Optimization of scalar complexity of Chudnovsky-type algorithm in finite fields

Thanh-Hung Dang
Joint work with

Alexis Bonnecaze and Stéphane Ballet

Institut de Mathématiques de Marseille
Aix-Marseille Université

Seminar of ATI group
05 mars 2020

Introduction

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

Let $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/\langle P(x) \rangle$ and 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 $P(\beta)$

Complexity?

Number of elementary operations in $\mathbb{F}_q$:

1. Addition
2. Scalar multiplication (by a constant which does not depend on A or B)
3. Bilinear multiplication (the 2 operands depend on A and B)

Multiplication of the evaluation-Interpolation type

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

- Find $(2n-1)$ distinct points in $\mathbb{F}_q$: $\alpha_0, \ldots, \alpha_{2n-2}$
- Evaluate A and B at these points
- Multiply term by term these evaluations : $C(\alpha_i) = A(\alpha_i)B(\alpha_i)$
- Interpolate to obtain $C = A \cdot B$.

Example: Karatsuba's trick

Product of two polynomials of degree 1: $A(x) = a_0 + a_1 x$ and $B(x) = b_0 + b_1 x$

- Evaluation on the 3 points on the projective line over $\mathbb{F}_2$: $0, 1, \infty$

$$C(0) = a_0 b_0$$
$$C(1) = (a_0 + a_1)(b_0 + b_1)$$
$$C(\infty) = a_1 b_1$$

- $C(x) = C(0) + [C(1) - C(0) - C(\infty)]x + C(\infty)x^2$

Complexity:

$$Karatsuba : 3\ bilinear\ mult.,\ 4\ additions$$
$$vs$$
$$School - book\ method : 4\ bilinear\ mult.,\ 1\ addition$$

For polynomials of higher degrees, apply the method recursively,

Asymptotic bilinear/addition/ total complexity: $O(n^{\log_2 3})$ better than $O(n^2)$ of school-book method

Other algorithms

- Toom-Cook3: with 5 interpolation points
- Fast Fourier Transform (FFT): interpolation points are n-th roots of unity of $\mathbb{F}_q$
- FFT-based algorithm of Schönhage-Strassen

Algorithm	$m_q^b(n)$	$m_q^s(n)$	$M_q(n)$
Karatsuba	$O(n^{\log 3})$		$O(n^{\log 3})$
Toom-Cook3	$O(n^{\log_3 5})$	$O(n^{\log_3 5})$	$O(n^{\log_3 5})$
FFT$^{(*)}$	$O(n)$	$O(n \log n)$	$O(n \log n)$
Schönhage-Strassen	$O(n \log n)$	$O(n \log n \log_2 \log n)$	$O(n \log n \log \log n)$

$(*)$: FFT algorithm is done in condition that F_q containing an n^{th} primitive root of unity.

Chudnovsky^2 multiplication algorithm (CCMA)

David and Gregory Chudnovsky, 1988
Interpolation on algebraic curves

- allows more interpolation points
- Bilinear complexity in $O(n)$;

  Note that bilinear multiplications are the most expensive.

Problem

Scalar Complexity of Chudnovsky's algorithm?

Description

Theorem 1 ([1])

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* $\operatorname{supp} D \cap \{Q, P_1, \ldots, P_N\} = \varnothing$.

If

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

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

[1] D. V. Chudnovsky and G. V. Chudnovsky, "Algebraic complexities and algebraic curves over finite fields".

then

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

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

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) Let $\mathcal{U}$ denote the algorithm (1). Then we have:

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

Computational route for CCMA-based multiplication

$$
\begin{array}{rccl}
 & \mathcal{O}_Q & \xrightarrow{E_Q} & \mathrm{F}_Q \\
Q \notin \operatorname{supp} \mathcal{D} & \cup & & \wr\Vert \\
\mathrm{Ev}_Q : & \mathscr{L}(\mathcal{D}) & \xrightarrow{\mathrm{Ev}_Q = E_{Q\,|\,\mathscr{L}(\mathcal{D})}} & \mathbb{F}_{q^n} \\
 & & & \Cup \\
 & f & \dashrightarrow & x = f(Q) \\
 & g & \dashrightarrow & y = g(Q)
\end{array}
$$

$$
\begin{array}{rccl}
\mathrm{Ev}_{\mathcal{P}} : & \mathscr{L}(2\mathcal{D}) & \xhookrightarrow{\mathrm{Ev}_{\mathcal{P}}} & \mathbb{F}_q^N \\
 & f & \longmapsto & \bar{f} := \big(f(P_1), \ldots, f(P_N)\big) \\
 & g & \longmapsto & \bar{g} := \big(g(P_1), \ldots, g(P_N)\big) \\
 & & & \downarrow \\
 & fg & \dashrightarrow & \bar{h} := (f(P_1)g(P_1), \ldots, f(P_N) \\
 & {\scriptstyle E_Q} \big\downarrow & & \rightsquigarrow \\
 & & & \text{N } \textbf{bilinear} \text{ multiplications} \\
 & (fg)(Q) & = f(Q)g(Q) = xy &
\end{array}
$$

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

Let q be a prime power and let n be an integer > 1.
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 such that:

(i) The evaluation map

$$\begin{array}{rccc} Ev_Q : & \mathcal{L}(D) & \rightarrow & \frac{\mathcal{O}_Q}{Q} \\ & f & \mapsto & f(Q) \end{array}$$

is an isomorphism of vector spaces over $\mathbb{F}_q$.

(ii) There exist places $P_1,\ldots,P_N$ such that the evaluation map

$$\begin{array}{rccc} Ev_{\mathcal{P}} : & \mathcal{L}(2D) & \rightarrow & \mathbb{F}_q^N \\ & f & \mapsto & \Big(f(P_1), \ldots, f(P_N)\Big) \end{array}$$

is an isomorphism of vector spaces over $\mathbb{F}_q$ with $N = 2n+g-1$.

Construction of CCMA

Construction of CCMA is based on the choice of the following geometric objects:

Choice of $Q, D, \mathcal{L}(D), \mathcal{L}(2D)$**:**

- Place Q of degree n among the n places lying above an irreducible, totally decomposed polynomial $Q(x)$ of degree n in $\mathbb{F}_q[X]$
- Divisor D as a place of degree $n+g-1$ s.t $D-Q$ is non-special

Note: in practice, we take a divisor D one place of degree $n+g-1$. It has the advantage to solve the problem of the support of D as well as the effectivity of D (then $\mathcal{L}(D) \subseteq \mathcal{L}(2D)$)

Choice of $Q, D, \mathcal{L}(D), \mathcal{L}(2D)$

- Basis $\mathcal{B}_D$ of Rienman-Roch space $\mathcal{L}(D)$:

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

- Basis $\mathcal{B}_Q$ of $\mathcal{O}_Q/\langle Q\rangle = F_Q \cong \mathbb{F}_{q^n}$:

$$\mathcal{B}_Q = \mathcal{B}_Q^c := \{1, b, ..., b^{n-1}\};$$

  b is primitive root of $Q(x)$.

- 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 $\mathcal{L}(2D)$.

Algorithm 1 Original CCMA in $\mathbb{F}_{q^n}$

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

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

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

Algorithm 2 Kernel-type construction of CCMA

INPUT: $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$.

OUTPUT: xy.

1.

$$\begin{pmatrix} a_1 \\ \vdots \\ a_{2n+g-1} \end{pmatrix} = T_{2D} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \\ 0 \\ \vdots \\ 0 \end{pmatrix} \text{ and } \begin{pmatrix} b_1 \\ \vdots \\ b_{2n+g-1} \end{pmatrix} = T_{2D} \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

2. Compute $u = (u_1 \cdots u_{2n+g-1})^t$ where $u_i = a_i \cdot b_i$ for $i = 1, \ldots, 2n+g-1$.
3. Compute $v = (v_1 \cdots v_{2n+g-1})^t = T_{2D}^{-1} \cdot u$
4. Return $xy = (v_1, \ldots, v_n)$.

[2] Kevin Atighehchi et al. "Arithmetic in finite fields based on the Chudnovsky-Chudnovsky multiplication algorithm". In: Mathematics of Computation 86.308 (2017), pp. 2975–3000.

Optimization of scalar complexity for CCMA

Parameters to evaluate scalar complexity

Number of scalar multiplications:

$$N_s = 3n(2n + g - 1) - N_z,$$

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

- Original construction:

$$N_z = 2N_{zero}(T_D) + N_{zero}(CT_{2D}^{-1}).$$

- Kernel-type construction:

$$N_z = 2N_{zero}(T_D) + N_{zero}(T_{2D,n}^{-1}).$$

T_D is the first n columns of T_{2D},
$T_{2D,n}^{-1}$ is the first n rows of T_{2D}^{-1}

Objective

Let $\mathcal{U}_{D,Q,\mathcal{P}}^{F,n}$ be the original CCMA in $\mathbb{F}_{q^n}$.

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

$$N_z := 2N_{zero}(T_D) + N_{zero}(CT_{2D}^{-1})$$

the number of zeros in CCMA.

Brute force optimization

For each divisor D, each place Q, we vary the bases

- Basis $\mathcal{B}_D$ of the Riemann-Roch vector space $\mathcal{L}(D)$
- Basis $\mathcal{B}_Q$ of F_Q
- Basis $\mathcal{B}_D^c$ of the complementary subspace of $\mathcal{L}(D)$ in $\mathcal{L}(2D)$
- Basis $\mathcal{B}_{2D}$ of the Riemann-Roch vector space $\mathcal{L}(2D)$

Cost of optimization by brute force is very **expensive** !!

Strategy of scalar complexity optimization

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

Proposition[3]
Let us consider an original 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, $N_{zero}(CT^{-1}_{2D})$ is constant under this action.

[3] Stéphane Ballet, Alexis Bonnecaze, and Thanh-Hung Dang. "On the Scalar Complexity of Chudnovsky[2] Multiplication Algorithm in Finite Fields". In: Algebraic Informatics, CAI 2019, Lecture Notes in Computer Science, vol 11545. Springer Cham, 2019, pp. 64–75.

Proposition
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 3 First setup algorithm for the scalar complexity optimization[4]

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) 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 $\mathcal{L}(2D)$.

(iii) Go through the set of bases $\mathcal{B}_D$ of $\mathcal{L}(D)$. to compute T_{2D} and $T_{2D,n}^{-1}$ in the basis $\mathcal{B}_{2D} = \mathcal{B}_D \cup \mathcal{B}_D^c$.

(iv) Choose a basis $\mathcal{B}_D := (f_1, \ldots, f_n)$ such that N_z be the largest.

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

[4] Stéphane Ballet, Alexis Bonnecaze, and Thanh-Hung Dang. "On the Scalar Complexity of Chudnovsky[2] Multiplication Algorithm in Finite Fields". In: Algebraic Informatics, CAI 2019, Lecture Notes in Computer Science, vol 11545. Springer Cham, 2019, pp. 64–75.

Recall the definition of algebraic geometry code (Goppa 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 $suppP \cap suppD = \emptyset$.

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 $k = \dim \mathcal{L}(D) - \dim \mathcal{L}(D - G)$ and minimum distance d of the lower bound $(N - \deg D)$.

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 $C_{\mathcal{L}}(G, D)$.

In our construction of CCMA,

$Ev_{\mathcal{P}}(\mathcal{L}(D))$ is an algebraic geometry code $C_{\mathcal{L}}(G, D) = [N, n, d]$.

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

We observe that

$$T_D = M^t$$

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.

We see that

$$N_{nz}(T_D) \geqslant n \cdot d.$$

Since $d \geqslant N - \deg D$, we have

$$N_{nz}(T_D) \geqslant n(N - \deg D).$$

Thus,

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

If $N = 2n + g - 1$, in practical construction, we take the divisor D as a place of degree $n + g - 1$, then the upper bound of $N_{zero}(T_D)$ is $n(n + g - 1)$.

Remark 1

(i) *this 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) $N_{zero}(T^{-1}_{2D,n}) \leqslant ?? < n(2n + g - 1)$.
An intuitive idea: $T^{-1}_{2D,n} \rightsquigarrow$ *a certain "algebraic code" ?*

Theorem[5]
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

$$\mu^s_q(\mathcal{U}^{F,n}_{D,Q,\mathcal{P}}) > n(2n - 3g + 3).$$

[5] Thanh-Hung Dang, Stéphane Ballet, and Alexis Bonnecaze. "A note on improving scalar complexity of Chudnovsky[2] multiplication algorithm in finite fields". Submitted. 2020.

Based on upper-bound of $N_{zero}(T_D)$, we propose an efficient setup algorithm to improve the scalar complexity of CCMA

Algorithm 4 Second setup algorithm for an efficient optimization of scalar complexity

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_D 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 $\mathcal{B}_D^c := (f_{n+1}, ..., f_{2n+g-1})$ 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 $mB_D := \{\mathcal{B}_D \in \mathcal{S} \mid N_{zero}(T_D) = n(n+g\text{-}1)\}$.

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

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

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

- fixed D, Q, we vary $\mathcal{P}$
- fixed $Q, \mathcal{P}$, we vary D
- fixed $D, \mathcal{P}$, we vary Q
- we vary D, Q. Fix the set $\mathcal{P}$ in $F/\mathbb{F}_q$ associated to $\mathscr{C}/\mathbb{F}_q$

(i) First case: for a specific subcase that $\mathcal{P}' = \pi(\mathcal{P})$ for $\pi \in S_N$ -the symmetric group of order N.

Proposition[6]
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 $\{1, 2, ..., N\}$, then the quantities $N_{zero}(T_D)$ and $N_{zero}(T^{-1}_{2D,n})$ are constants under the action π.

[6] Thanh-Hung Dang, Stéphane Ballet, and Alexis Bonnecaze. "A note on improving scalar complexity of Chudnovsky[2] multiplication algorithm in finite fields". Submitted. 2020.

(ii) Second case, fixed Q and $\mathcal{P} = \{P_1, \ldots, P_{2n+g-1}\}$ of $F/\mathbb{F}_q$

Question: Is it possible to take an effective divisor D satisfying:

- $n + g - 1 < \deg D < 2n + g - 1$,
- $suppD \cap \{Q, P_1, \ldots, P_{2n+g-1}\} = \emptyset$,
- $D - Q$ is non-special

instead of choosing the divisor D as a place of degree $n + g - 1$ in $F/\mathbb{F}_q$?

If so, then the scalar complexity of CCMA will be reduced significantly.

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 4 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

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

Matrices in CCMA of kernel-type construction

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

and

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

Comparison

Compare to the result of using Baum-Shokrollahi's construction[7]

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

$(max N_{zero}(T_D) = n(n+g-1) = 16)$

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

[7] 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.

A comparison of complexities for the different methods

Method \ Complexity	$m_4^b(4)$	$m_4^s(4)$	$a_4(4)$	$M_4(4)$
Polynomial basis mult. (e.g. Karatsuba)	27	–	76	103
Baum-Shokrollahi's construction Kernel-type construction of CCMA$^{(*)}$	8	71	51	130
Kernel-type construction of CCMA$^{(**)}$	8	78	58	144
Our construction	8	52	32	92

(*) : using the canonical basis $\mathcal{B}_Q^c$ of F_Q,
(**) : using the normal basis $\mathcal{B}_Q^n$ of F_Q.

Scalar complexity/total complexity of our proposed construction is really better than other methods in case study $\mathbb{F}_{256}/\mathbb{F}_4$.

"We are the Champions !!"

Merci pour votre attention!