Soutenance de Thèse de Doctorat

Complexité scalaire des algorithmes de type Chudnovsky de multiplication dans les corps finis

présenté par

Thanh-Hung Dang

25 mai 2020

Membres du Jury

Rapporteur.euse: Laurent-Stéphane DIDIER
Sihem MESNAGER

Examinateurs.trice: Daniel AUGOT
Nadia EL-MRABET
Serge VLADUTS

Directeur de thèse: Alexis BONNECAZE
Co-directeur de thèse: Stéphane BALLET

Table of Contents

Multiplication in $\mathbb{F}_{q^n}/\mathbb{F}_q$

Let $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/\langle P(x)\rangle$ and β is a root of $P(x)$. Let

$$A = \sum_{i=0}^{n-1} a_i\beta^i \text{ and } B = \sum_{i=0}^{n-1} b_i\beta^i$$

1. Product of two polynomials
2. Reduction modulo $P(\beta)$

Elementary operations over $\mathbb{F}_q$

1. Addition
2. Scalar multiplication ($a_i \mapsto \alpha \cdot a_i$ where $\alpha, a_i \in \mathbb{F}_q$, and α is a constant not equal to $\mathbf{0}$ and $\mathbf{1}$)
   $\rightsquigarrow$ Scalar Complexity $\mu_q^s(n)$
3. Bilinear multiplication $\big((a_i, b_j) \mapsto a_i \cdot b_j$ where $a_i, b_j \in \mathbb{F}_q$ depend on the elements A and B of $\mathbb{F}_{q^n}$ which are multiplied$\big)$
   $\rightsquigarrow$ Bilinear Complexity $\mu_q^b(n)$

Chudnovsky^2 multiplication algorithm (CCMA)

Algorithm of Chudnovsky^2

Multiplication in $\mathbb{F}_{q^n}$:

David and Gregory Chudnovsky, 1988
$\rightsquigarrow$ Interpolation on algebraic curves of genus g

Advantages:

- Bilinear complexity in $O(n)$;
- Use of matrices favoring parallelism

Problem

Scalar Complexity of Chudnovsky^2 algorithm?

Description

Theorem

Let

- $F/\mathbb{F}_q$ be an algebraic function field defined over $\mathbb{F}_q$,
- Q be a place of degree n,
- $\mathcal{P} = \{P_1, \ldots, P_N\}$ be a set of places of degree one of $F/\mathbb{F}_q$,
- D be a divisor such that $\mathbf{supp}\, D \cap \{Q, P_1, \ldots, P_N\} = \varnothing$.

If

(i) the first evaluation map $\quad \mathrm{Ev}_Q : \begin{array}{ccc} \mathscr{L}(\mathcal{D}) & \longrightarrow & F_Q \cong \mathbb{F}_{q^n} \\ f & \longmapsto & f(Q) \end{array}$ is surjective,

(ii) the second evaluation map $\quad \mathrm{Ev}_{\mathcal{P}} : \begin{array}{ccc} \mathscr{L}(2D) & \longrightarrow & \mathbb{F}_q^N \\ f & \longmapsto & \big(f(P_1), \ldots, f(P_N)\big) \end{array}$

is injective.

then there exists an algorithm of multiplication $\mathcal{U}$ such that

(1) For any two elements x, y in $\mathbb{F}_{q^n}$, we have:

$$xy = E_Q \circ (Ev_{\mathcal{P}}^{-1})_{|_{ImEv_{\mathcal{P}}}} \left(E_{\mathcal{P}} \circ Ev_Q^{-1}(x) \odot E_{\mathcal{P}} \circ Ev_Q^{-1}(y) \right) \qquad (1)$$

where

- $E_Q : \mathcal{O}_Q \to \mathcal{O}_Q / \langle Q \rangle = F_Q$,
- $E_{\mathcal{P}}$: the extension of $Ev_{\mathcal{P}}$ on the valuation ring $\mathcal{O}_Q$,
- $\odot$: the Hadamard product (element-wise multiplication) .

(2) Then we have:

$$\mu_q^b(\mathcal{U}) \leqslant N.$$

with equality if $N = dim\mathcal{L}(2D)$

$$\boxed{\mu_q^s(\mathcal{U}) \leqslant ??}$$

Sufficient conditions to apply the algorithm

S. Ballet (1999) introduced simple numerical conditions on algebraic curves giving a sufficient condition for the application of CCMA.
Let N_k be the number of places of degree k in an algebraic function field $F/\mathbb{F}_q$.

Theorem 2

If there exists an algebraic function field $F/\mathbb{F}_q$ of genus g satisfying the conditions

1. $N_n > 0$ (which is always the case if $2g + 1 \leqslant q^{\frac{n-1}{2}}(q^{\frac{1}{2}} - 1)$),
2. $N_1 \geqslant 2n + 2g - 1$,

then there exists a divisor D of degree $n+g-1$ and a place Q of degree n such that:

(i) The evaluation map Ev_Q is an isomorphism of vector spaces over $\mathbb{F}_q$.

(ii) There exist places $P_1,\ldots,P_N$ such that the evaluation map $Ev_{\mathcal{P}}$ is an isomorphism of vector spaces over $\mathbb{F}_q$ with $N = 2n + g - 1$.

Computational route for CCMA-based multiplication

$$
\begin{tikzcd}[column sep=huge]
\mathcal{O}_Q \arrow[r, two heads, "E_Q"] & F_Q \\
\cup & \wr\| \\
\mathscr{L}(\mathcal{D}) \arrow[r, "Ev_Q", "\cong"'] & \mathbb{F}_{q^n} \\
 & \rotatebox{90}{$\in$} \\
Ev_Q^{-1}(x) = f & x \arrow[l, dashed] \\
Ev_Q^{-1}(y) = g & y \arrow[l, dashed] \\
\mathscr{L}(2\mathcal{D}) \arrow[r, "Ev_{\mathcal{P}}", "\cong"'] & \mathbb{F}_q^N \\
f \arrow[r, mapsto] & \bar{f} := \big(f(P_1), \ldots, f(P_N)\big) \\
g \arrow[r, mapsto] & \bar{g} := \big(g(P_1), \ldots, g(P_N)\big) \arrow[d, mapsto, "\odot"'] \\
Ev_{\mathcal{P}}^{-1}(\bar{h}) =: fg \arrow[d, mapsto, "E_Q"'] & \bar{h} := \big(f(P_1)g(P_1), \ldots, f(P_N)g(P_N)\big) \arrow[d, squiggly] \\
(fg)(Q) = f(Q)g(Q) = xy & \begin{array}{l} \mu_q^b(\mathcal{U}) = N \\ \mu_q^s(\mathcal{U}) = ?? \end{array}
\end{tikzcd}
$$

Fixed a place Q of degree n, an effective divisor D of degree $n+g-1$ for given a function field $F/\mathbb{F}_q$.

Problem

Seek the best possible representation of spaces

$$\mathcal{L}(D), F_Q, \mathcal{L}(2D) \text{ and } \mathbb{F}_q^N$$

i.e. the best possible bases, respectively

$$\mathcal{B}_D, \mathcal{B}_Q, \mathcal{B}_{2D} \text{ and } \mathcal{B}_{\mathbb{F}_q^N}$$

such that the scalar complexity $\mu_q^s(\mathcal{U})$ is the best possible.

Let us denote $\mathcal{B}_Q$ a basis of $F_Q = \mathcal{O}_Q/\langle Q\rangle \cong \mathbb{F}_{q^n}$.

Basis $\mathcal{B}_D$ of Riemann-Roch space $\mathcal{L}(D)$. Then

$$\mathcal{B}_D = Ev_Q^{-1}(\mathcal{B}_Q),$$

or

$$\mathcal{B}_Q = Ev_Q(\mathcal{B}_D).$$

Basis $\mathcal{B}_{2D}$ of $\mathcal{L}(2D) = \mathcal{L}(D) \oplus M$:

$$\mathcal{B}_{2D} = \mathcal{B}_D \cup \mathcal{B}_D^c$$

$\mathcal{B}_D^c$ denotes the basis of complementary subspace M of $\mathcal{L}(D)$ in $\mathcal{L}(2D)$.

$\mathcal{B}^c_{\mathbb{F}_q^N}$ is the canonical basis of vector space $\mathbb{F}_q^N$.

Matrices

The basis of Riemann-Roch space $\mathcal{L}(2D)$ is $\mathcal{B}_{2D} = \{f_1, ..., f_N\}$ for $N = 2n + g - 1$.

- T_{2D} is the matrix of $Ev_{\mathcal{P}} : \mathcal{L}(2D) \to \mathbb{F}_q^N$:

$$T_{2D} := \begin{pmatrix} f_1(P_1) & f_2(P_1) & \cdots & f_N(P_1) \\ f_1(P_2) & f_2(P_2) & \cdots & f_N(P_2) \\ \vdots & \vdots & \vdots & \vdots \\ f_1(P_N) & f_2(P_N) & \cdots & f_N(P_N) \end{pmatrix}$$

- T_D is the matrix of $Ev_{\mathcal{P}}|_{\mathcal{L}(D)}$. (i.e. T_D is the matrix of the first n columns of T_{2D})
- C is the matrix of $E_Q|_{\mathcal{L}(2D)}$:

$$C := \begin{pmatrix} c_1^1 & \cdots & c_N^1 \\ c_1^2 & \cdots & c_N^2 \\ \vdots & \vdots & \vdots \\ c_1^n & \cdots & c_N^n \end{pmatrix}$$

Algorithm

Algorithm 1 Chudnovsky^2 Multiplication in $\mathbb{F}_{q^n}$ (CCMA)

INPUT: $x = \sum_{i=1}^{n} x_i Ev_Q(f_i)$ and $y = \sum_{i=1}^{n} y_i Ev_Q(f_i) \quad // x_i, y_i \in \mathbb{F}_q$

OUTPUT: $z = xy = \sum_{i=1}^{n} z_i Ev_Q(f_i)$

1. $X := \begin{pmatrix} X_1 \\ \vdots \\ X_N \end{pmatrix} \leftarrow T_D \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ and $Y := \begin{pmatrix} Y_1 \\ \vdots \\ Y_N \end{pmatrix} \leftarrow T_D \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$.
2. $(Z_1, ..., Z_N)^t \leftarrow (X_1Y_1, \ldots, X_NY_N)^t =: X \odot Y$
3. $(z_1, \ldots, z_n)^t \leftarrow C^t T_{2D}^{-1} \cdot \begin{pmatrix} Z_1 \\ \vdots \\ Z_N \end{pmatrix}$

Optimization of scalar complexity for CCMA

Framework

We call $\mathcal{U}^{F,n}_{D,Q,\mathcal{P}} := (\mathcal{U}^{A}_{D,Q,\mathcal{P}}, \mathcal{U}^{R}_{D,Q,\mathcal{P}})$ the Chudnovsky[2] multiplication algorithm of type

$$xy = E_Q \circ Ev_{\mathcal{P}}^{-1}\left(Ev_{\mathcal{P}} \circ Ev_Q^{-1}(x) \odot Ev_{\mathcal{P}} \circ Ev_Q^{-1}(y)\right)$$

- $\mathcal{U}^{A}_{D,Q,\mathcal{P}} := Ev_{\mathcal{P}} \circ Ev_Q^{-1} \qquad \rightsquigarrow \text{"}Aller - Phase\text{"}$
- $\mathcal{U}^{R}_{D,Q,\mathcal{P}} := E_Q \circ Ev_{\mathcal{P}}^{-1} \qquad \rightsquigarrow \text{"}Retour - Phase\text{"}$

satisfying the assumption of Theorem 2.

We will say that two algorithms $\mathcal{U}^{F,n}_{D,Q,\mathcal{P}} = \mathcal{U}^{F,n}_{D',Q',\mathcal{P}'}$ if

$$\mathcal{U}^{A}_{D,Q,\mathcal{P}} = \mathcal{U}^{A}_{D',Q',\mathcal{P}'} \quad \text{and} \quad \mathcal{U}^{R}_{D,Q,\mathcal{P}} = \mathcal{U}^{R}_{D',Q',\mathcal{P}'}.$$

Remark: If we choose the construction of $\mathcal{U}^{F,n}_{D,Q,\mathcal{P}}$ as above, then

$$\mu^b_q(\mathcal{U}^{F,n}_{D,Q,\mathcal{P}}) = N = 2n + g - 1 \ \ (optimal).$$

First case study, the scalar multiplication is computed with respect to the number of zeros of matrices.

Number of scalar multiplications of $\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}$:

$$N_s = 3n(2n + g - 1) - N_z, \tag{2}$$

where N_z is the number of zeros in CCMA, is computed by:

$$N_z = 2N_{zero}(T_D) + N_{zero}(C^t T_{2D}^{-1}). \tag{3}$$

Aim

To improve the scalar complexity $\mu_q^s(\mathcal{U}_{D,Q,\mathcal{P}}^{F,n})$, we seek to maximize N_z.

Given an algebraic function field $F/\mathbb{F}_q$, we fix an effective divisor D, a place Q and $\mathcal{P} = \{P_1, \ldots, P_N\}$. Fixing the bases: $\mathcal{B}_Q$ of $F_Q \cong \mathbb{F}_{q^n}$ and $\mathcal{B}^c_{\mathbb{F}_q^N}$ of $\mathbb{F}_q^N$.

Aller-Phase: $\mathcal{U}^A_{D,Q,\mathcal{P}} = Ev_{\mathcal{P}} \circ Ev_Q^{-1} = Ev_{\mathcal{P}}|_{\mathcal{L}(D)} \circ Ev_Q^{-1}$

$$\begin{tikzcd}
\mathcal{L}(D) \diagup \{\mathcal{B}_D\} \arrow[d, phantom, "\cap"] \arrow[drr, dashed, "Ev_{\mathcal{P}}|_{\mathcal{L}(D)}"] & & F_Q \diagup \{\mathcal{B}_Q\} \arrow[ll, dashed, "Ev_Q^{-1}"', "\cong"] \arrow[d, dashed, red] \\
\mathcal{L}(2D) \diagup \{\mathcal{B}_{2D}\} \arrow[rr, "\cong", "Ev_{\mathcal{P}}"'] & & \mathbb{F}_q^N \diagup \{\mathcal{B}^c_{\mathbb{F}_q^N}\}
\end{tikzcd}$$

$\Rightarrow$ Matrix T_D of $\mathcal{U}^A_{D,Q,\mathcal{P}}$ is invariant under the action of $\sigma \in GL_{\mathbb{F}_q}(n)$ on the basis $\mathcal{B}_D$.

Analysis on CCMA

Retour-Phase: $\mathcal{U}^R_{D,Q,\mathcal{P}} = E_Q \circ Ev_{\mathcal{P}}^{-1} = E_Q|_{\mathcal{L}(2D)} \circ Ev_{\mathcal{P}}^{-1}$

$$\begin{tikzcd}
\mathcal{O}_Q \arrow[r, two heads, "E_Q"] & F_Q \big/ \{\mathcal{B}_Q\} \\
\mathcal{L}(2D) \big/ \{\mathcal{B}_{2D}\} \arrow[ur, dashed, "E_Q|_{\mathcal{L}(2D)}"] & \mathbb{F}_q^N \big/ \{\mathcal{B}^c_{\mathbb{F}_q^N}\} \arrow[l, dashed, "\cong"', "Ev_{\mathcal{P}}^{-1}"] \arrow[u, dashed]
\end{tikzcd}$$

$\Rightarrow$ Matrix $C^t T_{2D}^{-1}$ of $\mathcal{U}^R_{D,Q,\mathcal{P}}$ is <u>invariant</u> under the action of $\sigma \in GL_{\mathbb{F}_q}(2n+g-1)$ on the basis $\mathcal{B}_{2D}$.

Fixed appropriate triplet $(D, Q, \mathcal{P})$ for a given algebraic function field $F/\mathbb{F}_q$ of genus g.

Proposition 1 [Ballet, Bonnecaze and D. (2019)]

Let us consider a algorithm $\mathcal{U}^{F,n}_{D,Q,\mathcal{P}}$ such that D is an effective divisor, $D - Q$ is non-special divisor of degree $g - 1$, $|\mathcal{P}| = \dim(\mathcal{L}(2D)) = 2n + g - 1$.
Then, we can choose the basis $\mathcal{B}_{2D} = \mathcal{B}_D \cup \mathcal{B}^c_D$, and for any $\sigma \in GL_{\mathbb{F}_q}(2n + g - 1)$, we have

$$\mathcal{U}^{F,n}_{\sigma(D),Q,\mathcal{P}} = \mathcal{U}^{F,n}_{D,Q,\mathcal{P}}$$

where $\sigma(D)$ denotes the action of σ on the basis $\mathcal{B}_D$ in $\mathcal{U}^{F,n}_{D,Q,\mathcal{P}}$, with a fixed $\mathcal{B}_Q$ and $\mathcal{B}^c_{\mathbb{F}_q^{2n+g-1}}$. In particular, $N_{zero}(C^t T^{-1}_{2D})$ is constant under this action.

Idea of the scalar complexity optimization:

1. Starting from the initial basis $\mathcal{B}_{D,0} = Ev_Q^{-1}(\mathcal{B}_Q)$, by the action of $\sigma \in GL_{\mathbb{F}_q}(n)$ we vary this basis to $\mathcal{B}_{D,i}$ for $i = 1, \dots, |GL_{\mathbb{F}_q}(n)|$.
2. For each new basis $\mathcal{B}_{D,i}$ of $\mathcal{L}(D)$, we have $\mathcal{B}_{Q,i} = Ev_Q(\mathcal{B}_{D,i})$. Fixing bases $\mathcal{B}_{Q,i}$ and $\mathcal{B}^c_{\mathbb{F}_q^{2n+g-1}}$, the matrix $C^t T_{2D}^{-1}$ of Retour-Phase is always invariant under any action of $\sigma \in GL_{\mathbb{F}_q}(2n+g-1)$
3. The variation of $\mathcal{B}_{D,i}$ reaches $\mathcal{B}_{D,max}$ such that that the parameter $N_{zero}(T_D)$ is maximal.

Fact: With respect to the basis $\mathcal{B}_{2D,i} = \mathcal{B}_{D,i} \cup \mathcal{B}^c_{D,i}$

- both C and T_{2D} vary,
- $C^t T_{2D}^{-1}$ is invariant.

Proposition 2 [Ballet, Bonnecaze and D. (2019)]

The optimal scalar complexity $\mu^{s,o}(\mathcal{U}^{F,n}_{D,Q,\mathcal{P}})$ of $\mathcal{U}^{F,n}_{D,Q,\mathcal{P}}$ is reached for the set $\{\mathcal{B}_{D,max}, \mathcal{B}_Q\}$ such that $\mathcal{B}_{D,max}$ is the basis of $\mathcal{L}(D)$ satisfying

$$N_{zero}(T_{D,max}) = \max_{\sigma \in GL_{\mathbb{F}_q}(n)} N_{zero}(T_{\sigma(D)})$$

where: $\sigma(D)$ denotes the action of σ on $\mathcal{B}_D$ in $\mathcal{U}^{F,n}_{D,Q,\mathcal{P}}$; $T_{D,max}$ is the matrix of $Ev_{\mathcal{P}}|_{\mathcal{L}(D)}$ equipped with the bases $\mathcal{B}_{D,max}$ and $\mathcal{B}_Q = Ev_Q(\mathcal{B}_{D,max})$. In particular,

$$\mu^{s,o}(\mathcal{U}^{F,n}_{D,Q,\mathcal{P}}) = \min_{\sigma \in GL_{\mathbb{F}_q}(n)} \{\mu^s_q(\mathcal{U}^{F,n}_{\sigma(D),Q,\mathcal{P}}) \mid \sigma(\mathcal{B}_D) \text{ is the basis of } \mathcal{L}(D) \text{ and } \mathcal{B}_Q = Ev_Q(\mathcal{B}_D)\}$$

$$= 3n(2n+g-1) - (2N_{zero}(T_{D,max}) + N_{zero}(T^{-1}_{2D,n})),$$

where C and T_{2D} are defined with respect to $\mathcal{B}_Q = Ev_Q(\mathcal{B}_{D,max})$, and $\mathcal{B}_{2D} = \mathcal{B}_{D,max} \cup \mathcal{B}^c_D$ with $\mathcal{B}^c_D$ a basis of the kernel of $E_Q|_{\mathcal{L}(2D)}$.

Algorithm 2 Setup algorithm for the scalar complexity optimization

INPUT: $F/\mathbb{F}_q$, Q, D, $\mathcal{P} = \{P_1, \ldots, P_{2n+g-1}\}$.

OUTPUT: $\mathcal{B}_{2D} = \mathcal{B}_D \cup \mathcal{B}_D^c$, T_{2D} and $T_{2D,n}^{-1}$.

(i) Check the function field $F/\mathbb{F}_q$, the place Q, the divisor D are such that Conditions (i) and (ii) in Theorem 2 are satisfied.

(ii) Go through the set of bases $\mathcal{B}_D$ of $\mathcal{L}(D)$.

(iii) Choose a basis $\mathcal{B}_D := (f_1, \ldots, f_n)$ such that $N_{zero}(T_D)$ is the largest.

(iv) Construct a basis $\mathcal{B}_D^c := (f_{n+1}, \ldots, f_{2n+g-1})$ of the complementary space $\mathcal{M} := KerE_Q|_{\mathcal{L}(2D)}$ of $\mathcal{L}(D)$ in $\mathcal{L}(2D)$.

(v) Compute T_{2D}, $T_{2D,n}^{-1}$ in the basis $\mathcal{B}_{2D} = \mathcal{B}_D \cup \mathcal{B}_D^c$.

(vi) Set $\mathcal{B}_Q := Ev_Q(\mathcal{B}_D)$.

Recall the definition of algebraic geometry code (AG code) given by V.D. Goppa. Let

- $F/\mathbb{F}_q$ be an algebraic function field of genus g,
- $P_1, \ldots, P_N$ are pairwise distinct places of $F/\mathbb{F}_q$ of degree one,
- $G = P_1 + \cdots + P_N$,
- D are divisors of $F/\mathbb{F}_q$ such that $suppG \cap suppD = \varnothing$.

The AG code $C_{\mathcal{L}}(G, D)$ associated with the divisors G and D is defined as

$$C_{\mathcal{L}}(G, D) := \{(f(P_1), \ldots, f(P_N)) | f \in \mathcal{L}(D)\} \subseteq \mathbb{F}_q^N.$$

Then $C_{\mathcal{L}}(G, D)$ is an $[N, k, d]$ code with parameters:

- dimension $k = \dim \mathcal{L}(D) - \dim \mathcal{L}(D - G)$
- minimum distance $d \geqslant N - \deg D$.

If $\{f_1, ..., f_n\}$ is a basis of $\mathcal{L}(D)$, the matrix

$$M := \begin{pmatrix} f_1(P_1) & \cdots & f_1(P_N) \\ f_2(P_1) & \cdots & f_2(P_N) \\ \vdots & \vdots & \vdots \\ f_n(P_1) & \cdots & f_n(P_N) \end{pmatrix}$$

is a generator matrix for $C_{\mathcal{L}}(G, D)$.

Observation

In our construction of CCMA,

We observe that:

- $Ev_{\mathcal{P}}(\mathcal{L}(D))$ is an AG code $C_{\mathcal{L}}(G, D) = [N, n, d]$
- The matrix of the restriction of $Ev_{\mathcal{P}}$ on $\mathcal{L}(D)$ is $T_D = M^t$

Upper-bound of $N_{zero}(T_D)$

We have

$$N_{zero}(T_D) = n \cdot N - N_{nz}(T_D),$$

where $N_{nz}(T_D)$ denotes the number of non-zero entries of T_D.

By the definition of minimum distance and its lower bound in AG code, we obtain:

$$\boxed{N_{zero}(T_D) \leqslant n \cdot \deg D}$$

If $N = 2n + g - 1$, in practical construction, we take the divisor D as a place of degree $n + g - 1$, then

$$\boxed{N_{zero}(T_D) \leqslant n(n + g - 1)}$$

.

Improved setup algorithm

We proposed a new setup algorithm for an efficient optimization of scalar complexity.

Algorithm 3 New setup algorithm for scalar complexity optimization (D. 2020)

INPUT: $F/\mathbb{F}_q$, Q, D, $\mathcal{P} = \{P_1, \dots, P_{2n+g-1}\}$.
OUTPUT: $\mathcal{B}_{2D} = \mathcal{B}_D \cup \mathcal{B}_D^c$, T_{2D} and $T_{2D,n}^{-1}$.

(i) Check that the function field $F/\mathbb{F}_q$ the place Q, the divisor D such that Conditions (i) and (ii) in Theorem 2 are satisfied.

(ii) Construct a basis $\mathcal{B}_D^c := (f_{n+1}, \dots, f_{2n+g-1})$ of the complementary space $KerE_Q|_{\mathcal{L}(2D)}$ of $\mathcal{L}(D)$ in $\mathcal{L}(2D)$.

(iii) Go through the set $\mathcal{S}$ of bases $\mathcal{B}_D$ of $\mathcal{L}(D)$, set $\underline{mB_D := \{\mathcal{B}_D \in \mathcal{S} \mid N_{zero}(T_D) = n(n+g-1)\}}$.

(iv) Search in mB_D a basis $opt\mathcal{B}_D := (f_1, \dots, f_n)$ such that $\underline{N_{zero}(T_{2D,n}^{-1})}$ (with respect to $\mathcal{B}_{2D} := opt\mathcal{B}_D \cup \mathcal{B}_D^c$) be the <u>largest</u>.

(v) Set $\mathcal{B}_Q := Ev_Q(opt\mathcal{B}_D)$.

Remark 1

(i) *The upper-bound depends on* $\deg D$*, not depend on the choice of a divisor among all effective divisors* D *such that* $D - Q$ *non-special.*

(ii) $$\boxed{N_{zero}(T^{-1}_{2D,n}) \leqslant ?? < n(2n+g-1)}$$

Theorem [D. (2020)]

Let $\mathcal{U}^{F,n}_{D,Q,\mathcal{P}}$ be a Chudnovsky[2] multiplication algorithm in a finite field $\mathbb{F}_{q^n}$ such that D is an effective divisor, $D - Q$ is non-special divisor of degree $g-1$, $|\mathcal{P}| = \dim(\mathcal{L}(2D)) = 2n+g-1$. Then

$$\mu^s_q(\mathcal{U}^{F,n}_{D,Q,\mathcal{P}}) > 2n^2$$

Other Strategies

Optimization strategies based on variations of the appropriate triplet $(D, Q, \mathcal{P})$.

1. Fixing a divisor D and a place Q, we change $\mathcal{P} = \{P_1, \ldots, P_N\}$ of $F/\mathbb{F}_q$.

Specific case: Permuting the order of interpolation points P_i, for $i = 1, \ldots, N$.

Proposition 3 [D. (2020)]

Let us consider an algorithm $\mathcal{U}^{F,n}_{D,Q,\mathcal{P}}$ such that D is an effective divisor, $D - Q$ a non-special divisor of degree $g-1$, and $|\mathcal{P}| = \dim \mathcal{L}(2D) = N$. For any π in S_N where S_N is the symmetric group on the set $\{1, 2, \ldots, N\}$, then the quantities $N_{zero}(T_D)$ and $N_{zero}(T^{-1}_{2D,n})$ are constants under the action π.

Optimization of scalar complexity of the elliptic CCMA

Experiment of Baum-Shokrollahi over an elliptic function field

Consider the multiplication in $\mathbb{F}_{256}$ over $\mathbb{F}_4 = \mathbb{F}_2(\omega)$ ($q = 4$ and $n = 4$) using the maximal elliptic curve $(\mathscr{C}) : y^2 + y = x^3 + 1$.

Let function field $F/\mathbb{F}_4$ associated to $\mathscr{C}$ over $\mathbb{F}_4$.

Then

$$N_1(\mathrm{F}) = q + 1 + 2gq^{\frac{1}{2}} = 9.$$

Check the conditions of Theorem 2 for using the algorithm of CCMA on $\mathrm{F}/\mathbb{F}_4$ to multiply in $\mathbb{F}_{4^4}$:

- $N_n > 0 \qquad \left(\Leftarrow 2g + 1 \leqslant q^{\frac{n-1}{2}}(q^{\frac{1}{2}} - 1)\right)$
- $N_1 \geqslant 2n + 2g - 1 \quad \Leftrightarrow \quad n \leqslant \frac{1}{2}(N_1 - 2g + 1)$

Consequence: the multiplication in the extension of degree $n = 4$ of $\mathbb{F}_4$ is possible with the curve $\mathscr{C}/\mathbb{F}_4$.

We obtain

$$\mu_q^b(\mathscr{C}/\mathbb{F}_4) = 2n + g - 1 = 8 \ \text{(optimal)}$$

Applying Algorithm 3 and using computations in Magma, we gave an improved basis $\mathcal{B}_{2D} = (f_1, f_2, \ldots, f_8)$ of $\mathcal{L}(2D)$, where

$$
\begin{aligned}
f_1 &= \frac{y + \omega x + \omega^2}{x^2 + x + \omega}, \\
f_2 &= \frac{y + \omega^2 x + \omega}{x^2 + x + \omega}, \\
f_3 &= \frac{\omega x^2 + \omega^2 x}{x^2 + x + \omega}, \\
f_4 &= \frac{\omega y}{x^2 + x + \omega}, \\
f_5 &= \frac{(\omega x^2 + \omega x)y + \omega^2 x^4 + \omega x^3 + x^2 + x + \omega}{x^4 + x^2 + \omega^2}, \\
f_6 &= \frac{\omega^2 x^2 y + \omega x^4 + \omega x^3 + x^2 + \omega x}{x^4 + x^2 + \omega^2}, \\
f_7 &= \frac{(x^2 + \omega^2 x)y + \omega x^4 + \omega x^2}{x^4 + x^2 + \omega^2}, \\
f_8 &= \frac{(\omega x + \omega)y + \omega x^4}{x^4 + x^2 + \omega^2}.
\end{aligned}
$$

$$T_{2D} = \left(\begin{array}{cccc|cccc}
0 & 0 & \omega & 0 & \omega^2 & \omega & \omega & \omega \\
\omega^2 & 0 & 0 & \omega & \omega^2 & 0 & 0 & 1 \\
0 & \omega^2 & 0 & \omega^2 & \omega^2 & 0 & 0 & \omega \\
\omega^2 & \omega^2 & \omega^2 & 0 & 1 & 1 & 0 & \omega^2 \\
0 & 0 & \omega^2 & 1 & 1 & 0 & \omega^2 & \omega^2 \\
0 & 1 & 0 & 0 & 0 & \omega^2 & 1 & \omega \\
\omega & \omega^2 & 0 & \omega^2 & 1 & \omega & 0 & 1 \\
\omega^2 & 0 & \omega & 0 & \omega & 0 & 1 & \omega^2
\end{array}\right)$$

$N_{zero}(T_D) = 16 = n(n+g-1) = \text{maximal}$

$$T_{2D,4}^{-1} = \begin{pmatrix}
1 & 0 & 0 & \omega^2 & \omega & 0 & \omega^2 & \omega^2 \\
1 & 1 & \omega^2 & 0 & 0 & \omega^2 & 0 & 1 \\
0 & 1 & \omega & 1 & \omega^2 & \omega & 0 & 0 \\
\omega^2 & \omega & \omega^2 & 0 & \omega & 0 & \omega^2 & 0
\end{pmatrix}$$

$N_{zero}(T_{2D,4}^{-1}) = 12$

Comparison

Method	$N_{zero}(T_D)$	$N_{zero}(T_{2D,4}^{-1})$	N_z	N_s
Baum-Shokrollahi	10	5	25	71
Our construction	16	12	44	52

We have a gain of 27% over Baum and Shokrollahi[1]'s method.

[1] Ulrich Baum and Amin Shokrollahi. "An optimal algorithm for multiplication in $\mathbb{F}_{256}/\mathbb{F}_4$". In: Applicable Algebra in Engineering, Communication and Computing 2.1 (1991), pp. 15–20.

Merci pour votre attention!