Division polynomials for hyperelliptic curves defined by Dickson polynomials

E. Malygina and S. Novoselov

Immanuel Kant Baltic Federal University
Kaliningrad

June 7, 2019
CTCrypt'19

Plan

- Main definitions and notations.
- Cryptographic applications.
- Actual research results.
- Why Dickson polynomials?
- Obtaining of division polynomials.

Introduction: Main definitions and notations

- Let $\mathbb{F}_q$ be a finite field of size $q = p^n$, $p > 2$.

Introduction: Main definitions and notations

- Let $\mathbb{F}_q$ be a finite field of size $q = p^n$, $p > 2$.
- A hyperelliptic curve C of genus g is a nonsingular curve defined by equation

$$y^2 = f(x),$$

where f is a monic polynomial of degree $2g + 1$ or $2g + 2$.

Introduction: Main definitions and notations

- Let $\mathbb{F}_q$ be a finite field of size $q = p^n$, $p > 2$.
- A hyperelliptic curve C of genus g is a nonsingular curve defined by equation

$$y^2 = f(x),$$

  where f is a monic polynomial of degree $2g + 1$ or $2g + 2$.
- A divisor: $D = \sum_{P \in C} n_P P$.

Introduction: Main definitions and notations

- Let $\mathbb{F}_q$ be a finite field of size $q = p^n$, $p > 2$.
- A hyperelliptic curve C of genus g is a nonsingular curve defined by equation

$$y^2 = f(x),$$

  where f is a monic polynomial of degree $2g + 1$ or $2g + 2$.
- A divisor: $D = \sum_{P \in C} n_P P$.
- A degree of divisor: $\deg D = \sum n_P$.

Introduction: Main definitions and notations

- Let $\mathbb{F}_q$ be a finite field of size $q = p^n$, $p > 2$.
- A hyperelliptic curve C of genus g is a nonsingular curve defined by equation

$$y^2 = f(x),$$

  where f is a monic polynomial of degree $2g + 1$ or $2g + 2$.
- A divisor: $D = \sum_{P \in C} n_P P$.
- A degree of divisor: $\deg D = \sum n_P$.
- A group of divisors of degree 0: $\mathbb{D}^0$.

Introduction: Main definitions and notations

- Let $\mathbb{F}_q$ be a finite field of size $q = p^n$, $p > 2$.
- A hyperelliptic curve C of genus g is a nonsingular curve defined by equation

$$y^2 = f(x),$$

  where f is a monic polynomial of degree $2g + 1$ or $2g + 2$.
- A divisor: $D = \sum_{P \in C} n_P P$.
- A degree of divisor: $\deg D = \sum n_P$.
- A group of divisors of degree 0: $\mathbb{D}^0$.
- A principal divisor: $D = \mathrm{div} R = \sum_{P \in C} (\mathrm{ord}_P R) P$ for some rational function $R \in \bar{\mathbb{F}}_q(C)$.

Introduction: Main definitions and notations

- Let $\mathbb{F}_q$ be a finite field of size $q = p^n$, $p > 2$.
- A hyperelliptic curve C of genus g is a nonsingular curve defined by equation

$$y^2 = f(x),$$

  where f is a monic polynomial of degree $2g + 1$ or $2g + 2$.
- A divisor: $D = \sum_{P \in C} n_P P$.
- A degree of divisor: $\deg D = \sum n_P$.
- A group of divisors of degree 0: $\mathbb{D}^0$.
- A principal divisor: $D = \mathrm{div} R = \sum_{P \in C} (\mathrm{ord}_P R) P$ for some rational function $R \in \bar{\mathbb{F}}_q(C)$.
- A group of principal divisors: $\mathbb{P}$.

Introduction: Main definitions and notations

- Let $\mathbb{F}_q$ be a finite field of size $q = p^n$, $p > 2$.
- A hyperelliptic curve C of genus g is a nonsingular curve defined by equation

$$y^2 = f(x),$$

  where f is a monic polynomial of degree $2g + 1$ or $2g + 2$.
- A divisor: $D = \sum_{P \in C} n_P P$.
- A degree of divisor: $\deg D = \sum n_P$.
- A group of divisors of degree 0: $\mathbb{D}^0$.
- A principal divisor: $D = \mathrm{div} R = \sum_{P \in C} (\mathrm{ord}_P R) P$ for some rational function $R \in \bar{\mathbb{F}}_q(C)$.
- A group of principal divisors: $\mathbb{P}$.
- The Jacobian of curve C: $\mathrm{Jac}_{\bar{\mathbb{F}}_q}(C) = \mathbb{D}^0 / \mathbb{P}$.

Introduction: Main definitions and notations

- By Riemann-Roch theorem: each element $[D]$ in $\mathrm{Jac}_{\overline{\mathbb{F}}_q}(C)$ can be uniquely represented by a divisor of the form

$$D = P_1 + \ldots + P_r - r\infty$$

with $r \leq g$ and $P_i \neq \tau(P_j)$ for $i \neq g$ and the hyperelliptic involution τ on C.

Introduction: Main definitions and notations

- By Riemann-Roch theorem: each element $[D]$ in $\mathrm{Jac}_{\overline{\mathbb{F}}_q}(C)$ can be uniquely represented by a divisor of the form

$$D = P_1 + \ldots + P_r - r\infty$$

with $r \leq g$ and $P_i \neq \tau(P_j)$ for $i \neq g$ and the hyperelliptic involution τ on C.

- The Mumford-Cantor's representation: $D = (d(X), e(X))$,
$d(X) = X^r + d_{r-1}X^{r-1} + \ldots + d_0$,
$e(X) = e_{r-1}X^{r-1} + \ldots + e_0$.

Introduction: Main definitions and notations

- By Riemann-Roch theorem: each element $[D]$ in $\mathrm{Jac}_{\overline{\mathbb{F}}_q}(C)$ can be uniquely represented by a divisor of the form

$$D = P_1 + \ldots + P_r - r\infty$$

with $r \leq g$ and $P_i \neq \tau(P_j)$ for $i \neq g$ and the hyperelliptic involution τ on C.

- The Mumford-Cantor's representation: $D = (d(X), e(X))$,
$d(X) = X^r + d_{r-1}X^{r-1} + \ldots + d_0$,
$e(X) = e_{r-1}X^{r-1} + \ldots + e_0$.
Properties: for $P_i = (x_i, y_i) \in C(\mathbb{F}_q)$:
$d(X) = \prod_{i=1}^{r}(X - x_i)$,
$e(x_i) = y_i$,
$\deg e(X) < \deg d(X) \leq g$, $d(X)|(e^2(X) - f(X))$.

Introduction: Main definitions and notations

- By Riemann-Roch theorem: each element $[D]$ in $\mathrm{Jac}_{\bar{\mathbb{F}}_q}(C)$ can be uniquely represented by a divisor of the form

$$D = P_1 + \ldots + P_r - r\infty$$

with $r \leq g$ and $P_i \neq \tau(P_j)$ for $i \neq g$ and the hyperelliptic involution τ on C.

- The Mumford-Cantor's representation: $D = (d(X), e(X))$,
$d(X) = X^r + d_{r-1}X^{r-1} + \ldots + d_0$,
$e(X) = e_{r-1}X^{r-1} + \ldots + e_0$.
Properties: for $P_i = (x_i, y_i) \in C(\mathbb{F}_q)$:
$d(X) = \prod_{i=1}^{r}(X - x_i)$,
$e(x_i) = y_i$,
$\deg e(X) < \deg d(X) \leq g$, $d(X)|(e^2(X) - f(X))$.

- The l-torsion subgroup:
$\mathrm{Jac}_{\bar{\mathbb{F}}_q}(C)[l] = \{[D] \in \mathrm{Jac}_{\bar{\mathbb{F}}_q}(C) | l \cdot [D] = 0\}$.

Introduction: Main definitions and notations

- All generic non-zero divisors $D \in \mathrm{Jac}_k(C)[l]$ have a weight g: $D = P_1 + \ldots + P_g - g\infty$.

Introduction: Main definitions and notations

- All generic non-zero divisors $D \in \mathrm{Jac}_k(C)[l]$ have a weight g: $D = P_1 + \ldots + P_g - g\infty$.
- In this work: $g = 2$ and then for $D = P_1 + P_2 - 2\infty$ we have

$$[l]D = 0 \quad \Leftrightarrow \quad [l](P_1 - \infty) = -[l](P_2 - \infty).$$

Introduction: Main definitions and notations

- All generic non-zero divisors $D \in \mathrm{Jac}_k(C)[l]$ have a weight g: $D = P_1 + \ldots + P_g - g\infty$.
- In this work: $g = 2$ and then for $D = P_1 + P_2 - 2\infty$ we have

$$[l]D = 0 \quad \Leftrightarrow \quad [l](P_1 - \infty) = -[l](P_2 - \infty).$$

- Setting $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, the Mumford-Cantor's coordinates:

$$[l](P_i - \infty) = \left(\delta_l\left(\frac{x_i - X}{4y_i^2}\right), \epsilon_l\left(\frac{x_i - X}{4y_i^2}\right)\right).$$

with $i = 1, 2$.

Introduction: Main definitions and notations

- All generic non-zero divisors $D \in \mathrm{Jac}_k(C)[l]$ have a weight g: $D = P_1 + \ldots + P_g - g\infty$.
- In this work: $g = 2$ and then for $D = P_1 + P_2 - 2\infty$ we have

$$[l]D = 0 \quad \Leftrightarrow \quad [l](P_1 - \infty) = -[l](P_2 - \infty).$$

- Setting $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, the Mumford-Cantor's coordinates:

$$[l](P_i - \infty) = \left(\delta_l\left(\frac{x_i - X}{4y_i^2}\right), \epsilon_l\left(\frac{x_i - X}{4y_i^2}\right)\right).$$

with $i = 1, 2$.

- Remark: $\delta_l\left(\frac{x_i - X}{4y_i^2}\right)$ is not necessarily a monic polynomial.

Cryptographic applications

1. Public-key cryptography with the DLP ($g \leq 3$).
2. Pairing-based cryptography ($g \leq 3$).
3. Isogeny-based cryptography (there is no limitation on genus).

Cryptographic applications

1. Verification of a curve security $\leftrightarrow$ Point counting algorithms.
2. Constructing of a secure curve $\leftrightarrow$ CM-method.
3. Computing of isogenies $\leftrightarrow$ Computing modular polynomials.

Cryptographic applications

1. Verification of a curve security $\leftrightarrow$ Point counting algorithms.
2. Constructing of a secure curve $\leftrightarrow$ CM-method.
3. Computing of isogenies $\leftrightarrow$ Computing modular polynomials.

$$\Downarrow$$

Division polynomials as a base!

Actual research

2011: P. Gaudry, D.R. Kohel, B.A. Smith. Counting points on genus 2 curves with real multiplication.

Actual research

2011: P. Gaudry, D.R. Kohel, B.A. Smith. Counting points on genus 2 curves with real multiplication.

- The authors present an accelerated Schoof-type point-counting algorithm for curves of genus 2 equipped with an efficiently computable RM endomorphism.

Actual research

2011: P. Gaudry, D.R. Kohel, B.A. Smith. Counting points on genus 2 curves with real multiplication.

- The authors present an accelerated Schoof-type point-counting algorithm for curves of genus 2 equipped with an efficiently computable RM endomorphism.
- The RM formulae are also compatible with fast arithmetic based on theta functions.

Actual research

2011: P. Gaudry, D.R. Kohel, B.A. Smith. Counting points on genus 2 curves with real multiplication.

- The authors present an accelerated Schoof-type point-counting algorithm for curves of genus 2 equipped with an efficiently computable RM endomorphism.
- The RM formulae are also compatible with fast arithmetic based on theta functions.
- There exists an algorithm (without algorithm) for the point counting problem in a family of genus 2 curves with efficiently computable RM of class number 1 ($C_T : Y^2 = X^5 - 5X^3 + 5X + t$, $t \in \mathbb{F}_q$, $q \neq 5^\nu$, concerning $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$).

Actual research

2011: P. Gaudry, D.R. Kohel, B.A. Smith. Counting points on genus 2 curves with real multiplication.

- The authors present an accelerated Schoof-type point-counting algorithm for curves of genus 2 equipped with an efficiently computable RM endomorphism.
- The RM formulae are also compatible with fast arithmetic based on theta functions.
- There exists an algorithm (without algorithm) for the point counting problem in a family of genus 2 curves with efficiently computable RM of class number 1 ($C_T : Y^2 = X^5 - 5X^3 + 5X + t$, $t \in \mathbb{F}_q$, $q \neq 5^\nu$, concerning $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$).
- Explicit formulae for division polynomials $\phi_T \in \mathbb{F}_q(\tau_5)[X]$:

$$d_2 = 1, \quad d_1 = -\tau_5 X, \quad d_0 = X^2 + \tau_5^2 - 4, \quad e_1 = 0, \quad e_0 = 1,$$

with $\tau_5 = \zeta_5 + \zeta_5^{-1}$ and ζ_5 is a 5th root of unity in $\bar{\mathbb{F}}_q$.

Actual research

2018: S. Abelard. Counting points on hyperelliptic curves in large characteristic: algorithms and complexity (Doctoral dissertation).

Actual research

2018: S. Abelard. Counting points on hyperelliptic curves in large characteristic: algorithms and complexity (Doctoral dissertation).

- Again RM-type.

Actual research

2018: S. Abelard. Counting points on hyperelliptic curves in large characteristic: algorithms and complexity (Doctoral dissertation).

- Again RM-type.
- Using of l-torsion (division) ideal I_l without explonation how it can be obtained.

Actual research

2018: S. Abelard. Counting points on hyperelliptic curves in large characteristic: algorithms and complexity (Doctoral dissertation).

- Again RM-type.
- Using of l-torsion (division) ideal I_l without explonation how it can be obtained.
- No explicit formulae for division polynomials.

Actual research

2018: S. Abelard. Counting points on hyperelliptic curves in large characteristic: algorithms and complexity (Doctoral dissertation).

- Again RM-type.
- Using of l-torsion (division) ideal I_l without explonation how it can be obtained.
- No explicit formulae for division polynomials.

2019: E.V. Flynn and Yan Bo Ti. Genus Two Isogeny Cryptography.

Actual research

2018: S. Abelard. Counting points on hyperelliptic curves in large characteristic: algorithms and complexity (Doctoral dissertation).

- Again RM-type.
- Using of l-torsion (division) ideal I_l without explonation how it can be obtained.
- No explicit formulae for division polynomials.

2019: E.V. Flynn and Yan Bo Ti. Genus Two Isogeny Cryptography.

- Proposed a first post-quantum isogeny-based scheme on genus 2 curves (case of principally polarised supersingular abelian surface). The authors used Richelot isogenies for computing of degree 2 isogenies and Kummer surfaces for degree 3 case.

Actual research

2018: S. Abelard. Counting points on hyperelliptic curves in large characteristic: algorithms and complexity (Doctoral dissertation).

- Again RM-type.
- Using of l-torsion (division) ideal I_l without explonation how it can be obtained.
- No explicit formulae for division polynomials.

2019: E.V. Flynn and Yan Bo Ti. Genus Two Isogeny Cryptography.

- Proposed a first post-quantum isogeny-based scheme on genus 2 curves (case of principally polarised supersingular abelian surface). The authors used Richelot isogenies for computing of degree 2 isogenies and Kummer surfaces for degree 3 case.
- The hyperelliptic curve $C : Y^2 = X^6 + 1$. In this case $\mathrm{Jac}(C) \sim \mathrm{Jac}(C_1) \times \mathrm{Jac}(C_2)$.

Reason for choice of hyperelliptic curves defined by Dickson polynomials

- Dickson polynomial: $D_n(X,\alpha)=\sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-\alpha)^i X^{n-2i}$.
- Let $C/\mathbb{F}_q : y^2 = x^{2g+1} + ax^{g+1} + bx$ be a hyperelliptic curve.

Theorem (Novoselov, 2019)

If genus g is odd then

$$\mathrm{Jac}_{\mathbb{F}_q[\sqrt[g]{b}]}(C) \sim \mathrm{Jac}_{\mathbb{F}_q[\sqrt[g]{b}]}(C_1) \times J_{\mathbb{F}_q[\sqrt[g]{b}]}(C_2)$$

where

$$C_1 : Y^2 = D_g(X, \sqrt[g]{b}) + a$$

and

$$C_2 : Y^2 = (X^2 - 4\sqrt[g]{b})(D_g(X, \sqrt[g]{b}) + a).$$

If genus g of C is even then

$$\mathrm{Jac}_{\mathbb{F}_q[\sqrt[2g]{b}]}(C) \sim \mathrm{Jac}_{\mathbb{F}_q[\sqrt[2g]{b}]}(C_3) \times \mathrm{Jac}_{\mathbb{F}_q[\sqrt[2g]{b}]}(\tilde{C}_3)$$

where

$$C_3 : Y^2 = (X + 2\sqrt[2g]{b})(D_g(X, \sqrt[g]{b}) + a)$$

and

$$\tilde{C}_3 : Y^2 = (X - 2\sqrt[2g]{b})(D_g(X, \sqrt[g]{b}) + a).$$

Reason for choice of hyperelliptic curves defined by Dickson polynomials

Advantages:

- Computation of the number of points on the $\mathrm{Jac}_{\mathbb{F}_q}(C)$ can be reduced to computation of the number of points on $\mathrm{Jac}\, C_1, \mathrm{Jac}\, C_2, \mathrm{Jac}\, C_3, \mathrm{Jac}\, \tilde{C}_3$.
- $\mathrm{Jac}_{\mathbb{F}_q[\sqrt[g]{b}]}(C_1)$ and $J_{\mathbb{F}_q[\sqrt[g]{b}]}(C_2)$, $\mathrm{Jac}_{\mathbb{F}_q[\sqrt[2g]{b}]}(C_3)$ and $\mathrm{Jac}_{\mathbb{F}_q[\sqrt[2g]{b}]}(\tilde{C}_3)$ are genercally absolutly irreducible $\Rightarrow$ are candidates for cryptography.

Division polynomials

We will obtain the explicit formulae for the division polynomials d_0, d_1, d_2, e_0, e_1 and as a consequence we obtain explicit formulae for the Mumford-Cantor's coordinates via the Padé approximants $A_r(Z), B_r(Z)$ and assocoated with them the values $C_r(Z)$, $D_r(Z)$ for $g = 2$.

[$*$] Cantor D. G. On the analogue of the division polynomials for hyperelliptic curves.//Journal fur die reine und angewandte Mathematik, №447, pp. 91—146, 1994.

Division polynomials

1. Consider the hyperelliptic curve $Y^2 = X^{2g+1} + cX^{g+1} + \alpha^4 X$ of genus $g = 4$ over $\mathbb{F}_q$. By result of Novoselov we have a hyperelliptic curve defined by the equation

$$C : Y^2 = (X \pm 2)(D_4(X, \alpha) + c),$$

where $D_4(X, \alpha) = X^4 - 4X^2\alpha + 2\alpha^2$, $\alpha, c \in \mathbb{F}_q$ and $g(C) = 2$.

Division polynomials

1. Consider the hyperelliptic curve $Y^2 = X^{2g+1} + cX^{g+1} + \alpha^4 X$ of genus $g = 4$ over $\mathbb{F}_q$. By result of Novoselov we have a hyperelliptic curve defined by the equation

$$C : Y^2 = (X \pm 2)(D_4(X, \alpha) + c),$$

where $D_4(X, \alpha) = X^4 - 4X^2\alpha + 2\alpha^2$, $\alpha, c \in \mathbb{F}_q$ and $g(C) = 2$.
2. Let $P = (x, y) \in C(\mathbb{F}_q)$. We make a following change of variables

$$P = (x, y) \mapsto \tilde{P} = (0, -y).$$

Then by setting

$$X = x - Z, \quad \tilde{f}(Z) = f(x - Z),$$

the curve C is replaced by the curve

$$\tilde{C} : \tilde{Y}^2 = (x-Z)^5 \pm 2(x-Z)^4 - 4\alpha(x-Z)^3 \mp 8\alpha(x-Z)^2 + (2\alpha^2+c)(x-Z) \pm (4\alpha^2+2c) = \tilde{f}(Z).$$

Division polynomials

3. Expand $\sqrt{\tilde{f}(Z)}$ in a Taylor series around $Z = 0$:

$$S(Z) := \sqrt{\tilde{f}(Z)} = \sum_{i=1}^{\infty} s_i(x) Z^i.$$

with constant term $s_0 = -y$.

Division polynomials

3. Expand $\sqrt{\tilde{f}(Z)}$ in a Taylor series around $Z = 0$:

$$S(Z) := \sqrt{\tilde{f}(Z)} = \sum_{i=1}^{\infty} s_i(x) Z^i.$$

with constant term $s_0 = -y$.

4. Denote

$$\det(S)_{mn} = \begin{vmatrix} s_{m-n+1} & s_{m-n+2} & \cdots & s_m \\ s_{m-n+2} & s_{m-n+3} & \cdots & s_{m+1} \\ \vdots & \vdots & \cdots & \vdots \\ s_{m-1} & s_m & \cdots & s_{m+n-2} \\ s_m & s_{m+1} & \cdots & s_{m+n-1} \end{vmatrix}$$

Division polynomials

Division polynomials

5. The first four values for the Cantor's division polynomials are

$$\psi_1 = 0,$$

$$\psi_2 = 1,$$

$$\psi_3 = (2y)^2,$$

$$\psi_4 = (2y)^5 s_3.$$

6. Let

$$m_r = \left\lfloor \frac{r+g}{2} \right\rfloor, \quad n_r = \left\lfloor \frac{r-g-1}{2} \right\rfloor.$$

and for $r \geq 5$ we can express ψ_r by terms $\det(S)_{m_r n_r}$ using [$*$]:

$$\psi_r = (2y)^{\frac{r^2-r-2}{2}} \cdot \det(S)_{m_{r+1} n_{r+1}}.$$

Division polynomials

Definition

Let $A_r(Z)$ and $B_r(Z)$ be non-zero polynomials, such that the formal power series $A_r(Z) - B_r(Z)S(Z)$ is divided by $Z^{m_r+n_r+1}$ and $\deg A_r \leq m_r$, $\deg B_r \leq n_r$, then a pair (A_r, B_r) is (m_r, n_r)-Padé approximants of series $S(Z)$, namely $\frac{A_r(Z)}{B_r(Z)} = S(Z)$ up to order $m_r + n_r$.

Therefore the solution of Padé approximation problem can be reduced to the finding of polynomials $A_r(Z)$ and $B_r(Z)$.

Definition

The value

$$C_r(Z) = -\frac{A_r(Z) - B_r(Z)S(Z)}{Z^r},$$

is called an error value showing how far $\frac{A_r(Z)}{B_r(Z)}$ is from approximating $S(Z)$.

Definition

$$D_r(Z) = -(A_r(Z) + B_r(Z)S(Z))C_r(Z).$$

The zeros of the polynomial $D_r(Z)$ correspond Z-coordinates of divisor representation $[r](\tilde{P} - \infty)$.

Division polynomials

7. Initial values for $A(Z), B(Z), C(Z)$ and $D(Z)$:

r	$A_r(Z)$	$B_r(Z)$	$C_r(Z)$	$D_r(Z)$
0	-1	0	1	–
1	$-Z$	0	1	–
2	$-Z^2$	0	1	$-Z^2$
3	$\sum_{i=0}^{2} s_i Z^i$	1	$\sum_{i=3}^{\infty} s_i Z^{i-3}$	$2(s_0 s_5 + s_1 s_4 + s_2 s_3)Z^2 + 2(s_0 s_4 + s_1 s_3)Z + 2 s_0 s_3$
4	$\sum_{i=0}^{3} s_i Z^i$	1	$\sum_{i=4}^{\infty} s_i Z^{i-4}$	$2(s_0 s_6 + s_1 s_5 + s_2 s_4)Z^2 + 2(s_0 s_5 + s_1 s_4)Z + 2 s_0 s_4$

Division polynomials

8. Knowing only ψ_r and the initial values given above, we get recursion formulae for A_r, B_r, C_r, D_r with $r \geq 5$:

$$A_r(Z) = (2y)^{-r+2} \cdot \frac{\psi_{r-1}}{\psi_{r-2}} \cdot A_{r-1}(Z) - (2y)^{-2r+3} \cdot \frac{\psi_r}{\psi_{r-2}} \cdot A_{r-2}(Z) \cdot Z.$$

$$B_r(Z) = (2y)^{-r+2} \cdot \frac{\psi_{r-1}}{\psi_{r-2}} \cdot B_{r-1}(Z) - (2y)^{-2r+3} \cdot \frac{\psi_r}{\psi_{r-2}} \cdot B_{r-2}(Z) \cdot Z.$$

$$C_r(Z) = \left((2y)^{-r+2} \cdot \frac{\psi_{r-1}}{\psi_{r-2}} \cdot C_{r-1}(Z) - (2y)^{-2r+3} \cdot \frac{\psi_r}{\psi_{r-2}} \cdot C_{r-2}(Z) \right) / Z.$$

$$D_r(Z) = 2 \left(\frac{(2y)^{-2r+4} \cdot \frac{\psi_{r-1}^2}{\psi_{r-2}^2} \cdot A_{r-1}(Z) \cdot C_{r-1}(Z)}{Z} - \frac{(2y)^{-3r+5} \cdot \frac{\psi_{r-1}\psi_r}{\psi_{r-2}^2} \cdot A_{r-1}(Z) \cdot C_{r-2}(Z)}{Z} + \right.$$

$$\left. + (2y)^{-4r+6} \cdot \frac{\psi_{r-1}^2}{\psi_{r-2}^2} \cdot A_{r-2}(Z) \cdot C_{r-2}(Z) - (2y)^{-3r+5} \cdot \frac{\psi_{r-1}\psi_r}{\psi_{r-2}^2} \cdot A_{r-2}(Z) \cdot C_{r-1}(Z) \right) \{i_2\} =$$

$$= 2(A_r(Z) \cdot C_r(Z))\{i_2\},$$

where a symbol $\{i_2\}$ denotes omitting all terms in branches of degree more than 2.

Division polynomials

Theorem (Cantor)

If $r \geq 3$ then element $[r](\tilde{P} - \infty)$ in the Jacobian $\mathrm{Jac}_{\bar{k}}(\tilde{C})$ of the curve $\tilde{C}$ can be represented by the pair $(D_r(Z), E_r(Z))$, where

$$E_r(Z) = 2y \cdot \frac{\psi_{r-1}\psi_{r+1}}{\psi_r^2} \cdot Z \cdot \left(\frac{(2y)^{r^2+r-2} D_{r+1}(Z)}{\psi_{r+1}^2} - \frac{(2y)^{r^2-3r} D_{r-1}(Z)}{\psi_{r-1}^2} \right) \pmod{D_r(Z)}.$$

9. Returning to the original curve C and to divisor $[r](P - \infty)$ with $r \geq 3$, the Mumford-Cantor's coordinates are the polynomials of following form:

$$\delta_r(Z) = (2y)^{r^2-r-2} \cdot D_r(4y^2 Z),$$

$$\epsilon_r(Z) = \frac{y \cdot (\psi_{r-1}^2 \cdot \delta_{r+1}(Z) - \psi_{r+1}^2 \cdot \delta_{r-1}(Z)) \cdot Z}{\psi_{r-1} \cdot \psi_r^2 \cdot \psi_{r+1}} \pmod{\delta_r(Z)}.$$

Example: case $l = 3$

Consider a hyperelliptic curve $C/\mathbb{F}_q$ of genus $g = 2$ with the equation

$$Y^2 = (X-2)(D_4(X,\alpha)+c) = X^5-2X^4-4\alpha X^3+8\alpha X^2+(2\alpha^2+c)X-4\alpha^2-2c,$$

where $D_4(X,\alpha) = X^4 - 4\alpha X^2 + 2\alpha^2$ is the Dickson polynomial. Set $\alpha = 1$, then

$$Y^2 = X^5 - 2X^4 - 4X^3 + 8X^2 + (c+2)X + (-2c-4).$$

For the divisor $D = P_1 + P_2 - 2\infty$ with $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, we have

$$[l]D = 0 \Leftrightarrow [l](P_1 - \infty) = -[l](P_2 - \infty).$$

For $l = 3$ we denote the Mumford-Cantor's representation as

$$[3](P_1 - \infty) = \left(\delta_3\left(\frac{x_1 - X}{4y_1^2}\right), \epsilon_3\left(\frac{x_1 - X}{4y_1^2}\right)\right),$$

$$[3](P_2 - \infty) = \left(\delta_3\left(\frac{x_2 - X}{4y_2^2}\right), \epsilon_3\left(\frac{x_2 - X}{4y_2^2}\right)\right)$$

or

$$[3](P_1-\infty) = \left(d_2(x_1,y_1)X^2 + d_1(x_1,y_1)X + d_0(x_1,y_1), e_1(x_1,y_1)X + e_0(x_1,y_1)\right),$$

$$[3](P_2-\infty) = \left(d_2(x_2,y_2)X^2 + d_1(x_2,y_2)X + d_0(x_2,y_2), e_1(x_2,y_2)X + e_0(x_2,y_2)\right),$$

where d_2, d_1, d_0, e_1, e_0 are rational functions of variables x_i, y_i, $i = 1, 2$.

Example: case $l = 3$

$$
\begin{aligned}
d_2 = -\frac{1}{4y^4}\Big(&64x^{20} - 512x^{19} + 512x^{18} + 6144x^{17} + (256c - 16896)x^{16} + (-2048c - 20480)x^{15} + \\
&+ (120832 + 3072c)x^{14} + (-32768 + 16384c)x^{13} + (-391680 - 55808c + 384c^2)x^{12} + \\
&+ (-3072c^2 - 12288c + 380928)x^{11} + (6144c^2 + 253952c + 614400)x^{10} + \\
&+ (12288c^2 - 212992c - 999424)x^9 + (-439296c + 256c^3 - 59904c^2 - 374784)x^8 + \\
&+ (1228800 + 36864c^2 + 696320c - 2048c^3)x^7 + (129024c^2 + 5120c^3 + 192512c - 90112)x^6 + \\
&+ (-786432 - 786432c - 196608c^2)x^5 + (-19968c^3 - 23040c^2 + 230400 + 64c^4 + 149504c)x^4 + \\
&+ (253952 - 512c^4 + 28672c^3 + 184320c^2 + 376832c)x^3 + \\
&+ (-4096c^3 - 106496 - 147456c + 1536c^4 - 61440c^2)x^2 + \\
&+ (-65536c - 49152c^2 - 2048c^4 - 16384c^3 - 32768)x + \\
&+ 16384 + 8192c^3 + 1024c^4 + 24576c^2 + 32768c\Big),
\end{aligned}
$$

Example: case $l = 3$

$$
\begin{aligned}
d_1 = -\frac{1}{4y^4}\Big(& -128x^{21} + 1024x^{20} - 1024x^{19} - 12288x^{18} + (33792 - 512c)x^{17} + \\
& + (4096c + 95y^2 + 40960)x^{16} + (-608y^2 - 241664 - 6144c)x^{15} + \\
& + (144y^2 + 65536 - 32768c)x^{14} + (783360 - 768c^2 + 111616c + 6464y^2)x^{13} + \\
& + (24576c - 761856 + 6144c^2 + 60cy^2 - 9960y^2)x^{12} + \\
& + (-1228800 - 12288c^2 - 26688y^2 - 507904c + 96cy^2)x^{11} + \\
& + (70240y^2 - 3408cy^2 + 425984c - 24576c^2 + 1998848)x^{10} + \\
& + (25216y^2 + 119808c^2 + 878592c + 11072cy^2 - 512c^3 + 749568)x^9 + \\
& + (90c^2y^2 + 552cy^2 + 4096c^3 - 2457600 - 192024y^2 - 73728c^2 - 1392640c)x^8 + \\
& + (-59520cy^2 - 10240c^3 + 180224 - 258048c^2 - 385024c + 104320y^2 + 480c^2y^2)x^7 + \\
& + (142528y^2 + 393216c^2 + 98240cy^2 + 1572864c + 1572864 - 6992c^2y^2)x^6 + \\
& + (-128c^4 + 23232c^2y^2 - 460800 + 39936c^3 - 134400y^2 - 20736cy^2 - 299008c + 46080c^2)x^5 + \\
& + (-368640c^2 + 380c^3y^2 + 1024c^4 - 507904 - 69552cy^2 - 753664c - \\
& - 15776y^2 - 57344c^3 - 30072c^2y^2)x^4 + \\
& + (39296cy^2 - 3072c^4 + 122880c^2 - 2272c^3y^2 + 8192c^3 + 294912c + \\
& + 32000y^2 + 212992 + 7104c^2y^2)x^3 + \\
& + (65536 + 4096c^4 + 32768c^3 + 131072c + 4752c^3y^2 + 7872cy^2 + 16224c^2y^2 + 98304c^2 - 11136y^2)x^2 + \\
& + (-65536c - 11136c^2y^2 + 2304cy^2 - 16384c^3 - 2048c^4 - 32768 - 49152c^2 - 3904c^3y^2 + 17920y^2)x + \\
& + 888c^3y^2 - c^4y^2 - 9232y^2 - 5664cy^2 + 1256c^2y^2\Big)
\end{aligned}
$$

Example: case $l = 3$

$$
\begin{aligned}
d_0 = -\frac{1}{4y^4}\Big(&64x^{22} - 512x^{21} + 512x^{20} + 6144x^{19} + (-16896 + 256c)x^{18} + (-95y^2 - 20480 - 2048c)x^{17} + \\
&+ (120832 + 608y^2 + 3072c)x^{16} + (-32768 - 144y^2 + 16384c)x^{15} + \\
&+ (-391680 - 55808c - 6464y^2 + 384c^2)x^{14} + \\
&+ (-60cy^2 + 9960y^2 - 12288c - 3072c^2 + 380928)x^{13} + \\
&+ (6144c^2 + 40y^4 + 253952c + 26688y^2 - 96cy^2 + 614400)x^{12} + \\
&+ (-192y^4 - 999424 - 70240y^2 + 12288c^2 + 3408cy^2 - 212992c)x^{11} + \\
&+ (-11072cy^2 - 374784 + 256c^3 - 439296c - 160y^4 - 25216y^2 - 59904c^2)x^{10} + \\
&+ (-90c^2y^2 + 1920y^4 + 696320c - 2048c^3 - 552cy^2 + 36864c^2 + 192024y^2 + 1228800)x^9 + \\
&+ (5120c^3 + 192512c - 480c^2y^2 + 59520cy^2 - 40cy^4 - 90112 + 129024c^2 - 720y^4 - 104320y^2)x^8 + \\
&+ (-786432 - 98240cy^2 - 8960y^4 - 196608c^2 - 142528y^2 + 640cy^4 - 786432c + 6992c^2y^2)x^7 + \\
&+ (-19968c^3 + 149504c + 20736cy^2 - 23232c^2y^2 + 230400 - 23040c^2 + \\
&+ 64c^4 + 12672y^4 - 3136cy^4 + 134400y^2)x^6 + \\
&+ (376832c + 253952 + 184320c^2 - 380c^3y^2 + 15776y^2 + 2560y^4 + 69552cy^2 + \\
&+ 28672c^3 + 6400cy^4 - 512c^4 + 30072c^2y^2)x^5 + \\
&+ (2272c^3y^2 - 106496 - 147456c - 61440c^2 - 32000y^2 - 9760y^4 + 440c^2y^4 - \\
&- 39296cy^2 - 7104c^2y^2 - 4000cy^4 + 1536c^4 - 4096c^3)x^4 + \\
&+ (-2240c^2y^4 - 16384c^3 - 4752c^3y^2 - 49152c^2 - 32768 + 11136y^2 - 16224c^2y^2 -
\end{aligned}
$$

Example: case $l = 3$

$$
\begin{aligned}
&- 3840cy^4 + 1280y^4 - 2048c^4 - 65536c - 7872cy^2)x^3 + \\
&+ (1024c^4 + 11136c^2y^2 - 2304cy^2 + 32768c + 16384 + 24576c^2 + 3680c^2y^4 + \\
&+ 8192c^3 - 17920y^2 + 4480cy^4 - 5760y^4 + 3904c^3y^2)x^2 + \\
&+ (-1664c^2y^4 + 1536cy^4 + c^4y^2 + 5664cy^2 + 9232y^2 + 9728y^4 - 888c^3y^2 - 1256c^2y^2)x - \\
&- 1952cy^4 + 8c^3y^4 - 464c^2y^4 - 1984y^4\Big),
\end{aligned}
$$

Example: case $l = 3$

$$
\begin{aligned}
e_1 = \frac{1}{(2y)^9}(&145x^{24} - 1392x^{23} + 2472x^{22} + 16288x^{21} + (-1626c - 59460)x^{20} + (20880c - 89952)x^{19} + \\
&+ (689296 - 96568c)x^{18} + (116064c - 459072)x^{17} + (-5649c^2 + 597564c - 3226692)x^{16} + \\
&+ (81568c^2 - 2566528c + 7090816)x^{15} + (-456816c^2 + 3031872c + 659520)x^{14} + \\
&+ (1116480c^2 + 3700992c - 20189952)x^{13} + (1684c^3 - 194792c^2 - 15568016c + 25595680)x^{12} + \\
&+ (13344c^3 - 5577792c^2 + 18238848c + 2370816)x^{11} + \\
&+ (-274800c^3 + 13458528c^2 - 5592384c - 38119296)x^{10} + \\
&+ (1462208c^3 - 11625856c^2 - 8844032c + 34221568)x^9 + \\
&+ 9(c+2)(999c^3 - 413782c^2 + 505556c + 757304)x^8 + \\
&+ (-48(c+2)(1889c^3 - 98362c^2 - 70260c + 481032))x^7 + \\
&+ 8(c+2)(45865c^3 - 229418c^2 - 450196c + 1301704)x^6 + \\
&+ (-96(c+2)^2(7693c^2 + 8724c - 52236))x^5 + \\
&+ (-6(c+2)^2(111c^3 - 115790c^2 - 250476c + 978904))x^4 + \\
&+ 16(c+2)^2(277c^3 - 4298c^2 - 33828c + 50056)x^3 + \\
&+ (-24(c+2)^3(457c^2 + 16676c - 38108))x^2 + \\
&+ 96(c+2)^3(125c^2 + 3188c - 6412)x + \\
&+ (c+2)^3(c^3 - 4922c^2 - 72948c + 135944))
\end{aligned}
$$

Example: case $l = 3$

$$
\begin{aligned}
e_0 = \frac{1}{(2y^9)}(&-145x^2 51392x^{24} - 2472x^{23} - 16288x^{22} + (1626c + 59460)x^{21} + \\
&+ (88y^2 - 20880c + 89952)x^{20} + (-704y^2 + 96568c - 689296)x^{19} + \\
&+ (480y^2 - 116064 * c + 459072)x^{18} + \\
&+ (9600y^2 + 5649c^2 - 597564c + 3226692)x^{17} + \\
&+ (-1448cy^2 - 17488y^2 - 81568c^2 + 2566528c - 7090816)x^{16} + \\
&+ (17664cy^2 - 87552y^2 + 456816c^2 - 3031872c - 659520)x^{15} + \\
&+ (-80512cy^2 + 333568y^2 - 1116480c^2 - 3700992c + 20189952)x^{14} + \\
&+ (133632cy^2 - 138240y^2 - 1684c^3 + 194792c^2 + 15568016c - 25595680)x^{13} + \\
&+ 16(143c^2y^2 + 10828cy^2 - 69156y^2 - 834c^3 + 348612c^2 - 1139928c - 148176)x^{12} + \\
&+ (-6272c^2y^2 - 1120768cy^2 + 2223616y^2 + 274800c^3 - 13458528c^2 + 5592384c + 38119296)x^{11} + \\
&+ (-64(1243c^2y^2 - 28852cy^2 + 21932y^2 + 22847c^3 - 181654c^2 - 138188c + 534712))x^{10} + \\
&+ (535808c^2y^2 - 961536cy^2 - 822272y^2 - 8991c^4 + 3706056c^3 + \\
&+ 2898072c^2 - 15915744c - 13631472)x^9 + \\
&+ 16(707c^3y^2 - 83358c^2y^2 - 41500cy^2 + 206936y^2 + 5667c^4 - 283752c^3 - 800952c^2 + \\
&+ 1021536c + 2886192)x^8 + \\
&+ (-8(c+2)(12640c^2y^2 - 196736cy^2 + 289152y^2 + 45865c^3 - 229418c^2 - 450196c + 1301704))x^7 + \\
&+ 32(c+2)(11084c^2y^2 - 17520cy^2 + 16880y^2 + 23079c^3 + 72330c^2 - 104364c - 313416)x^6 +
\end{aligned}
$$

Example: case $l = 3$

$$+(-6(c+2)(97536c^2y^2+56320cy^2-408576y^2-111c^4+115568c^3+$$
$$+482056c^2-477952c-1957808))x^5+$$
$$+(-8(c+2)(89c^3y^2-44618c^2y^2-17748cy^2+274760y^2+$$
$$+554c^4-7488c^3-84848c^2-35200c+200224))x^4+$$
$$+8(c+2)^2(680c^2y^2+23456cy^2-37728y^2+1371c^3+52770c^2-14268c-228648)x^3+$$
$$+(-32(c+2)^2(481c^2y^2+11012cy^2-24956y^2+375c^3+10314c^2-108c-38472))x^2+$$
$$+(c+2)^2(18816c^2y^2+124416cy^2-350720y^2-c^4+4920c^3+82792c^2+9952c-271888)x+$$
$$+(-8(c+2)^3(c^2+1028c-2044))y^2).$$

Plans for future

For hyperelliptic curves of genus 2 defining by Dickson polynomials we will plan:

- to find the 3-torsion (division) ideal I_3.
- to find the modular equation $\Xi_3(T)$.
- to optimize Pila's algorithm.
- to obtain something for $l = 5$.

Thank you for attention!

EMalygina@kantiana.ru
SNovoselov@kantiana.ru