Computing a power of an element in a finite extension of a finite field

R. Rolland

Aix-Marseille Univ
web: http://www.acrypta.fr/

May 23, 2013

This presentation uses the Beamer LaTeXclass

Introduction

Let q be a prime power and $\mathbb{F}_q$ the finite field with q elements. We consider an extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$. The bilinear complexity of the multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ has been widely studied by many authors. The linearity of the bilinear complexity with respect to the degree n of the extension was claimed in Chudnovsky and Chudnovsky where a clever algorithm performing multipication is given: the so-called algorithm of Chudnovsky and Chudnovsky. Some remarks and improvements are developed in the article of Shparlinski, Tsfasman, Vladuts. Unfortunately these papers containing very interesting new ideas are not completely correct. A complete proof of the linearity of the bilinear complexity of the multiplication in a finite extension of a finite field was provided by Ballet. In this paper we tackle the problem of computing a^k where $a \in \mathbb{F}_{q^n}$ and $k \geq 1$.

The algebraic function field

Let $F/\mathbb{F}_q$ be an algebraic function field over the finite field $\mathbb{F}_q$ of genus $g(F)$. We denote by $N_1(F/\mathbb{F}_q)$ the number of rational points of F over $\mathbb{F}_q$. If D is a divisor, $\mathcal{L}(D)$ denotes the Riemann-Roch space associated to D. The following theorem groups some results of Ballet.

Theorem 1

Let n be an integer such that

$$2g(F) + 1 \leq q^{\frac{n-1}{2}} \left(q^{\frac{1}{2}} - 1 \right).$$

Then there is a place Q of degree n. Moreover, if $N_1(F/\mathbb{F}_q) > 2n + 2g - 2$ there is an effective divisor D such that:

1. Q is not in the support of D,
2. the evaluation map E defined by

$$\begin{array}{rccc} E: & \mathcal{L}(D) & \to & F_Q \\ & f & \mapsto & f(Q) \end{array}$$

   is an isomorphism of vector spaces over $\mathbb{F}_q$,
3. there exists $2n+g-1$ $\mathbb{F}_q$-rational points P_i which are not in the support of D such that the multi-evaluation map T defined by

$$\begin{array}{rccc} T: & \mathcal{L}(2D) & \to & (\mathbb{F}_q)^{2n+g-1} \\ & f & \mapsto & \left(f(P_1), \cdots, f(P_{2n+g-1})\right) \end{array}$$

   is an isomorphism.

Hypothesis

From now on we suppose that $F/\mathbb{F}_q$ is such that

1. $2g(F) + 1 \leq q^{\frac{n-1}{2}} \left(q^{\frac{1}{2}} - 1\right)$
2. $N_1(F/\mathbb{F}_q) > 2n + 2g - 2.$

so that Theorem 1 applies. The place Q, the effective divisor D and the points P_i are those given by Theorem 1.

The divisors D and $2D$

As the divisor D is effective, we have $\mathcal{L}(D) \subset \mathcal{L}(2D)$. If we consider the construction of D given by Ballet, the following holds:

$$\deg D = n + g - 1,$$

$$\dim \mathcal{L}(D) = n.$$

In particular D is non-special.

As $\deg 2D \geq 2g - 2$, the divisor $2D$ is non special and

$$\deg 2D = 2n + 2g - 2,$$

$$\dim \mathcal{L}(2D) = 2n + g - 1.$$

An adapted basis

Let P be the map from $\mathcal{L}(2D)$ to $\mathcal{L}(2D)$ defined in the following way: if $f \in \mathcal{L}(2D)$ then $f(Q)$ is in the residual field F_Q; define $P(f) = J \circ E^{-1}\left(f(Q)\right)$ where J is the injection map from $\mathcal{L}(D)$ into $\mathcal{L}(2D)$. Then P is a linear map from $\mathcal{L}(2D)$ into $\mathcal{L}(2D)$ whose image is $\mathcal{L}(D)$. More precisely, P is a projection from $\mathcal{L}(2D)$ onto $\mathcal{L}(D)$. Let $\mathcal{M}$ be the kernel of P. Then

$$\mathcal{L}(2D) = \mathcal{L}(D) \oplus \mathcal{M}.$$

Let $(f_1, \cdots, f_n)$ be a basis of $\mathcal{L}(D)$ and $(f_{n+1}, \cdots, f_{2n+g-1})$ a basis of $\mathcal{M}$. Remark that using this basis, if

$$x = (x_1, \cdots, x_n, x_{n+1}, \cdots, x_{2n+g-1}) \in \mathcal{L}(2D)$$

then

$$P(x) = (x_1, \cdots, x_n, 0, \cdots, 0).$$

Product of two elements

This product is computed by the algorithm of Chudnovsky and Chudnovsky. Let $x = (x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_n)$ be two elements of $\mathbb{F}_{q^n}$ given by their components over $\mathbb{F}_q$ relative to a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. As $\mathbb{F}_{q^n}$ is isomorphic to the residual field F_Q and then to $\mathcal{L}(D)$ we can consider that x and y are the following elements of $\mathcal{L}(D)$:

$$x = \sum_{i=1}^{n} x_i f_i \quad \text{and} \quad y = \sum_{i=1}^{n} y_i f_i.$$

This is an identification of $\mathbb{F}_{q^n}$ to $\mathcal{L}(D)$ that we use now. More precisely, we will consider that x and y are elements of $\mathcal{L}(2D)$ where the $n + g - 1$ last components are 0.

Let us define the following product in $(\mathbb{F}_q)^{2n+g-1}$:

$$(u_1, \cdots, u_{2n+g-1}).(v_1, \cdots, v_{2n+g-1}) = (u_1 v_1, \cdots, u_{2n+g-1} v_{2n+g-1}).$$

The product of x by y is

$$xy = P\left(T^{-1}\left(T(x).T(y)\right)\right).$$

Product of 3 elements

To understand how we can iterate the previous algorithm let us write the product of three elements x, y, z in $\mathcal{L}(D)$ (or in $\mathbb{F}_{q^n}$).

1. compute
$$u = T \circ P \circ T^{-1}\left(T(x).T(y)\right),$$
2. compute $v = T(z)$,
3. then compute $w = u.v$ (this is the product in $(\mathbb{F}_q)^{2n+g-1}$)
4. and finally the result is $P \circ T^{-1}(w)$.

Computing x^k

In order to compute x^k in $\mathbb{F}_{q^n}$ we are going to mix the previous algorithm with the algorithm square and multiply that is nothing else than a rewriting of the Hörner's algorithm.
Let us set $T_1 = T \circ P \circ T^{-1}$. Denote by K the unidimensional array of length $s+1$ containing the bits of k. This array will be indexed by $i = 0, \cdots, s$. More precisely

$$k = \sum_{i=0}^{s} K[i] 2^i.$$

In order to bind operations we must iterate the use of the operator T_1.
Then it will be interesting to choose a basis (f_i) giving a "simple" matrix for T_1.
The details of the algorithm are given in the next subsection.

Power(x, K);
(initializing)
$X_0 \leftarrow T(x)$;
$X \leftarrow (1, 1, \cdots, 1)$;
(iterative part)
while $i > 0$
do
$X \leftarrow X.X$;
$X \leftarrow T_1(X)$;
if $K[i] == 1$ then
$X \leftarrow X.X_0$;
$X \leftarrow T_1(X)$;
fi;
$i \leftarrow i - 1$;
od;
(closing)
$X \leftarrow X.X$;
if $K[0] == 1$ then
$X \leftarrow T_1(X)$;
$X \leftarrow X.X_0$;
fi;
$Y \leftarrow P \circ T^{-1}(X)$;
Return Y;
End;

Obviously the crucial part of the algorithm consuming more time is the iterative call to T_1, namely the iterative call to the composition $T \circ P \circ T^{-1}$. The matrix T is the following:

$$\begin{pmatrix} f_1(P_1) & f_2(P_1) & \cdots & f_{2n+g-1}(P_1)) \\ f_1(P_2) & f_2(P_2) & \cdots & f_{2n+g-1}(P_2)) \\ \vdots & \vdots & \vdots & \vdots \\ f_1(P_n) & f_2(P_n) & \cdots & f_{2n+g-1}(P_n)) \\ \vdots & \vdots & \vdots & \vdots \\ f_1(P_{2n+g-1}) & f_2(P_{2n+g-1}) & \cdots & f_{2n+g-1}(P_{2n+g-1})) \end{pmatrix}$$

The matrix P is the following

$$\left(\begin{array}{c|c} I_n & 0 \\ \hline 0 & 0 \end{array}\right)$$

where I_n is the unit matrix of size $n \times n$.

Let us define the following blocs:

$$T = \left(\begin{array}{c|c} A & C \\ \hline B & D \end{array}\right)$$

where A is a $n \times n$-matrix, B is a $(n+g-1) \times n$-matrix, C is a $n \times (n+g-1)$-matrix and D is a $(n+g-1) \times (n+g-1)$-matrix.

In the same way, we can write T^{-1} in the following form:

$$T^{-1} = \left(\begin{array}{c|c} U & W \\ \hline V & T \end{array}\right)$$

Then

$$T\,P\,T^{-1} = \left(\begin{array}{c|c} AU & AW \\ \hline BU & BW \end{array}\right)$$

Moreover we have the following relations hold:

$$AU + CV = I_n,$$

$$AW + CT = 0,$$

$$BU + DV = 0,$$

$$BW + DT = I_{n+g-1}.$$

The problem now is to choose the basis (f_i) of $\mathcal{L}(2D)$ and the rational points P_i in order to obtain a "simple" matrix.