s_1, s_2 \leq g$, respectively, then find a reduced representation $D_3 = \sum_{i=1}^{s_3} P_{3i} - s_3 P_\heartsuit$ of $g_3 = g_1 + g_2$.*

1.2 Jacobian varieties over finite fields

Definition 1.1 *Let C be a non-singular complete curve defined over $\mathbb{F}_q$, and let $M_r = \#C(\mathbb{F}_{q^r})$ for $r \geq 1$. The power series*

$$Z(C/\mathbb{F}_q; T) = \exp(\sum M_r T^r/r), \tag{1}$$

is called the zeta-function *of C.*

Theorem 1.1 (Weil) *Let C be a genus g curve defined over $\mathbb{F}_q$, and let $Z(C/\mathbb{F}_q;T)$ be its* zeta-function. *Then*

1. *$Z(C/\mathbb{F}_q;T)$ is a rational function of the form*

$$Z(C/\mathbb{F}_q;T) = \frac{P(T)}{(1-T)(1-qT)}, \tag{2}$$

where $P(T)$ is a polynomial of degree $2g$ with integer coefficients such that

$$\begin{aligned} P(T) &= 1 + a_1T + \ldots + a_{g-2}T^{g-2} + a_{g-1}T^{g-1} + a_gT^g \\ &\quad + qa_{g-1}T^{g+1} + q^2a_{g-2}T^{g+2} + \ldots + q^{g-1}a_1T^{2g-1} + q^gT^{2g}. \end{aligned}$$

(In fact $P_\pi(T) = T^{2g}P(1/T)$ is nothing but the characteristic polynomial of the frobenius endomorphism π of $J(C)$ relative to $\mathbb{F}_q$.)

2. *The polynomial $P(T)$ factors as*

$$P(T) = \prod_{i=1}^{g}(1-\alpha_iT)(1-\overline{\alpha}_iT),$$

where the α_i's are complex numbers of absolute value $\sqrt{q}$ and $\bar{\cdot}$ denotes complex conjugation.

3. *The numbers $N_r = \#J(C)(\mathbb{F}_{q^r})$ are given by*

$$N_r = \prod_{i=1}^{g}\|1-\alpha_i^r\|^2,$$

where $\|\cdot\|$ denotes the usual absolute value. Note that in particular $N_1 = \prod_{i=1}^{g}\|1-\alpha_i\|^2 = P(1)$

Remark 1.1 *Using equations (1) and (2) we see the numbers $M_1, \ldots, M_g$ are enough to determine $a_1, \ldots, a_g$ and therefore all the numbers N_r for $r \geq 1$.*

2 Elliptic curves

An elliptic curve E (defined) over a field $\mathbb{F}$ is a non singular plane projective curve defined by the equation

$$Y^2W + a_1YXW + a_3YW^2 = X^3 + a_2X^2W + a_4XW^3 + a_6W^3, \tag{3}$$

with $a_i \in \mathbb{F}$. For $\mathbb{K} \supset \mathbb{F}$, let $E(\mathbb{K})$ denotes the set of points $(x:y:w) \in \mathbb{P}(\mathbb{K})$ that satisfy this equation, i.e. the affine $(x,y) := (x:y:1)$ satisfying (3)

and the point at infinity $O = (0 : 1 : 0)$. The non singularity condition amounts to say that there is no affine point $(x, y) \in E(\overline{\mathbb{F}})$ which is also a solution of the system

$$a_1 Y = 3X^2 + 2a_2 + a_4, \;\; 2Y + a_1 X + a_3 = 0.$$

If char $(\mathbb{F}) \neq 2$ then without lost of generality we may suppose $a_1 = a_3 = 0$. Moreover, if char $(\mathbb{F}) \neq 2, 3$ then we may suppose our equation is of the form

$$Y^2 W = X^3 + aXW^2 + bW^3 \tag{4}$$

and the non singularity condition translates to $-(4a^3 + 27b^2) \neq 0$.

For any field $\mathbb{K} \supset \mathbb{F}$, the set $E(\mathbb{K})$ is an abelian group whose identity element is the point O. This group structure is given by (we suppose E is given by equation (4)):

1. Define the point of O as the identity element, i.e. $-O = O$ and for any Q, we have $Q + O = Q$.

2. If $P = (x, y) \neq O$ then define $-P := (x, -y)$. If $Q := -P$ then we define $P + Q = O$.

3. Given P and Q with different x-coordinates, we see the line $l = \overline{PQ}$ intersects E in exactly one more point R. Then we define $P + Q$ as the point $-R$.

4. If $P = Q$, then the tangent line l to E at P intersects E in one more point R. Define $P + Q$ as $-R$.

Remark 2.1 *All these rules may be stated as: the points P, Q and R add to zero iif there exists a projective line intersecting E exactly at P, Q, R. If $P = (x_1, y_1)$ and $P = (x_2, y_2)$ and $R = P + Q = (x_3, y_3)$, then these relations are expressed in coordinates as*

1. *If $P \neq Q$ then*

$$\begin{array}{rcl} x_3 & = & (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2; \\ y_3 & = & -y_1 + (\frac{y_2 - y_1}{x_2 - x_1})(x_1 - x_3). \end{array} \tag{5}$$

2. *If $P = Q$ then*

$$\begin{array}{rcl} x_3 & = & (\frac{3x_1^2 + a}{2y_1})^2 - 2x_1; \\ y_3 & = & -y_1 + (\frac{3x_1^2 + a}{2y_1})(x_1 - x_3). \end{array} \tag{6}$$

2.1 Elliptic curves over finite fields

In the rest of this section $\mathbb{F}$ will be a finite field $\mathbb{F}_q$ with $q = p^f$ elemens. Let E be an elliptic curve defined over $\mathbb{F}_q$, then it is also defined over the fields $\mathbb{F}_{q^r}$ for all $r = 1, 2, \ldots$, and it makes sense to look at the F_q^r-points on E. Let N_r denote the number of F_q^r-points on E. These numbers are used to define the so called *zeta-function* of the elliptic curve E (over $\mathbb{F}_q$) by setting

$$Z(E/\mathbb{F}_q; T) = \exp(\sum N_r T^r / r), \tag{7}$$

where T denotes an indeterminate and the notation $E/\mathbb{F}_q$ is used to stress the fact we are considering E as an elliptic curve defined over F_q.

Theorem 2.1 (Hasse) *The zeta-function of an Elliptic curve $E/\mathbb{F}_q$ is a rational function on T of the form*

$$Z(E/\mathbb{F}_q; T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}.$$

Coefficient a depends on E and it is related to N_1 as follows: $N_1 = q+1-a$. Moreover we have $a \leq 4q$, so that the polynomial $T^2 - aT + q$ has two complex conjugated roots α, $\overline{\alpha}$ with absolute value $q^{1/2}$.

Corollary 2.1 *If N_r denotes the number of $\mathbb{F}_q^r$-points on E and α, $\overline{\alpha}$ the roots of the quadratic polynomial $T^2 - aT + q$. Then*

$$N_r = \|\alpha^r - 1\|^2 = q^r + 1 - \alpha^r - \overline{\alpha}^r, \tag{8}$$

where $\|\|$ denotes the usual complex absolute value.

Corollary 2.2 *The number N_1 of F_q-points on an elliptic curve defined over $\mathbb{F}_q$ is bounded by*

$$q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q}.$$

Example 2.1 *Consider the elliptic curve (over $\mathbb{F}_2$) define by $E : Y^2W + YW^2 = X^3$. This curve has 3 rational points (over $\mathbb{F}_2$), so it follows that its zeta-function has a numerator of the form $1 + 2T^2$. As the roots of this polynomial are $\pm i\sqrt{2}$ we find the number N_r of $\mathbb{F}_{2^r}$-points of E is*

$$N_r = \begin{cases} 2^r + 1, & \text{if } r \text{ is odd} \\ 2^r + 1 - 2(-2)^{r/2}, & \text{if } r \text{ is even.} \end{cases}$$

Taking $r = 101$ we obtain

$$N_r = 3 \cdot 845100400152152934331135470251,$$

or $r = 127$

$$N_r = 3 \cdot 567137278201564105772291012386280352 43,$$

or $r = 167$

$$N_r = 3 \cdot 623574031927851911766905528625614088386531218336 43.$$

For algorithms to compute the size of the group E over $\mathbb{F}_q$ for an arbitrary elliptic curve E the reader may consult: [14], [9], [11] and [10].

3 Hyperelliptic curves

Definition 3.1 *A hyperelliptic curve $\hat{C}$ is the* completion *of a non-singular affine curve defined by an equation*

$$C : v^2 + h(u)v = f(u) \tag{9}$$

where $h(u) \in \mathbb{F}[u]$ is of degree at most g and $f(u) \in \mathbb{F}[u]$ is a monic polynomial of degree $2g + 1$.

Remark 3.1

1. *If $h(u) = 0$ then* char $(\mathbb{F}) \neq 2$. *Moreover, in case* char $(\mathbb{F}) \neq 2$, *by means of change of variables*

$$u \to U, v \to (v - h(u)/2),$$

we may suppose C is of the form $v^2 = f(u)$ where $f(u)$ has degree $2g + 1$.

2. *In case $h(u) = 0$ then the non-singularity conditions is equivalent to impose the condition that $f(u)$ has no repeated roots in $\overline{\mathbb{F}}$.*

3. *By the term* completion *we mean the affine curve C, given by (9), plus one point at infinity ∞. This notion can be made precise, for example in the case $h(u) = 0$, by considering the algebraic curve $\hat{C}$ defined by glueing the curve given by (9) and the curve*

$$C_1 : y^2 = x \prod_{i=1}^{2g+1} (1 - \alpha_i x),$$

where $f(u) = \prod_{i=1}^{2g+1}(u - \alpha_i)$, along the glueing morphism given by $u = 1/x$ and $v = y/x^{g+1}$. Note that the mysterious point ∞ now corresponds to the well defined point $(0, 0)$ on C_1.

4. *Let $\hat{C}$ be a hyperelliptic curve defined as in the previous point. Consider a point $P_0 = (u_0, v_0)$. It follows that the divisor associated to the rational function $u - u_0$ is equal to $(u - u_0) = P_0 + \sigma P_0 - 2\infty$, where $\sigma P_0 = (u_0, -v_0)$ (is called the conjugated of P_0). To see this note $x = 1/u$. Note that if we take P_0 equal to one of the $2g+2$ points $R_1 = (\alpha_1, 0), \ldots, R_{2g+1} = (\alpha_{2g+1}, 0), \infty$ then we have $\sigma P_0 = P_0$ (these are all the ramification points of the covering morphism $(u, v) \mapsto u$).*

3.1 Adding on the Jacobian of an Hyperelliptic curve

For simplicity we are going to suppose char $\mathbb{K} \neq 2$ and our hyperelliptic curve $\hat{C}$ is defined by an affine equation, as in (9), with $h(u) = 0$.

Definition 3.2 *The* greatest commun divisor *of $D = \sum m_i P_i \in \mathbb{D}^0$ and $\hat{D} = \sum \hat{m}_i P_i$ is defined to be $\sum \min(m_i, \hat{m}_i) P_i - (*)\infty$, where the coefficient $(*)$ is chosen so that the greatest common divisor has degree 0.*

Definition 3.3 *A divisor $D = \sum m_i P_i - (*)\infty \in \mathbb{D}^0$ is said to be semi-reduced if:*

a) All the m_i are non-negative, and $m_i \leq 1$ if P_i is a ramification point (i.e. $P_i = \sigma P_i$).

b) If $P_i \neq \sigma P_i$, then P_i and σP_i do not occur both in the sum.

A semi-reduced divisor is called reduced *if it satisfies the additional condition*

c) $\sum m_i \leq g$.

Any *semi-reduced divisor $D = \sum m_i P_i - (*)\infty$* can be uniquely represented as g.c.d. of the divisor of the rational function $a(u) = \prod(u - x_i)$ and the divisor of the rational function $b(u) - v$, where $P_i = (x_i, y_i)$ and $b(u)$ is the unique monic polynomial of degree less than degree of $a(u)$ interpolating the values y_i with multiplicities m_i (i.e. $b(x_i) = y_i$ for each i and $b(u)^2 - f(u)$ is divisible by $a(u)$). That is denoted $D = div(a, b)$.

Theorem 3.1 *For each divisor $D \in \mathbb{D}^0$ there is a unique reduced divisor D_1 such that $D \sim D_1$.*

Proof. See [7, Theorem 6.1.]. ♣

The set $J(C)(\mathbb{F})$ of all divisor classes in $J(C)$ that have a representative that is defined over $\mathbb{F}$ is a finite subgroup of $J(C)$. Each element of $J(C)(\mathbb{F})$ has a unique representation as a reduced divisor $div(a, b)$, where $a(u), b(u) \in \mathbb{F}[u]$ with $\deg_u a(u) \leq g$ and $\deg_u b(u) < \deg_u a(u)$.

Let $D_1 = div(a_1, b_1)$ and $D_2 = div(a_2, b_2)$ be two reduced divisors defined over $\mathbb{F}$. The following algorithm find a semi-reduced divisor $D = div(a, b)$ such that $D \sim D_1 + D_2$. (See [1] and [5]).

Algorithm 1

Input: Semi-reduced divisors $D_1 = div(a_1, b_1)$ and $D_2 = div(a_2, b_2)$, both defined over $\mathbb{F}$.
Output: A semi-reduced divisor $D = div(a, b)$ defined over $\mathbb{F}$ such that $D \sim D_1 + D_2$.

1. Find polynomials $d_1, e_1, e_2 \in \mathbb{F}[u]$, by means of the Euclidean algorithm, such that $d_1 = g.c.d.(a_1, a_2)$ and $d_1 = e_1 a_1 + e_2 a_2$.

2. Find polynomials $d, c_1, c_2 \in \mathbb{F}[u]$ where $d = g.c.d.(d_1, b_1 + b_2)$ and $d = c_1 d_1 + c_2(b_1 + b_2)$.

3. Let $s_1 = c_1 e_1$, $s_2 = c_1 e_2$, and $s_3 = c_2$, so that
$$d = s_1 a_1 + s_2 a_2 + s_3(b_1 + b_2).$$

4. Set
$$a = \frac{a_1 a_2}{d^2}$$
and
$$b = \frac{s_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f)}{d} \mod a,$$
where $(*) \mod a$ denotes the remainder polynomial when $(*)$ is divided by a.

End Algorithm 1.

Remark 3.2 *For a proof of the correctness of the* **Algorithm 1** *see [7, Theorem 7.1.]*

Algorithm 2

Input: Semi-reduced divisors $D = div(a, b)$ defined over $\mathbb{F}$.
Output: The unique reduced divisor $\hat{D} = div(\hat{a}, \hat{b})$ defined over $\mathbb{F}$ such that $D \sim D_1 + D_2$.

1. Set
$$\hat{a} = (f - b^2)/a$$
and
$$\hat{b} = (-b) \mod \hat{a}.$$

2. If $deg_u \hat{a} > g$ then set $a \leftarrow\!\!\prec \hat{a}$, $b \leftarrow\!\!\prec \hat{b}$ and go to step 1.

3. Let c be the leading coefficient of $\hat{a}$, and set $\hat{a} = c^{-1}\hat{a}$.

4. Output$(\hat{a}, \hat{b})$.

End Algorithm 2.

Remark 3.3 *For a proof of the correctness of the* **Algorithm 2** *see [7, Theorem 7.2.]*

Example 3.1 *Let C be the elliptic curve C of genus 2 defined over $\mathbb{F}_2$ b:*

$$C : v^2 + v = u^5 + u^3 + u$$

Counting points over $\mathbb{F}_2$ and $\mathbb{F}_4$ we find the numerator of the zeta-function is $1 + 2T^2 + 4T^4 = (1 - \alpha_1 T)(1 - \overline{\alpha}_1 T)(1 - \alpha_2 T)(1 - \overline{\alpha}_2 T)$, where $\alpha_1 = (\sqrt{2} + \sqrt{6}i)/2$ and $\alpha_2 = (-\sqrt{2} + \sqrt{6}i)/2$. From here it follows

$$N_r = \|1 - \alpha_1^r\|^2 \cdot \|1 - \alpha_2^r\|^2 = \begin{cases} 2^{2r} + 2^r + 1, & \text{if } r \equiv 1, 5 \pmod 6, \\ (2^r + 2^{r/2} + 1)^2, & \text{if } r \equiv 2, 4 \pmod 6, \\ (2^r - 1)^2, & \text{if } r \equiv 3 \pmod 6, \\ (2^{r/2} - 1)^4, & \text{if } r \equiv 0 \pmod 6. \end{cases}$$

For $r = 101$

$$N_r = (7)(607)(15127682224137352558644030052641058393243747785206318539 93).$$

4 Picard Curves

Definition 4.1 *(Picard curves) Let k be any field of characteristic $\neq 3$. Then a Picard curve C is a* non-singular plane projective curve *with model:*

$$Y^3 W = W^4 p_4(X/W) \subset \mathbb{P}_k^2, \tag{10}$$

where $p_4(x) \in k[x]$ is a monic polynomial of degree 4 without multiple roots (in $\overline{k}$).

4.1 The naïve solution to the addition on Picard Jacobians

The problem of making explicit the addition on the jacobian variety of a Picard curve has been completely solved in [13]. In fact the underlying geometric idea supporting the construction given in [13] works for a more general class of plane projective quartics. That is for any *non-singular* plane projective quartic C (defined over a field k) containing a k-rational point $P_\heartsuit$ such that the tangent line to C at $P_\heartsuit$ intersects C only at $P_\heartsuit$; i.e. $P_\heartsuit$ is a k-rational *hyperflex* of C. The precise idea is the following:

1. By Riemann-Roch theorem, any element of $J(C)$ may be represented by a divisor D of the form

$$D = P_1 + P_2 + P_3 - 3P_\heartsuit.$$

Note this does not depends on the fact $P_\heartsuit$ is a hyperflex of C.

2. Suppose given

$$D_1 = P_{11} + P_{12} + P_{13} - 3P_\heartsuit, \qquad D_2 = P_{21} + P_{22} + P_{23} - 3P_\heartsuit,$$

two divisors representing the points $x_1, x_2 \in J(C)$, respectively. Making explicit the addition $x_1 + x_2$ (in $J(C)$) is nothing but finding a rational function $f \in k(C)$ and a divisor

$$D_f = Q_1 + Q_2 + Q_3 - 3P_\heartsuit,$$

such that

$$D_f + (f) = D_1 + D_2,$$

where (f) denotes the principal divisor associated to f and $+$ is the addition as divisors on C.

3. Given a divisor

$$D_0 = P_1 + P_2 + P_3 + P_4 - 4P_\heartsuit,$$

we show how to construct a divisor D_f and a function $f \in k(C)$ such that

$$D_0 + (f) = D_f.$$

First we *interpolate* the curve C with a conic v_0 having zeroes at the points $P_1, \ldots, P_4$ (with the corresponding multiplicities if some point P_i appears more than once at the support of D_0) and having a zero of order at least one at the point $P_\heartsuit$. By Bezout's Theorem, the conic v_0 intersects C (counting multiplicities) in at most three more points M_1, M_2, M_3, then we get

$$D_0 = (v_0/h_\heartsuit^2) - (M_1 + M_2 + M_3 - 3P_\heartsuit);$$

where $h_\heartsuit = \alpha X + \beta Y + \gamma Z$ is the homogeneous equation of the tangent line to C at $P_\heartsuit$. Note that here we strongly use $P_\heartsuit$ is an hyperflex of C. In order to get rid of the $-$ sign we repeat the process: we take a conic v_1 *interpolating* C at the points M_1, M_2, M_3 but now with a zero of order at least two at the point $P_\heartsuit$. The same argument applied, we conclude the existence of points Q_1, Q_2, Q_3 such that

$$D_0 + (v_0/v_1) = Q_1 + Q_2 + Q_3 - 3P_\heartsuit.$$

4. To solve 2 we apply 3 in a recursive way.

4.2 Factorization free addition algorithm for Picard Jacobians

In the previous section we has seen the general strategy in order to solve problem 1.1 for a class of quartics including Picard curves family (in Picard's case the point $P_\heartsuit$ can be chosen as the point $P_\infty = (0:1:0)$. In order to obtain a factorization free addition algorithm we will assign some kind of polynomial coordinates (as in hyperelliptic case) to divisors. Unfortunately, the the way to define these coordinates is not so strightforward as in Hyperelliptic case.

Lemma 4.1 *Let C be a Picard curve. A divisor $D = P_1 + P_2 + P_3$ satisfies $\dim_k \mathcal{L}(D) = 2$ iff P_1, P_2 and P_3 are collinear points of C.*

Proof. The canonical class K is given by the intresection of lines with C (that is true for any quartic). Then a divisor $D = P_1 + P_2 + P_3$ satisfies $l(D) = 2 \iff K \geq D$. ♣

Remark 4.1

1. *Let C be a Picard curve defined over a field k containing a 3^{th} root of unity $\delta \neq 1$. Then the curve C possesses an order three automorphism δ defined by $\delta((x_0 : y_0 : 1)) = (x_0 : \delta y_0 : 1)$ and $\delta((0:1:0)) = (0:1:0)$. This automorphism fixes the points $R_i = (r_i : 0 : 1)$, $i = 1, \ldots, 4$, where the r_i are the zeroes of $p_4(x) \in k[x]$, and also the point $P_\infty = (0:1:0)$. These are also the ramification points of the covering morphism $\pi : C \to \mathbb{P}^1_k$ induced by $k(x) \hookrightarrow k(C)$.*

2. *The divisor associated to the rational function $x - x_0$, where $x = X/W$ and x_0 is a constant such that there exist a point $P = (x_0 : y_0 : 1) \in C$, is equal to $(x - x_0) = P + \delta P + \delta^2 P - 3P_\infty$. Given a divisor $D = P_1 + P_2 + P_3 - 3P_\infty$ such that $\ell(P_1+P_2+P_3) = dim_k \mathcal{L}(P_1+P_2+P_3) = 2$, then $D \sim D_1$, where $D_1 = \delta M + \delta^2 M - 2P_\infty$ and M is the fourth point in which the line r crossing by P_1, P_2 and P_3 (see Lemma 4.1) intersects C.*

Theorem 4.1 *Given a $0 \neq g \in J(C)$ then it has a (unique) representative of one of the following forms*

1. *$P_1 + P_2 + P_3 - 3P_\infty$ with $\ell(P_1 + P_2 + P_3) = 1$ or $P_1 + \delta P_1 - 2P_\infty$ or*
2. *$P_1 + P_2 - 2P_\infty$ with $P_1 \neq \delta^k P_2$, $k = 1, 2$, or*
3. *$P_1 - P_\infty$.*

Proof. *By Remann-Roch Theorem we know there exists points P_1, P_2 and P_3 such that $P_1 + P_2 + P_3 - 3P_\infty \in g$. If some of the points P_i is equal to P_∞ then we obtain cases 2 and 3, if $\ell(P_1 + P_2 + P_3) = 2$ then we apply Remark 4.1.* ♣

Suppose given a divisor $D_0 = P_1 + \ldots + P_4 - 4P_\infty$ and $D_1 = M_1 + M_2 + M_3 - 3P_\infty$ and $D_2 = Q_1 + Q_2 + Q_3 - 3P_\infty$ such that

$$D_0 \sim -D_1 \sim D_2,$$

as in the previous section. We assign some kind of *polynomial coordinates* to the divisors D_i in order to avoid doing factorization in this reduction process.

1. For $D = \sum_{i=1}^{S_1} P_i - S_1 P_\infty$, $1 \leq S_1 \leq 3$, such that $P_i \neq \delta^k P_j$, for $i \neq j$ and $k = 1, 2$, we assign to it the coordinates $\hat{D} = (u(x), v(x, y))$, where

   - $u(x) = \prod_{i=1}^{S_1}(x - x_i)$, where $P_i = (x_i : y_i : 1)$.
   - $v(x, y) = y - b(x)$, where $b(x) \in k[x]$ is the unique monic polynomial interpolating the point P_i, i.e. $b(x_i) = y_i$ with the right multiplicity.

2. Given a divisor $D = P_1 + \ldots + P_4 - 4P_\infty$ we have to consider the cases:

   (a) The points $P_1, \ldots, P_4$, lie in the same line. Then $D_0 \sim 0$.

   (b) $D_0 = P_1 + \delta P_1 + \delta^2 P_1 + P_2 - 4P_\infty$ then $D_0 \sim P_2 - P_\infty$.

   (c) $D_0 = P_1 + \delta P_1 + P_2 + \delta P_2 - 4P_\infty$, where $P_1, P_2 \in C$. In this case $D_0 \sim M_1 + M_2 - 2P_\infty$, where M_1, M_2 are the two other points in which the line $r = \overline{(\delta^2 P_1, \delta^2 P_2)}$ intersects C. That is

   $$D_0 \sim -(\delta^2 P_1 + \delta^2 P_2 - 2P_\infty) \sim (M_1 + M_2 - 2P_\infty).$$

   In coordinates we have $\hat{D}_1 = (u_1 = (x - x_1)(x - x_2), r(x, y))$ and $\hat{D}_1 = (u_2(x), r(x, y))$, where $u_2 = R_y(r, C)/u_1$ and $R_y(*, *)$ means resultant with respect to y.

   (d) Otherwise we assign to D_0 the "polynomial coordinates" $\hat{D}_0 = (u_0(x), v_0(x, y), P_D)$ defined in the following way:

   - $u_0(x) = \prod_{i=1}^{4}(x - x_i)$, where $P_i = (x_i : y_i : 1)$.
   - $v_0(x, y) = a_{20}x^2 + a_{11}xy + a_{10}x + a_{01}y + a_{00}$ is the rational function (in $x = X/W$ and $y = Y/W$) having zeroes (with the right multiplicities) at the points $P_1, \ldots, P_4$ and a number of poles at P_∞ as small as possible (given the restriction we stated for the zeroes of $v(x, y)$). Such a function always exists and the minimality condition for the poles translates to the annilation of some of the coefficients: for example, if the points $P_1, \ldots, P_4$ lie in a line that means forcibly $a_{20} = a_{11} = 0$ (note that in that case $D \sim 0$).

- The point P_D will be equal to P_∞ except in the case $D = P_1 + P_2 + P_3 + \delta P_3 - 4P_\infty$ in which we define $P_D = \delta^2 P_3$. At first it may seems a very strange definition but the problem comes from the fact that the minimal $v(x, y)$, in that case, is of the form $v_0(x, y) = (a_1 y + a_2 y + a_3)(x - x_3)$, x_3 the x-coordinate of the point P_3, and the polynomials $u(x)$ and $v(x, y)$ do not provide enough information to recover D in a unique way (for example the divisor $D = P_1 + P_2 + P_3 + \delta^2 P_3 - 4P_\infty$ gives the same u and v). This difficulty can be overcome also by using a third polynomial $w(y) = \prod_{i=4}(y - y_i)$ but in practice is simpler, and more efficient, to use P_D.

Given these coordinates $\hat{D}_0$ we proceed to compute $\hat{D}_1$ and $\hat{D}_1$ (or in some cases the divisors D_1 and D_2) by:

- Set $u_1 := R_y(v_0, C)/u_0$. To get v_1 we try to solve the linear system
$$R_y(v_1, v_0) = \lambda \cdot u_1, \qquad 0 \neq \lambda \in k.$$
In case we can not solve the system we recover D_1 and D_2 explicitly.
- We set $u_2 = R_y(v_1, C)/u_1$ and $v_2 = v_1$.

3. The points 1. and 2. show how to efficiently reduce a degree 4 divisor. So, in order to completely solve the problem of the reduction of and arbitrary divisor we have to show how to compute from $\hat{D}_2$ and a divisor of the form $E := Q - P_\infty$ the coordinates corresponding to the divisor $D_0 := D_2 + E$ (mind that we don't know necessarily the points in the support of D_2, only its coordinates). We proceed as follows:

   - We set $u_0 = u_2 \cdot (x - x_Q)$, where $Q = (x_Q : y_Q : 1)$.
   - We try to find v_0 by solving the system
$$\begin{cases} R_y(v_0, v_2) &= \lambda \cdot u_2 \\ v_0(x_Q, y_Q) &= 0 \end{cases}$$
   In case the system has no solution we obtain D_0 explicitly.

4. Now given an arbitrary divisor $D = \sum_{i=0}^{N} P_i - NP_\infty$, $N > 3$, we find its reduction by means of the following algorithm

   A.0. **Input**: $D = \sum_{i=0}^{N} P_i - NP_\infty$.

   A.1. Set $D = P_1 + \ldots + P_4 - 4P_\infty$ and $D = D - (D_0)$ and $I := 5$

   A.2. Compute $\hat{D}_0$,

   A.3. Compute $\hat{D}_1$, and $\hat{D}_2$.

A.4. If $\deg\ D_+ > 0$ then set $\hat{D}_0 = \hat{D}_2 + (P_I - P_\infty)$, $D = D - (P_I - P_\infty)$, $I = I + 1$ and go step A.3. Else finish with output $\hat{D}_2$

A.5. **Output**: The coordinates $\hat{D}_2$.

Of course this is a simplified version of the real algorithm.

Remark 4.2 *For C a genus 3 curve defined over $\mathbb{F}_q$ let $P_\pi(\lambda) = \sum_{i=0}^{6} a_i \lambda^i$ be the characteristic polynomial of the Frobenius endomorphism π of $J(C)$ relative to $\mathbb{F}_q$ and $\mu_r = N_r - (q^r + 1)$, $r = 1, 2, 3$, where the N_r are the number of $\mathbb{F}_{q^r}$-rational points of C. Then we have*

1. $a_6 = 1$ *and* $a_0 = q^3$
2. $a_5 = \mu_1$, $a_4 = \frac{1}{2}(\mu_2 + \mu_1^2)$ *and* $a_3 = \frac{1}{3}\mu_3 + \frac{1}{2}\mu_2\mu_1 + \frac{1}{6}\mu_1^3$.
3. $a_1 = q^2 a_5$ *and* $a_2 = q a_4$.

Therefore, $P_\pi(\lambda)$ is completely determined by the numbers N_1, N_2 and N_3.

Example 4.1 *Let C be the Picard curve defined by the equation $Y^3W = X^4 + X^2W^2 + XW^3 + W^4$ over $\mathbb{F}_2$. By direct computation we find $\mu_1 = \mu_2 = \mu_3 = 0$ and $P_\pi(\lambda) = (\lambda^2 + 2)(\lambda^4 - 2\lambda^2 + 4)$. The roots of $P_\pi(\lambda)$ are*

$$i\sqrt{2}, -i\sqrt{2}, \sqrt{1 - i\sqrt{3}}, -\sqrt{1 - i\sqrt{3}}, \sqrt{1 + i\sqrt{3}}, -\sqrt{1 + i\sqrt{3}}.$$

That gives

$$N_r = \begin{cases} (1+2^r)(1+2\sum_{j=0}^{s} 3^{2*j} + 2^{4s+2}) & r = 2s+1 \\ \\ (1+2^r-2(-2)^{r/2})(1+2\sum_{j=0}^{s} 3^{2j} + 2^{4s+2} - 4(2^{4s}+1)\sum_{0\le j\le s}{}' 3^{j/2} + 2^{8s}) & r = 2s, \end{cases}$$

where $\sum'$ means j takes only even values. For example, if we take $r = 101$ we obtain $N_{101} = A \cdot B$ where

$$A = (3)(845100400152152934331135470251),$$

and

$$B = (17)(293)(647)(19945195691191041263104264194230137730891404719680539 01).$$

It follows from the above prime decomposition that $J(C)(\mathbb{F}_{2^{101}})$ is a cyclic abelian group.

References

[1] D.Cantor, Computing in the Jacobian of a hyperelliptic curve, Math. of Computation, 48 (1987), 95-101.

[2] J. Buchmann, T. Hoeholdt, H.Tapia-Recillas, H. Stichtenoth, Eds., Coding Theory, Cryptography and Related Areas, Springer-Verlag. Proceedings of an International Conference on Coding Theory, Cryptography and Related Areas, held in Guanajuato, in April 1998.

[3] S.D. Galbraith, S. Paulus, and N. P. Smart, Arithemetic of Superelliptic curves,...

[4] Huang, M.-D and Ierardi, D.J., Efficient Algorithms for the effective Riemann-Roch problem and for addition in the Jacobian of a curve, J. Symbolic Comp., Vol. 18, 519-539, 1994.

[5] N. Koblitz, Hyperelliptic cryptosystemsm J. Cryptology 1, 139-150, 1989.

[6] N. Koblitz, A Course in Number Theory and Cryptography, "nd ed., Springer-Verlag, 1994.

[7] N. Koblitz, Algebraic Aspects of Cryptography, Algorithm and Computation in Mathematics, Springer-Verlag, 1998.

[8] G. Lachaud, Courves diagonales et courves de Picard, preprint Num. 97-30, IML-Luminy.

[9] R. Lercier, F. Morain. Counting the number of points on elliptic curves over fields: strategies and perfonmances, Advandces in Cyptology- Eurocrypt'95, Springer-Verlag, 79-94, (1995).

[10] F. Lehmann, M. Maurer, V. Müller, V. Shoup, Counting the number of points on elliptic curves over finite fields of characteristic greater than three., Algorithmic Number Theory, Lect. Notes Comp. Sci., 877, Springer-Verlag, 60-70, 1994.

[11] R. Lercier, F. Morain. Counting ponts on elliptic curves over $\mathbb{F}_{p^n}$ using Couvignes' algorithm, preprint.

[12] D. Mumford, Abelian Varieties, Tata Inst. Fund. Research.
and Oxford Univ. Press, 1974. (2nd Edition).

[13] E. Reinaldo-Barreiro, J. Estrada-Sarlabous and J.-P. Cherdieu, Efficient Reduction on the Jacobian Variety of Picard Curves. In [2].

[14] Elliptic curves over finite fields and the computation of square roots mod p, Math. Comp. 44, 483-494, 1985.