Chaining Multiplications in Finite Fields with Chudnovsky-type Algorithms and Tensor Rank of the k-multiplication

Stéphane Ballet and Robert Rolland

2022 October 29

Institut de Mathématiques de Marseille

Notations

Let $\mathbb{F}_q$ be a finite field with $q = p^r$ elements, where p is a prime number. Let $\mathbb{F}_{q^n}$ an extension of degree n of the field $\mathbb{F}_q$. We know that $\mathbb{F}_{q^n}$ can be considered as the quotient

$$\mathbb{F}_q[X]/(\Pi(X))$$

where $\Pi(X)$ is a degree n polynomial, with coefficients in $\mathbb{F}_q$, which is irreducible in $\mathbb{F}_q$. Hence :

Multiplication

The **multiplication** of two elements of $\mathbb{F}_{q^n}$ is the product of two polynomial in $\mathbb{F}_q[X]$, of degree $< n$, modulo $\Pi(X)$.

Algebraic interpretation

The multiplication m in the finite field $\mathbb{F}_{q^n}$ is a bilinear application of $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ in $\mathbb{F}_{q^n}$. Then it can be considered as a linear application M of the tensor product
$\mathbb{F}_{q^n} \bigotimes \mathbb{F}_{q^n}$ in $\mathbb{F}_{q^n}$ and can be represented as a tensor
$t_M \in \mathbb{F}^*_{q^n} \bigotimes \mathbb{F}^*_{q^n} \bigotimes \mathbb{F}_{q^n}$ where $\mathbb{F}^*_{q^n}$ denotes the dual of $\mathbb{F}_{q^n}$.
Any decomposition

$$t_M = \sum_{i=1}^{k} a_i^* \otimes b_i^* \otimes c_i \tag{1}$$

of the tensor t_M, where $a_i^*, b_i^* \in \mathbb{F}^*_{q^n}$ et $c_i \in \mathbb{F}_{q^n}$,leads to a multiplication algorithm

$$x.y = t_M(x \otimes y) = \sum_{i=1}^{k} a_i^*(x) b_i^*(y) c_i.$$

Definition

The **bilinear complexity** of the multiplication in $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$, denoted by $\mu_q(n)$, is the minimal number of terms in the decomposition (1). Namely the bilinear complexity of the multiplication is the rank of the tensor t_M.

Let us remark that the bilinear complexity of the multiplication is far from being the overall complexity. If one uses the decomposition (1), the linear operations, that is to say the computation of $x_i^*(x)$ and $y_i^*(y)$, are not taken into account in the bilinear complexity.

Interpolation on algebraic curves

We know that interpolation on points of $\mathbb{F}_q$ can give a multiplication algorithm. But if the number of points of $\mathbb{F}_q$ is $< 2n-2$ these algorithms do not succeed. D.V. and G.V. Chudnowski constructed in [3] an algorithm using interpolation on algebraic curves over F_q having enough rational points.

Theorem of D.V. Chudnovski and G.V. Chudnovski

Let $F/\mathbb{F}_q$ be an algebraic function field, Q a place of degré n of $F/\mathbb{F}_q$, $\mathcal{D}$ an effective divisor of $F/\mathbb{F}_q$ and $\mathcal{P} = \{P_1, ..., P_N\}$ a set of places of degree 1.
We suppose that Q, $P_1, \cdots, P_N$ are not in the spport of $\mathcal{D}$ and that
a) the evaluation function $Ev_Q : \mathcal{L}(\mathcal{D}) \to \mathbb{F}_{q^n} \simeq F_Q$ in the residual field in Q is onto.
b) the function

$$Ev_{\mathcal{P}} : \begin{cases} \mathcal{L}(2\mathcal{D}) & \to & \mathbb{F}_q^N \\ f & \mapsto & (f(P_1), ..., f(P_N)) \end{cases}$$

is injective.
Then

$$\mu_q(n) \leq N.$$

Details

First transform (similar to a Laplace transform)

$$\begin{array}{ccc} \mathbb{F}_{q^n} \simeq F_Q = \mathcal{O}_Q/Q & \xleftarrow{\curvearrowright} & \mathcal{L}(\mathcal{D}) \\ x = f(Q) & & f \\ y = g(Q) & & g \end{array}$$

Second Transform (similar to a Fourier transform)

$$\begin{array}{ccc} \mathcal{L}(\mathcal{D}) & \longrightarrow & (\mathbb{F}_q)^N \\ f & & (f(P_1), f(P_2), \cdots, f(P_N))) \\ g & & (g(P_1), g(P_2), \cdots, g(P_N))) \end{array}$$

Hadamard product

$$\begin{array}{ccc} Im(Ev_{\mathcal{P}}) \subset (\mathbb{F}_q)^N & \longrightarrow & \mathcal{L}(2\mathcal{D}) \\ (f(P_1)g(P_1), f(P_2)g(P_2), \cdots, f(P_N)g(P_N)) & & f.g \end{array}$$

Return

$$\begin{array}{ccc} \mathcal{L}(2\mathcal{D}) \subset \mathcal{O}_Q & \longrightarrow & F_Q = \mathcal{O}_Q/Q \simeq \mathbb{F}_{q^n} \\ f.g & & f.g(Q) = f(Q).g(Q) = x.y \end{array}$$

Example of hypothethis allowing the use of the method

(S. Ballet) Let q be a power of a prime number and $n > 1$ an integer. If it exists an algebraic function field $F/\mathbb{F}_q$ of genus $g(F)$ with $2g(F) + 1 \leq q^{\frac{n-1}{2}}(q^{\frac{1}{2}} - 1)$, having a number $N_1(F)$ of rational points such that $N_1(F) > 2n + 2g(F) - 2$, then

$$\mu_q(n) \leq 2n + g(F) - 1.$$

Consequences

Let $q = p^r$ be a power of the prime p and let n be an integer > 1. Then the bilinear complexity of multiplication in any finite field $\mathbb{F}_{q^n}$ is linear with respect to the extension degree n. More precisely, there exists a constant C_q such that for any $n > 1$:

$$\mu_q(n) \leq C_q n.$$

The best current values of the constants C_q are :

$$C_q = \begin{cases} \text{if } q = 2, & \text{then (1)} \quad 15.4575 \\ \text{else if } q = 3, & \text{then (2)} \quad \frac{1933}{250} \simeq 7.732 \\ \text{else if } q = p \geq 7, & \text{then (3)} \quad 3\left(1 + \frac{8}{3p-5}\right) \\ \text{else if } q = p^2 \geq 25, & \text{then (4)} \quad 2\left(1 + \frac{2}{p-\frac{33}{16}}\right) \\ \text{else if } q = p^{2k} \geq 64 \quad (k \geq 2), & \\ \quad \text{then (5)} \quad 2\left(1 + \frac{p}{\sqrt{q}-3+(p-1)\frac{\sqrt{q}}{\sqrt{q}+1}}\right) & \\ \text{else if } q \geq 4, & \\ \quad \text{then (6)} \quad 3\left(1 + \frac{\frac{4}{3}p}{q-3+2(p-1)\frac{q}{q+1}}\right) & \end{cases}$$

Historical Context

Seminal papers:

- David Chudnovsky and Gregory Chudnovsky, Algebraic Complexities and Algebraic Curves over Finite Fields.[3]
- Igor Shparlinski and Michael Tsfasman and Serguei Vladut, Curves with Many Points and Multiplication in Finite Fields.[7]

First uniform bounds (and correct proof of the linearity of bilinear complexity):

- author="Stéphane Ballet", title="Curves with Many Points and Multiplication Complexity in Any Extension of $\mathbb{F}_q$".[1]

A survey on further improvements done by numerous authors:

- Ballet, Stéphane and Pieltant, Julia and Rambaud, Matthieu and Randriambololona, Hugues and Rolland, Robert and Chaumine, Jean, On the tensor rank of multiplication in finite extension of finite fields and related issues in algebraic geometry.[2]

Generalization: multiplication of $k \geq 2$ elements

Now we want to generalize this theory to the case of the multiplication of k elements of $\mathbb{F}_{qn}$. If k is an integer ≥ 2, the multiplication m_k of k elements in the finite field $\mathbb{F}_{q^n}$ is a k-multilinear map from $\left(\mathbb{F}_{q^n}\right)^k$ into $\mathbb{F}_{q^n}$ over the field $\mathbb{F}_q$, thus it corresponds to a linear map M_k from the tensor power $\left(\mathbb{F}_{q^n}\right)^{\otimes k}$ into $\mathbb{F}_{q^n}$. One can also represent M_k by a k-covariant and 1-contravariant tensor $t_{M_k} \in \left(\mathbb{F}_{q^n}^*\right)^{\otimes k} \otimes \mathbb{F}_{q^n}$ where $\mathbb{F}_{q^n}^*$ denotes the algebraic dual of $\mathbb{F}_{q^n}$.

Each decomposition

$$t_{M_k} = \sum_{i=1}^{s} \left(\otimes_{j=1}^{k} a_{i,j}^* \right) \otimes c_i \tag{2}$$

of the tensor t_{M_k}, where $a_{i,j}^* \in \mathbb{F}_{q^n}^*$ and $c_i \in \mathbb{F}_{q^n}$, brings forth a multiplication algorithm of k elements

$$\prod_{j=1}^{k} x_j = t_{M_k}(\otimes_{i=1}^{k} x_j) = \sum_{i=1}^{s} \left(\prod_{j=1}^{k} a_{i,j}^*(x_j) \right) c_i. \tag{3}$$

Definition

A k-multilinear multiplication algorithm $\mathcal{U}_{q,n,k}$ in $\mathbb{F}_{q^n}$ is an expression

$$\prod_{j=1}^{k} x_j = \sum_{i=1}^{s} \left(\prod_{j=1}^{k} a_{i,j}^{*}(x_j) \right) c_i.$$

where $a_{i,j}^{\star} \in (\mathbb{F}_{q^n})^{\star}$, and $c_i \in \mathbb{F}_{q^n}$.
The number s of summands in this expression is called the k-multilinear complexity of the algorithm $\mathcal{U}_{q,n,k}$ and is denoted by $\mu_M(\mathcal{U}_{q,n,k})$. If k=2, it is the bilinear complexity of the algorithm.

It will be interesting to relate the k-multilinear complexity of the multiplication to the minimal number $\nu_{q,k}(n)$ of bilinear multiplications in $\mathbb{F}_q$ required to compute the product of k elements in the extension $\mathbb{F}_{q^n}$.

Lemma

$$\nu_{q,k}(1) \leq k-1, \tag{4}$$

$$\nu_{q,k}(n) \leq (k-1) \times \mu_q(n), \tag{5}$$

$$\mu_{q,k}(n) \leq \mu_{q,k}(mn) \leq \mu_{q,k}(m) \times \mu_{q^m,k}(n), \tag{6}$$

$$\nu_{q,k}(n) \leq \nu_{q,k}(mn) \leq \nu_{q,k}(m) \times \nu_{q^m,k}(n). \tag{7}$$

From a generalization of Chudnovsky-type algorithms to the k-multiplication, obtained by Randriambololona and Rousseau in [5] (cf. also [6]), that we generalize to places of arbitrary degree, we obtain upper bounds for the rank of the k-multiplication tensor in the finite fields. In this aim, we apply this type of algorithms to an explicit tower of Garcia-Stichtenoth [4] and the corresponding descent tower. Note that Randriambololona and Rousseau only obtain an asymptotic upper bound in $O(n)$ by using Shimura curves used by Shparlinski, Tsfasman and Vladut in [7].

theoretical construction

Let $F/\mathbb{F}_q$ be an algebraic function field over the finite field $\mathbb{F}_q$ of genus g. We denote by $N_i(F/\mathbb{F}_q)$ the number of places of degree i of F over $\mathbb{F}_q$. If D is a divisor, $\mathcal{L}(D)$ denotes the Riemann-Roch space associated to D. Let Q be a place of $F/\mathbb{F}_q$. We denote by $\mathcal{O}_Q$ the valuation ring of the place Q and by F_Q the residue class field $\mathcal{O}_Q/Q$ of the place Q which is isomorphic to $\mathbb{F}_{q^{\deg(Q)}}$ where $\deg(Q)$ is the degree of the place Q. Let us recall that for any $g \in \mathcal{O}_Q$, $g(Q)$ denotes the class of g in $\mathcal{O}_Q/Q = F_Q$.

Let us define the following Hadamard product in $\mathbb{F}_q^{N_1} \times \mathbb{F}_{q^2}^{N_2} \times \cdots \times \mathbb{F}_{q^d}^{N_d}$ where the N_i denote integers ≥ 0:

$$\bigodot_{i=1}^{k}(u_{1,1}^i, \cdots, u_{1,N_1}^i, \cdots, u_{d,1}^i, \cdots, u_{d,N_d}^i) =$$

$$\left(\prod_{i=1}^{k} u_{1,1}^i, \cdots, \prod_{i=1}^{k} u_{1,N_1}^i, \cdots, \prod_{i=1}^{k} u_{d,1}^i, \cdots, \prod_{i=1}^{k} u_{d,N_d}^i\right)$$

Theorem (Algorithm)

Let

1. q *be a prime power and* $k \geq 2$ *be an integer,*
2. $F/\mathbb{F}_q$ *be an algebraic function field,*
3. Q *be a degree* n *place of* $F/\mathbb{F}_q$*,*
4. $\mathcal{D}$ *be a divisor of* $F/\mathbb{F}_q$*,*
5. $\mathcal{P} = \{P_{1,1}, \cdots, P_{1,N_1}, \cdots, P_{d,1}, \cdots, P_{d,N_d}\}$ *be a set of* $N = \sum_{i=1}^{d} N_i$ *places of arbitrary degree where* $P_{i,j}$ *denotes a place of degree* i *and* N_i *a number of places of degree* i*.*

We suppose that Q and all the places in $\mathcal{P}$ are not in the support of $\mathcal{D}$ and that:

1. the map

$$Ev_Q : \left\{ \begin{array}{ccc} \mathcal{L}(\mathcal{D}) & \to & \mathbb{F}_{q^n} \simeq F_Q \\ f & \longmapsto & f(Q) \end{array} \right.$$

   is onto,

2. the map

$$Ev_{\mathcal{P}} : \left\{ \begin{array}{ccc} \mathcal{L}(k\mathcal{D}) & \longrightarrow & \mathbb{F}_q^{N_1} \times \mathbb{F}_{q^2}^{N_2} \times \cdots \times \mathbb{F}_{q^d}^{N_d} \\ f & \longmapsto & \big(f(P_{1,1}), \cdots, f(P_{1,N_1}), \cdots, f(P_{d,1}), \\ & & \cdots, f(P_{d,N_d})\big) \end{array} \right.$$

   is injective

Then, for any k elements $x_1, ..., x_k$ in $\mathbb{F}_{q^n}$, we have

$$m_k(x_1, ..., x_k) = Ev_Q\left(Ev_{\mathcal{P}}^{-1}\left(\bigodot_{i=1}^{k}\left(Ev_{\mathcal{P}}\left(Ev_Q^{-1}(x_i)\right)\right)\right)\right),$$

and

$$\mu_{q,k}(n) \leq \sum_{i=1}^{d} N_i \mu_{q,k}(i), \tag{8}$$

$$\nu_{q,k}(n) \leq (k-1)\sum_{i=1}^{d} N_i \mu_q(i). \tag{9}$$

Theorem (main)

Let q be a prime power and let n be an integer > 1. Let $F/\mathbb{F}_q$ be an algebraic function field of genus g. Let $\mathcal{P}_i$ be a set of places of degree i in $F/\mathbb{F}_q$ and N_i the cardinality of $\mathcal{P}_i$. We denote $\mathcal{P} = \bigcup_{i=1}^{r} \mathcal{P}_i$. Let us suppose that there is a place of degree n and a non-special divisor of degree $g-1$. If there is an integer $r \geq 1$ such that:

$$\sum_{i=1}^{r} iN_i > kn + kg - k \tag{10}$$

then

$$\mu_{q,k}(n) \leq \sum_{i=1}^{r} N_i \, \mu_{q,k}(i).$$

Let r_0, r_0' such that

$$\frac{\mu_{q,k}(r_0)}{r_0} = \sup_{1\le i\le r} \frac{\mu_{q,k}(i)}{i} \text{ and } \frac{\mu_q(r_0')}{r_0'} = \sup_{1\le i\le r} \frac{\mu_q(i)}{i}.$$

Then,

$$\mu_{q,k}(n) \le (kn + kg - k + r)\ \frac{\mu_{q,k}(r_0)}{r_0}. \tag{11}$$

$$\nu_{q,k}(n) \le (k-1)(kn + kg - k + r)\ \frac{\mu_q(r_0')}{r_0'}. \tag{12}$$

Remark

A place of degree n and a non-special divisor of degree $g-1$ exist if elementary numerical conditions are satisfied. More precisely, if

$$2g+1 \leq q^{\frac{n-1}{2}}(q^{\frac{1}{2}}-1), \tag{13}$$

then there exists a place of degree n. Moreover, if $q \geq 4$ or $N_1 \geq g+1$ then there exits a non-special divisor of degree $g-1$.

The main condition (10) of Theorem 9 supposes that we can find algebraic function fields having good properties. In particular, it is sufficient to have a family of function fields having sufficiently places with a certain degree r. In this aim, we focalize on sequences of algebraic functions fields with increasing genus attaining the Drinfeld-Vladut bound of order r. Hence, let us find the minimal integer r for such a family, so that Condition (10) is satisfied.

Let us consider a finite field $\mathbb{F}_{l^2}$ where l is a prime power such that $\mathbb{F}_{l^2}$ is an extension field of $\mathbb{F}_q$. We consider the Garcia-Stichtenoth's elementary abelian tower $\mathcal{F}$ over $\mathbb{F}_{l^2}$ constructed in [4] and defined by the sequence $\mathcal{F} = (F_0, F_1, \cdots, F_i, \cdots)$ where

$$F_0 := \mathbb{F}_{l^2}(x_0)$$

is the rational function field over $\mathbb{F}_{l^2}$, and for any $i \geq 0$, $F_{i+1} := F_i(x_{i+1})$ with x_{i+1} satisfying the following equation:

$$x_{i+1}^l + x_{i+1} = \frac{x_i^l}{x_i^{l-1} + 1}.$$

Then we can consider the descent tower $\mathcal{G}/\mathbb{F}_q$ defined over $\mathbb{F}_q$ given by the sequence:

$$G_0 \subset G_1 \subset \cdots \subset G_i \subset \cdots$$

defined over the constant field $\mathbb{F}_q$ and related to the tower $\mathcal{F}$ by: $F_i = \mathbb{F}_{l^2} \otimes_{\mathbb{F}_q} G_i$ for all i.

Using this tower and intricated computations we cannot give here we have the following result.

Theorem

Let r be the smallest integer such that $r > 2log_q(k+1)$. Then for any $n > 2r+3$ there exist a step G_i of the tower $\mathcal{G}/\mathbb{F}_q$ defined over $\mathbb{F}_q$ such that the main theorem can be applied using the algebraic function field G_i.

Theorem

Let q be a prime power and $k \geq 2$ be an integer and r the smallest even integer $> 2\log_q(k+1)$. Let r_0, r_0' such that

$$\frac{\mu_{q,k}(r_0)}{r_0} = \sup_{1 \leq i \leq r} \frac{\mu_{q,k}(i)}{i} \text{ and } \frac{\mu_q(r_0')}{r_0'} = \sup_{1 \leq i \leq r} \frac{\mu_q(i)}{i}.$$

Then for any integer n, we have:

$$\mu_{q,k}(n) \leq \frac{k(kq^{\frac{r}{2}}+1)n - k + r}{r_0} \mu_{q,k}(r_0) \tag{14}$$

and consequently

$$\nu_{q,k}(n) \leq \frac{k(k-1)(kq^{\frac{r}{2}}+1)n - (k-1)(k-r)}{r_0'} \mu_q(r_0'). \tag{15}$$


S. Ballet – "Curves with many points and multiplication complexity in any extension of $\mathbb{F}_q$", *Finite Fields and Their Applications* **5** (1999), p. 364–377.


S. Ballet, J. Pieltant, M. Rambaud, H. Randriambololona, R. Rolland & J. Chaumine – "On the tensor rank of multiplication in finite extension of finite fields and related issues in algebraic geometry", *Uspekhi Mat. Nauk* (2021), no. 76, p. 31–94.


D. Chudnovsky & G. Chudnovsky – "Algebraic complexities and algebraic curves over finite fields", *J. Complexity* **4** (1988), p. 285–316.


A. Garcia, H. Stitchtenoth & H.-G. Ruck – "On tame towers over finite fields", *Journal fur die reine und angewandte Mathematik* **557** (2003), p. 53–80.


H. Randriambololona & E. Rousseau – "Trisymmetric multiplication formulae in finite fields", in *Arithmetic of finite fields*

(WAIFI 2020) (J.-C. Bajard & A. Topuzoglu, éds.), vol. 12542, Springer International Publishing.

E. Rousseau – "Arithmétique efficace des extensions de corps finis", Thèse, Institut Polytechnique de Paris, 2021.

I. Shparlinski, M. Tsfasman & S. Vladut – "Curves with many points and multiplication in finite fields", *Lectures Notes in Mathematics* **1518** (1992), p. 145–169.