Trisection for supersingular genus 2 curves in characteristic 2

Josep Miret\textsuperscript{1}, Jordi Pujolàs\textsuperscript{1}, and Nicolas Thériault\textsuperscript{2}

\textsuperscript{1}Departament de Matemàtica, Universitat de Lleida, España.
\textsuperscript{2}Departamento de Matemática, Universidad del Bío-Bío, Chile.
Introduction

3-torsions

Trisections
- General case
- Special cases

Structure of $\text{Jac}(C)[3^\infty](\mathbb{F}_{2^m})$
- Structure of $\text{Jac}(C)[3](\mathbb{F}_{2^m})$
- Structure of $\text{Jac}(C)[3^k](\mathbb{F}_{2^m})$, $k > 1$
Let $\mathbb{F}_q$ be a finite field of characteristic 2, then a super singular curve of genus 2 can be given by an equation of the form

$$y^2 + h_0 y = x^5 + f_3 x^3 + f_1 x + f_0$$

with $h_0 \neq 0$.

From a hyper elliptic curve, we can define the divisor class group: the quotient group of the divisors of degree zero modulo the principal divisors.

The reduced divisors in each class group can be given in Mumford representation,

$$D = [u(x), v(x)],$$

with $u$ monic of degree at most 2, $\deg(v) < \deg(u)$, and satisfying $u|v^2 + h_0 v + f$. 
Trisections

Given a reduced divisor $D_3 = [u_3(x), v_3(x)]$, we want to find all the possible reduced divisors $D_1 = [u_1(x), v_1(x)]$ such that

$$D_3 = 3D_1,$$

the trisections of $D_3$.

From the group structure, we know that

$$Jac(C)[3] \equiv (\mathbb{Z}/3\mathbb{Z})^4.$$

Over $\overline{\mathbb{F}}_q$, the problem consists in computing the 81 trisections of $D_3$.

Over $\mathbb{F}_q$, we have to identify which of the 81 trisections are defined over $\mathbb{F}_q$. 
3-torsions

We are looking for the non-zero trisections of the divisor class $0$ (Mumford representation: $[1, 0]$), i.e. divisors $D$ such that $3D \equiv 0$.

We first observe that for curves of genus 2, $D$ must have weight 2, so $D = [u(x), v(x)] = [x^2 + u_1x + u_0, v_1x + v_0]$.

Rather than solve $3D = 0$, we will solve $2D \equiv -D = [x^2 + u_1x + u_0, v_1x + (v_0 + h_0)]$.

To do this we look for an auxiliary polynomial $k(x)$ such that $\tilde{v}(x)$ in $2D = [u(x)^2, \tilde{v}(x)]$ is of the form $\tilde{v}(x) = v(x) + k(x)u(x)$.
3-torsions

The coefficients of $x^0$, $x^1$, $x^2$, and $x^3$ in

$$k_1^2 u(x)^2 = \frac{v^2(x) + h_0 v(x) + f(x)}{u(x)} + h_0 k(x) + k^2(x) u(x).$$

give us 4 equations in $\{u_1, u_0, v_1, v_0, k_1, k_0\}$, and the divisibility condition

$$v(x)^2 + h_0 v(x) + f(x) \equiv 0 \mod u(x)$$

gives us two more, completing the system.

In the system, $u_1$, $u_0$, and $v_1$ can be written in terms of $k_1$, $k_0$ and $v_0$. 
3-torsions

$k_1$ satisfies the degree 5 equation

$$h_0 k_1^5 + f_3 k_1^4 + 1 = 0,$$

$k_0$ satisfies a degree 8 equation (depending on $k_1$)

$$k_1^4 k_0^8 + h_0^2 k_1^{10} k_0^4 + h_0^2 k_1^8 k_0^2 + h_0^3 k_1^{12} k_0 + f_1^2 k_1^{12} + f_3 h_0^2 k_1^{10} + h_0^2 k_1^6 = 0,$$

and $v_0$ satisfies a degree 2 equation (depending on $k_1$ and $k_0$)

$$k_1^2 v_0^2 + h_0 k_1^2 v_0 + k_1^2 f_0 + h_0 k_0^3 = 0.$$

**Theorem**

There is a bijection between triples of solutions $(k_1, k_0, v_0) \in \mathbb{F}_2^m \times \mathbb{F}_2^m \times \mathbb{F}_2^m$ satisfying the three equations above, and the set of divisors of order 3 in $\text{Jac}(C)(\mathbb{F}_2^m)$. 
Factorization types

\( P_{u_1}(X) \) is the translate of a 2-linearized polynomial

\[ \iff \text{The number of roots is } 0, 1, 2, 4, 8 \text{ in any field extension.} \]

**Proposition**

The possible **factorization types** of \( P_{u_1}(X) \):

- \([1, 1, 1, 1, 2, 2], [1, 1, 2, 4], [2, 2, 2, 2], [4, 4] \text{ if } m \text{ is odd.}\)
- \([1, 1, 1, 1, 1, 1, 1], [1, 1, 1, 1, 2, 2], [1, 1, 3, 3], [2, 2, 2, 2], [2, 6], [4, 4] \text{ if } m \text{ is even.}\)

**Direct consequences:**

**Corollary**

- **if 3-torsion subgroup of rank 4, then** \( m \text{ is even.} \)
- **if** \( P_{u_1}(X) \) **has 8 linear factors, then** \( m \text{ is even.} \)

In general, restricts the possible extension degrees where the 3-torsion divisors are defined.
Reducing $3D_1$ (Cantor)

Suppose that we obtain $3D_1 = [u_1^3(x), \tilde{v}(x)]$ using Cantor’s composition algorithm ($D_1$ is not of order 3), then the simple reduction of Cantor works as follows (assuming $\tilde{v}(x)$ has degree 5):

$$u_a(x) = \text{Monic} \left( \frac{\tilde{v}^2 + h\tilde{v} + f}{u_1^3} \right)$$

$$v_a(x) = \tilde{v} + h \mod u_a(x)$$

$$u_3(x) = \text{Monic} \left( \frac{v_a^2 + hv_a + f}{u_a} \right)$$

$$v_3(x) = v_a + h \mod u_3(x).$$

We refer to this as double linear reduction.

Special cases:

- $D_1$ of weight 1
- $3D_1 = [u_1^3(x), \tilde{v}(x)]$ with $\tilde{v}(x)$ of degree $\leq 4$ (simple quadratic reduction)
- $D_3$ of weight 1 ($v_a(x)$ has degree $\leq 2$).
De-reduction

Our goal is to go from $D_3 = [u_3, v_3]$ to $3D_1 = [u_3^3(x), \tilde{v}(x)]$, or rather to $D_1 = [u_1, v_1]$ with $v_1 = \tilde{v} \mod u_1$, undoing the reduction algorithm.

There should be 81 valid solutions over $\overline{\mathbb{F}}_q$, and either 0 or $3^r$ solutions over $\mathbb{F}_q$ where $r$ is the 3-rank of the curve over $\mathbb{F}_q$.

Writing $v_a(x)$ and $\tilde{v}(x)$ as

$$v_a(x) = v_3(x) + (k_1x + k_0)u_3(x) + h(x)$$
$$\tilde{v}(x) = v_a(x) + (k_3x + k_2)u_a(x) + h(x)$$

where $k_1 \cdot k_3 \neq 0$.

Then de-reducing comes down to finding $k_1x + k_0$ and $k_3x + k_2$ which connect $[u_3, v_3]$ and $[u_1, v_1]$ (via $[u_a, v_a]$).

This is similar to the de-reduction technique used for bisections in genus 2 curves, hence the name double linear de-reduction.
General case

Using the representations of $v_a(x)$ and $\tilde{v}(x)$ into the equations for the $u(x)$-terms, we obtain

$$u_a(x) = \frac{1}{k_1^2} \left( \frac{v_3^2 + v_3 h + f}{u_3} + (k_1 x + k_0)^2 u_3 + (k_1 x + k_0) h \right)$$

and then

$$u_1(x)^3 = \frac{1}{k_1^3} \left( k_1^2 u_3 + (k_3 x + k_2)^2 u_a + (k_3 x + k_2) h \right).$$

Expanding this last equality according to the degrees in $x$, we obtain 6 equations en $u_{11}$, $u_{10}$, $k_0$, $k_1$, $k_2$, and $k_3$.

To simplify the equations, we make the substitutions

$$t_1 = 1/k_1$$

$$t_3 = 1/k_3$$

$$z = t_3 k_2 = k_2/k_3$$
General case

From the coefficients of $x^5$ and $x^4$ we get:

$$u_{11} = u_{31} + t_1^2$$

$$u_{10} = u_{30} + u_{31}^2 + z^2 + k_0^2 t_1^2 + u_{31} t_1^2 + t_1^4$$

and then the coefficients of $x^2$ and $x^3$ can be combined to find $k_0$:

$$k_0 = \frac{1}{h_0 u_{31}^2 t_1^4} \left( t_1^{14} + u_{31} t_1^{12} + t_1^6 z^4 + u_{31}^2 t_1^6 z^2 + u_{31}^4 t_1^6 + f_3 u_{31} t_1^8 
+ u_{31} t_1^4 z^4 + h_0 u_{31} t_1^7 + u_{31}^2 t_1^2 z^4 + u_{31}^4 t_1^2 z^2 
+ u_{31} v_{31}^2 t_1^4 + u_{31}^3 u_{30} t_1^4 + f_3 u_{31} t_1^4 z^2 + u_{30}^2 t_1^6 + f_3 t_1^6 
+ h_0 u_{31} t_1^3 z^2 + h_0 u_{31}^3 t_1^3 + u_{31} u_{30}^2 t_1^4 + f_3 u_{31} u_{30} t_1^4 
+ u_{31} u_{30} t_1^2 + h_0 u_{31} u_{30} t_1^2 + h_0^2 t_1^4 + u_{31}^2 t_3^2 \right)$$

Remark

The case $u_{31} = 0$ must be handled separately and is easier than the case $u_{31} \neq 0$. 
General case

The coefficients in $x^2$ and $x^3$ also leave us an equation

$$0 = t_1^{28} + u_{31}^2 t_1^{24} + t_1^{12} z^8 + u_{31}^4 t_1^{12} z^4 + u_{31}^8 t_1^{12} + f_3^2 u_{31}^2 t_1^{16} + u_{31}^2 t_1^8 z^8$$

$$+ h_0^2 u_{31}^2 t_1^{14} + h_0^2 u_{31}^3 t_1^{12} + u_{31}^4 t_1^4 z^8 + u_{31}^8 t_1^4 z^4 + u_{31}^4 v_{31}^4 t_1^8 + u_{31}^6 u_{30}^2 t_1^8$$

$$+ f_3^2 u_{31}^2 t_1^8 z^4 + h_0^2 u_{31}^4 t_1^{10} + u_{30}^4 t_1^{12} + f_3^4 t_1^{12} + h_0^2 u_{31}^3 t_1^8 z^2 + h_0^2 u_{31}^2 t_1^6 z^4$$

$$+ h_0^2 u_{31}^4 t_1^6 z^2 + u_{31}^2 u_{30}^4 t_1^8 + f_3^2 u_{31}^2 u_{30}^2 t_1^8 + h_0^2 u_{31}^3 u_{30}^8 t_1 + f_3^2 h_0^2 u_{31}^3 t_1^8$$

$$+ h_0^3 u_{31}^3 t_1^7 + u_{31}^4 u_{30}^4 t_1^4 + h_0^2 u_{31}^2 u_{30}^2 t_1^6 + h_0^4 t_1^8 + u_{31}^4 t_1^4$$

and substituting $k_0$ in the coefficients of $x^0$ and $x^1$ gives us two more equations in $z$, $t_1$ and $t_3$.

After some careful combinations, we can write $t_3$ in terms of $t_1$ and $z$, and obtain

$$p_1(t_1, z) = 0$$

$$p_2(t_1, z) = 0$$

with $p_1$ of degree 33 in $t_1$ and degree 12 in $z$, and $p_2$ of degree 15 in $t_1$ and degree 2 in $z$. 
General case

Taking the resultant (in $z$) of $p_1$ and $p_2$ and cleaning out “parasitic” factors, we find

$$\text{Res}_z(p_1(t_1, z), p_2(t_1, z)) = t_1^9 \cdot (t_1^5 + (u_{31}^2 + f_3)t_1 + h_0)^{12} \cdot q_{D_3}(t_1)$$

where $q_{D_3}(t_1)$ is a polynomial of degree 81 (except in some special cases).

Proposition

Each non-zero root $t_1$ of $q_{D_3}(X) = 0$ corresponds to a trisection $D_1$ of $D_3$ via double linear de-reduction.
Weight-1 trisections

If \( D_1 = [x + u_{10}, v_{10}] \), the reduction of \( 3D \) takes only one simple step. Setting \( \tilde{v}(x) = v_3(x) + k_0 u_3(x) + h(x) \), we obtain the equality

\[
(x + u_{10})^3 = \frac{v_3(x)^2 + v_3(x)h_0 + f(x)}{u_3(x)} + k_0^2 u_3(x) + k_0 h_0,
\]

which turns into 3 equations, first

\[
u_{10} = k_0^2 + u_{31},
\]

and then

\[
s_1(k_0) = k_0^4 + k_0^2 u_{31} + f_3 + u_{30}
\]
\[
s_2(k_0) = \left(u_{31}^2 + f_3\right) k_0^2 + h_0 k_0 + v_{31}^2 + u_{31} f_3
\]

Proposition

\( D_3 \) admits a trisection of weight 1 if and only if

\[
f_3^6 + f_3^4 u_{30}^2 + f_3^3 h_0^2 u_{31} + f_3^2 h_0^2 u_{31}^3 + f_3^2 h_0^2 u_{31} u_{30} + f_3^2 u_{31}^2 v_{31}^4 + f_3 h_0^4
\]
\[
+ f_3 h_0^2 u_{31}^5 + h_0^4 u_{30} + h_0^2 u_{31}^5 u_{30} + h_0^2 u_{31} v_{31}^4 + u_{31}^8 u_{30}^2 + u_{31}^6 v_{31}^4 + v_{31}^8 = 0
\]
Weight-1 trisectees

If $D_3 = [x + u_{31}, v_{31}]$ ($D_3$ has weight 1), the process is similar to the general case (double linear de-reduction), except that no special case can occur. (all trisections have weight 2 and all de-reductions are linear).

$$u_a = \frac{v_3^2 + v_3 h + f}{u_3} + (k_1 x + k_0)^2 u_3 + (k_1 x + k_0) h$$

$$(x^2 + u_{11} x + u_{10})^3 = \frac{u_3}{k_3^2} + \left(\frac{k_3 x + k_2}{k_3^2}\right)^2 u_a + \left(\frac{k_3 x + k_2}{k_3^2}\right) h$$

From which we get $u_{11}$, $u_{10}$ and $k_0$ in terms of $k_1$ and $t_0 = \frac{k_2}{k_3}$:

$$u_{11} = k_1^2 + u_{30}$$
$$u_{10} = k_1^4 + k_1^2 u_{30} + f_3 + t_0^2$$
$$k_0^2 = k_1^6 + k_1^2 f_3 + k_1 h_0$$

with the final three equations in terms of $k_1$, $t_0$ and $t_1 = \frac{1}{k_3}$.

Since one equation does not depend on $t_1$, solving the can be reduced (via two resultants) to a degree 81 polynomial in $k_1$. 
Simple quadratic de-reduction

In some cases, $D_1$ and $D_3$ both have weight 2, but $\tilde{v}$ in $3D_1 = [u_1^3, \tilde{v}]$ is of degree $\leq 4$. In this case, the reduction requires only one step, and we can write

$$\tilde{v}(x) = v_3(x) + (k_2x^2 + k_1x + k_0)u_3 + h(x)$$

Proposition

$D_3 = [x^2 + u_31x + u_30, v_31x + v_30]$ admits a simple quadratic de-reduction only if

$$u_{31}^5 + f_3^2u_{31} + h_0^2 = 0$$

and the associated $D_1$ has $u_{11} = u_{31}$.

working out the equations, we obtain a degree 9 trisection polynomial

$$p_{D_3}(t) = t^9 + u_{31}^4h_0^2t^3 + (u_{31}^{12} + u_{31}^6v_{31}^4 + u_{31}^8f_3^2 + u_{31}^5h_0^2u_{30})t + u_{31}^6h_0^3.$$ 

and $u_{10} = u_{30} + t^2/u_{31}$

Remark

If $u_{31}^5 + f_3^2u_{31} + h_0^2 = 0$, then the trisection polynomial for double linear de-reduction has degree 72 after removing 9 (false) roots $t_1 = 0$. 
Goals

- A supersingular curves of genus 2 over any field $\mathbb{F}_{2^m}$ with a 3-torsion subgroup of rank 3
- The exponents of $\text{Jac}(C)[3^\infty](\mathbb{F}_{2^m})$ are equal
- $\text{Jac}(C)[3^k](\mathbb{F}_{2^m})$ has a distinguished basis for every $k$

For curves with coefficients in $\mathbb{F}_2$, the first two results follow from C. Xing’s *On supersingular abelian varieties of dimension two over finite fields* (1996).
Structure of the group

Supersingular curves have simplified equation.

\[
D = \left[ x^2 + u_1 x + u_0, v_1 x + v_0 \right], \quad D' = \left[ x^2 + u_1 x + u'_0, v'_1 x + v'_0 \right]
\]

\[ \Rightarrow u_1(\pm(D + D')) = u_1(\pm(D - D')) \]

by direct computation + supersingularity.

Proposition

If \( P_{u_1}(X) \) has more than 4 roots (type \([1, \ldots, 1]\)), then \( \text{rank}(\text{Jac}(C)[3]) \neq 3 \):

if 3-torsion has 3 generators \( D_1, D_2, D_3 \) with the same \( u_1 \), there must be 5 other divisors in \( \langle D_1, D_2, D_3 \rangle \) with same \( u_1 \), but they go together in pairs by property above!
There are no supersingular $C$ in characteristic 2 such that $\text{Jac}(C)[3]$ has rank 3

- We can assume factorization type is not $[1, \ldots, 1]$
- for each $u_1$ obtain at most 4 $u_0$'s, so need the 5 $u_1$'s over $\mathbb{F}_{2^m}$.
- $40 - 13 = 27$ remaining pairs $(u_1, u_0)$ to be found over extension of degree 2, 3, 6 because of factorization types.
- But we need $26/2 = 13$ first coordinates over $\mathbb{F}_{2^m}$. This leads to contradiction for every $m = 2, 3, 6$. 
Distinguished Bases

Corollary (B)

There exists a basis of $\text{Jac}(C)[3]$ with elements having the same $u_1$.

- In rank 4, there must exist a root $u_1$ leading 8 $u_0$'s. From the divisors with these first components $x^2 + u_1 x + u_0$ there exists a basis of $\text{Jac}(C)[3]$
- In rank 2, it follows from the factorization types of $P_{u_1}(x)$

Call such divisors “distinguished”
Quadratic De-reductions

Consider the situation:

- \( D = [x^2 + u_1 x + u_0, v_1 x + v_0] \) a divisor such that \( u_1 \) satisfies
  \[ u_1^5 + f_3^2 u_1 + h_0^2 = 0 \]

- \( p_D(t) = t^9 + \ldots + u_{31}^6 h_0^3 \)
  the degree 9 quadratic-dereduction polynomial

- \( q_D(t_1) = (...) t_1^{72} + \ldots + h_0^{24} \)
  the degree 72 twice-linear-dereduction polynomial.

**Proposition (D)**

*If \( q_D(t_1) \) has a root \( \alpha_1 \in \mathbb{F}_{2^m} \) then \( p_D(t) \) has a root \( \beta_1 \in \mathbb{F}_{2^m} \).*

That is, if \( D \) has a trisection by twice-linear-dereduction \( D \) only if it has a trisection by quadratic-dereduction.
### Theorem

The nonzero exponents of $\text{Jac}(C)(\mathbb{F}_2)[3^\infty]$ are equal.

### Corollary

For every $k$, there is a distinguished basis of $\text{Jac}(C)[3^k](\mathbb{F}_2)$.

**Sketch:**

- By Corollary (B), we can take a distinguished basis in $\text{Jac}(C)[3]$.
- By Proposition (D), if a distinguished divisor has a trisection, it has a distinguished trisection (this is not trivial in rank 2).
- Prove by induction: For $D = [x^2 + u_{31}x + u_{30}, v_{31}x + v_{30}] \in \text{Jac}(C)[3^k](\mathbb{F}_2)$, $D$ distinguished of order $3^k$, $\Longrightarrow p_D(x)$ does not depend on undistinguished coefficients $u_{30}, v_{31}, v_{30}$ but only on $u_{31}$ and $k$. 
Group Structure

- $k = 1$: in 3-torsion the only "wrong" coefficients satisfy
  \[ h_0^2 u_{30} + v_{31}^4 u_{31} = f_3^2 u_{31}^3 + u_{31}^7 \]

- troubled coefficients in next level $p_{D'}(x)$ are
  \[ h_0^2 u_{11} + u_{31} v_{11}^4 = h_0^2 u_{30} + u_{31} v_{31}^4 + \left( \frac{h_0^2}{u_{31}} t^2 + (u_{31} + 1)^4 t^4 + \frac{(f_3 + u_{31}^2)^4}{h_0^2} t^8 \right) \]

By induction hypothesis there exists a formula by which $h_0^2 u_{30} + u_{31} v_{31}^4$ depends only on $u_{31}$, and $t$ (a root of $p_D(x) = p_{u_{31}}^k(x)$), then clearly $p_{D'}(x) = p_{u_{31}}^{k+1}(x)$ for any $D'$.

Hence $p_D(x)$ is the same for all distinguished $D$ of order $3^k$: $p_D(x) = p_{u_{31}}^k(x)$. 
It only remains to show: if $\frac{1}{3} \tilde{D} \neq \emptyset$ for some undistinguished $\tilde{D}$, does there exist a distinguished $D$ of the same order such that $\frac{1}{3} D \neq \emptyset$?

By induction, suppose there exists a distinguished $D \in \text{Jac}(C)[3^k](\mathbb{F}_2^m)$ such that $3^{k-1} D$ equals any distinguished basis elements in $\text{Jac}(C)[3](\mathbb{F}_2^m)$.

Let $\tilde{D} \in \text{Jac}(C)[3^k](\mathbb{F}_2^m)$ be undistinguished of order $3^k$ such that $\frac{1}{3} \tilde{D} \neq \emptyset$. By definition of $k$, $\text{Jac}(C)[3^k]$ must also contain a distinguished $D$ such that $3^{k-1} \tilde{D} = 3^{k-1} D$.

$\implies$ there exists an $E$ of order $3^s$ with $s < k$ such that $D = \tilde{D} + E$. Therefore $\frac{1}{3} E \neq \emptyset$, hence $\frac{1}{3} D \neq \emptyset$ and our proof is complete.