Optimal Algorithms for Multiplication in certain Finite Fields using Elliptic Curves

MOHAMMAD AMIN SHOKROLLAHI
Institut für Informatik V, Universität Bonn

July 31, 1990

Abstract

Using results of D.V. Chudnovsky, G.V. Chudnovsky [3] and W.C. Waterhouse [10] we prove that the rank (=bilinear complexity of multiplication) of the finite field $\mathbf{F}_{q^n}$ viewed as an $\mathbf{F}_q$-algebra is $2n$ if n satisfies $\frac{1}{2}q+1 < n < \frac{1}{2}(q+1+\epsilon(q))$. Here $\epsilon(q)$ is the greatest integer $\leq 2\sqrt{q}$ which is prime to q if q is not a perfect square and $\epsilon(q) = 2\sqrt{q}$ if q is a perfect square.

1 Introduction

Let K be a field and L a simple finite extension field of K. The *rank* $R(L/K)$ of L over K is defined to be the bilinear complexity of multiplication in L/K where K is regarded as the field of scalars [7]. Denoting by L^* the dual of L as a vector space over K we have thus

$$R(L/K) = \min\Big\{ r \in \mathbf{N} \;\Big|\; \exists\, u_i, v_i \in L^*, w_i \in L \;\forall a, b \in L : ab = \sum_{i=1}^{r} u_i(a)v_i(b)w_i \Big\}.$$

Let n denote the degree $(L : K)$. It is known that $R(L/K) \geq 2n-1$ with equality holding if and only if $|K| \geq 2n-2$ [6]. The optimal multiplication algorithms realizing the lower bound $2n-1$ all belong to the class of *interpolation algorithms* [11]. These algorithms are based on the principle of reconstruction of polynomial products by Lagrange-interpolation [3]. In other words, these algorithms can be viewed as interpolation algorithms on the projective line over $\mathbf{F}_q$.

Noticing that a switch to arbitrary algebraic curves results in the existence of more rational points than in the case of a projective line, D.V. Chudnovsky and G.V. Chudnovsky generalized the existing algorithms to projective curves having additional arithmetic properties [3]. Using special well studied algebraic curves, they were the first to show that for an infinite set of prime powers q the rank of $\mathbf{F}_{q^n}/\mathbf{F}_q$ is asymptotically bounded from above by a linear function of n.

Our paper is concerned with the application of the algorithm invented by Chudnovsky and Chudnovsky to the first nontrivial class of algebraic curves, the so called *elliptic curves*. Elliptic curves play an important role in different areas of mathematics and computer science and have been studied very well during the last decades.

Besides classical results about elliptic curves we are interested in the question of the existence of elliptic curves over the finite field $\mathbf{F}_q$ with as many rational points as possible. This question has been answered by Waterhouse [10]. Combining the results of Waterhouse with the mentioned interpolation algorithm on algebraic curves we are able to compute the exact rank of certain field extensions of the finite field $\mathbf{F}_q$ (Theorem 5).

The paper is organized as follows: In Section 2 we summarize some well known results about elliptic function fields (which are the function fields of the elliptic curves). Section 3 is devoted to the application of a slight modification of the algorithm presented in [3] to elliptic function fields. Section 4 discusses the question of the existence of elliptic function fields having those additional arithmetic properties required by the algorithm of Section 3. Section 5 is devoted to the formulation and proof of the main theorem.

2 Basic Facts about Elliptic Function Fields

In this section we are going to introduce some basic notations and summarize well known results about elliptic function fields over finite fields. All these facts can be found in standard textbooks such as [1, 2, 5, 9].

Let $K/\mathbf{F}_q$ be an elliptic function field with constant field $\mathbf{F}_q$, i.e. $\mathbf{F}_q$ is assumed to be algebraically closed in K. By $\mathbf{P}(K/\mathbf{F}_q)$ we denote the set of prime divisors of $K/\mathbf{F}_q$. $\mathbf{D}(K/\mathbf{F}_q)$ denotes the group of divisors of $K/\mathbf{F}_q$ defined to be the free abelian group over $\mathbf{P}(K/\mathbf{F}_q)$. The relation $\leq$ defined

by

$$\sum_{\mathfrak{p}} a_{\mathfrak{p}}\mathfrak{p} \leq \sum_{\mathfrak{p}} b_{\mathfrak{p}}\mathfrak{p} \quad :\Longleftrightarrow \quad \forall \mathfrak{p}\ \ a_{\mathfrak{p}} \leq b_{\mathfrak{p}}$$

is a partial order on $\mathbf{D}(K/\mathbf{F}_q)$.

For $\mathfrak{p} \in \mathbf{P}(K/\mathbf{F}_q)$ we define $K\mathfrak{p}$ to be the residue class field of $\mathfrak{p}$. It is well known that $K\mathfrak{p}$ is a finite extension of $\mathbf{F}_q$. The index $(K\mathfrak{p} : \mathbf{F}_q)$ is denoted by $\deg(\mathfrak{p})$ and is called the *degree of* $\mathfrak{p}$. The map $\mathfrak{p} \mapsto \deg(\mathfrak{p})$ can be uniquely extended to $\mathbf{D}(K/\mathbf{F}_q)$ by

$$\deg(\sum_{\mathfrak{p}} a_{\mathfrak{p}}\mathfrak{p}) := \sum_{\mathfrak{p}} a_{\mathfrak{p}} \deg(\mathfrak{p}).$$

To every non-vanishing function f in K one can associate the divisor

$$(f) := \sum_{\mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}(f)\,\mathfrak{p}$$

called the *principal divisor of* f. Here $\mathrm{ord}_{\mathfrak{p}}(f)$ denotes the $\mathfrak{p}$-order of f. The principal divisors form a subgroup $\mathbf{H}(K/\mathbf{F}_q)$ of $\mathbf{D}(K/\mathbf{F}_q)$ isomorphic to $K^{\times}/\mathbf{F}_q^{\times}$. All principal divisors are of degree zero. For a divisor $\mathfrak{A} \in \mathbf{D}(K/\mathbf{F}_q)$ the set $\mathfrak{A} + \mathbf{H}(K/\mathbf{F}_q)$ is called the *class of* $\mathfrak{A}$. Since principal divisors are of degree zero, the degree map is constant on classes of divisors.

For $\mathfrak{A} \in \mathbf{D}(K/\mathbf{F}_q)$ we denote by $\mathcal{L}(\mathfrak{A})$ the *linear space attached to* $\mathfrak{A}$ which besides 0 contains all non-vanishing functions f of K with $(f) \geq -\mathfrak{A}$. $\mathcal{L}(\mathfrak{A})$ is even a vector space of finite dimension $\dim(\mathfrak{A})$ over $\mathbf{F}_q$. The number $\dim(\mathfrak{A})$ is called the *dimension* of the divisor $\mathfrak{A}$. Like the degree, the dimension is also a class function.

The theorem of Riemann-Roch [9, Theorem 5.4] relates the dimension and the degree of an arbitrary divisor of $K/\mathbf{F}_q$.

Theorem 1 (Theorem of Riemann-Roch) *Let $K/\mathbf{F}_q$ be an elliptic function field and $\mathfrak{A} \in \mathbf{D}(K/\mathbf{F}_q)$ be an arbitrary divisor. Then we have*

$$\dim(\mathfrak{A}) = \begin{cases} 0 & \text{if } \deg(\mathfrak{A}) < 0, \\ 1 & \text{if } \mathfrak{A} \in \mathbf{H}(K/\mathbf{F}_q), \\ \deg(\mathfrak{A}) & \text{otherwise.} \end{cases}$$

The set of prime divisors of degree one of $K/\mathbf{F}_q$ is denoted by $\mathbf{P}_1(K/\mathbf{F}_q)$. Since $K/\mathbf{F}_q$ is elliptic this set is not empty. Hasse [8] proved the inequality

$$q + 1 - 2\sqrt{q} \leq |\mathbf{P}_1(K/\mathbf{F}_q)| \leq q + 1 + 2\sqrt{q}. \tag{1}$$

We shall be interested in elliptic function fields with as many prime divisors of degree one as possible. For example, if q is a perfect square we ask if there are elliptic function fields having $q+1+2\sqrt{q}$ prime divisors of degree one.

An answer to this question can be given using a more general theorem of Waterhouse [10] which gives necessary and sufficient conditions for the existence of an elliptic function field having $t+q+1$ prime divisors of degree one if t is a given natural number satisfying $|t| \leq 2\sqrt{q}$ in view of (1). Before stating the result, let us introduce the function ϵ defined by

$$\epsilon(q) := \begin{cases} \text{greatest integer} \leq 2\sqrt{q} \text{ prime to } q & \text{if } q \text{ is not a perfect square,} \\ 2\sqrt{q} & \text{if } q \text{ is a perfect square.} \end{cases}$$

Theorem 2 (Waterhouse [10]) *Let q be a prime power. Then there exists an elliptic function field over $\mathbf{F}_q$ having $q+1+\epsilon(q)$ prime divisors of degree one.*

3 Interpolation in Elliptic Function Fields

In this section we shall discuss a modified version of a bilinear algorithm due to D.V. Chudnovsky and G.V. Chudnovsky [3] for multiplication in a finite extension of $\mathbf{F}_q$. We shall first state the result.

Theorem 3 *Let q be a prime power and n be a natural number. Suppose that there exists an elliptic function field $K/\mathbf{F}_q$ satisfying the following conditions:*

(1) *K contains a prime divisor $\mathfrak{p}$ of degree n.*

(2) *K contains a divisor $\mathfrak{B}$ of degree n the class of which is different from that of $\mathfrak{p}$ and for which $\mathrm{ord}_{\mathfrak{P}}(\mathfrak{B}) = 0$ for all prime divisors $\mathfrak{P}$ of degree one of $K/\mathbf{F}_q$.*

(3) *$|\mathbf{P}_1(K/\mathbf{F}_q)| > 2n$.*

Then we have

$$R(\mathbf{F}_{q^n}/\mathbf{F}_q) \leq 2n.$$

Proof. The proof proceeds along the same lines as in [3].

Let $\mathfrak{p}$ and $\mathfrak{B}$ be as in the assumptions of the theorem. Since $\mathfrak{p}$ is of degree n the residue class field $K\mathfrak{p}$ of $\mathfrak{p}$ is isomporphic to $\mathbf{F}_{q^n}$. Further, since

$\mathfrak{B}$ and $\mathfrak{p}$ belong to different classes and $\mathfrak{p}$ is assumed to be prime, we have $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{B}) = 0$ showing that $\mathcal{L}(\mathfrak{B})$ is contained in the valuation ring of $\mathfrak{p}$. Let $\kappa : \mathcal{L}(\mathfrak{B}) \to K\mathfrak{p}$ denote the restriction of the residue class mapping on $\mathcal{L}(\mathfrak{B})$. Thus κ defines a vector space homomorphism. The kernel of κ is $\mathcal{L}(\mathfrak{B} - \mathfrak{p})$. Since $\mathfrak{B}$ and $\mathfrak{p}$ belong to different classes, $\mathfrak{B} - \mathfrak{p}$ is not principal. Theorem 1 implies now that $\mathcal{L}(\mathfrak{B} - \mathfrak{p})$ is trivial which shows that κ is injective. By Theorem 1 $\dim(\mathfrak{B}) = n$, hence κ is an isomorphism. So there exists a basis $f_1, \ldots, f_n$ of $\mathcal{L}(\mathfrak{B})$ which is mapped by κ onto a basis of $K\mathfrak{p}$ over $\mathbf{F}_q$.

Let $\{g_1, \ldots, g_{2n}\}$ be a basis of $\mathcal{L}(2\mathfrak{B})$. Then there exist elements $B_{ij}^r \in \mathbf{F}_q$ such that

$$f_i f_j = \sum_{r=1}^{2n} B_{ij}^r g_r.$$

Furthermore, $\mathcal{L}(2\mathfrak{B})$ is also contained in the valuation ring of $\mathfrak{p}$. By abuse of notation let us denote the extension of κ to $\mathcal{L}(2\mathfrak{B})$ again by κ. Then there exist $c_r^m \in \mathbf{F}_q$ such that we have

$$\kappa(g_r) = \sum_{m=1}^{n} c_r^m \kappa(f_m), \qquad r = 1, \ldots, 2n.$$

Let $\sum_{i=1}^n x_i \kappa(f_i)$ and $\sum_{j=1}^n y_j \kappa(f_j)$ be two arbitrary elements of $K\mathfrak{p} = \mathbf{F}_{q^n}$. Then we get

$$\Big(\sum_{i=1}^{n} x_i \kappa(f_i)\Big)\Big(\sum_{j=1}^{n} y_j \kappa(f_j)\Big) = \sum_{m=1}^{n} \Big(\sum_{r=1}^{2n} \Big(\sum_{i,j=1}^{n} x_i y_j B_{ij}^r\Big) c_r^m\Big) \kappa(f_m). \qquad (2)$$

Let the bilinear forms $Z_1, \ldots, Z_{2n}$ be defined by

$$Z_r := \sum_{i,j=1}^{n} x_i y_j B_{ij}^r, \qquad r = 1, \ldots, 2n.$$

By (2) every bilinear algorithm of length l for computing $Z_1, \ldots, Z_{2n}$ produces an algorithm of length l for multiplication in $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$. Hence we have

$$R(\mathbf{F}_{q^n}/\mathbf{F}_q) \leq R(\{Z_1, \ldots, Z_{2n}\}),$$

where $R(\{Z_1, \ldots, Z_{2n}\})$ denotes the bilinear complexity of the set of bilinear forms $\{Z_1, \ldots, Z_{2n}\}$ (certificate [6, Chapter I]).

For the computation of $Z_1, \ldots, Z_{2n}$ we are going to use the interpolation algorithm presented in [3].

Let $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_N\}$ be the set of prime divisors of degree one of $K/\mathbf{F}_q$. Further let the matrix Γ be defined by

$$\Gamma := \begin{pmatrix} g_1(\mathfrak{P}_1) & \cdots & g_{2n}(\mathfrak{P}_1) \\ \vdots & \ddots & \vdots \\ g_1(\mathfrak{P}_N) & \cdots & g_{2n}(\mathfrak{P}_N) \end{pmatrix}.$$

This matrix is defined since by the assumptions of the theorem $\mathrm{ord}_{\mathfrak{P}}(\mathfrak{B}) = 0$ for all $\mathfrak{P} \in \mathbf{P}_1(K/\mathbf{F}_q)$. The rank of Γ equals $2n$: Consider the homomorphism

$$\begin{aligned} \gamma : \ \mathcal{L}(2\mathfrak{B}) &\to \mathbf{F}_q^N \\ g &\mapsto (g(\mathfrak{P}_1), \ldots, g(\mathfrak{P}_N)). \end{aligned}$$

Γ is the representation matrix of γ with respect to the basis $\{g_1, \ldots, g_{2n}\}$ in $\mathcal{L}(2\mathfrak{B})$ and the canonical basis in $\mathbf{F}_q^N$. The kernel of γ is $\mathcal{L}(2\mathfrak{B} - (\mathfrak{P}_1 + \ldots + \mathfrak{P}_N))$ which is trivial by Theorem 1 since N is assumed to be larger than $2n$. So γ is injective meaning that Γ has rank $2n$. Without loss of generality suppose that the first $2n$ rows of Γ are linearly independent. Denote by Γ_0 the matrix formed by these rows of Γ. We define further

$$X_s := \sum_{i=1}^{n} x_i f_i(\mathfrak{P}_s), \ Y_s := \sum_{j=1}^{n} y_j f_j(\mathfrak{P}_s), \ s = 1, \ldots, 2n.$$

Now we compute $(X_1Y_1, \ldots, X_{2n}Y_{2n})$. This step of the algorithm requires $2n$ essential multiplications.

Since by (2) we have

$$\Gamma_0(Z_1, \ldots, Z_{2n})^\top = (X_1Y_1, \ldots, X_{2n}Y_{2n})^\top,$$

we get the desired bilinear forms $Z_1, \ldots, Z_{2n}$ without further essential multiplications. This proves the theorem. ∎

Note that in the algorithm presented above $\mathfrak{B}$ does not need to be integral, a condition assumed in [3].

4 Technical Tools

This section is rather technical and is primarily concerned with the question which elliptic function fields satisfy the conditions of Theorem 3.

The first problem we are concerned with is that of the existence of prime divisors of given degree in an elliptic function field. The next lemma answers this question.

Lemma 1 *Let q be a prime power, $q \geq 4$. Further let n be a natural number satisfying $n > \frac{1}{2}q + 1$. Then every elliptic function field over $\mathbf{F}_q$ contains a prime divisor of degree n.*

Proof. In [3] it is proved that the number N_n of prime divisors of degree n of an algebraic function field of genus g over $\mathbf{F}_q$ satisfies the inequality

$$N_n \geq \frac{1}{n}\left(q^n - q^{n/2}(4g+q)\right).$$

Since the genus of an elliptic function field is one, it suffices to prove the inequality

$$q^{n/2} > 4 + q.$$

Because $q \geq 4$ is assumed, the stronger inequality $q^{n/2} > 2q$ also yields the result. But this inequality is satisfied for all n with $n > 2\log 2/\log q + 2$. Now the assertion follows since for $q \geq 4$ we have $\frac{1}{2}q + 1 \geq 2\log 2/\log q + 2$. ∎

For proving the existence of the divisor $\mathfrak{B}$ we first have to show that there exist two different divisor classes of degree n. This is the content of the next lemma.

Lemma 2 *Let $K/\mathbf{F}_q$ be an elliptic function field which has at least two different prime divisors of degree one. Then K contains two different divisor classes of degree n for every natural number n.*

Proof. Let $\mathfrak{o}$ be a divisor of degree one of $K/\mathbf{F}_q$. Further let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be two different prime divisors of degree one of $K/\mathbf{F}_q$ and $\mathfrak{A}$ be a divisor of degree n of $K/\mathbf{F}_q$. Then $\mathfrak{A} + \mathfrak{p}_1 - \mathfrak{o}$ and $\mathfrak{A} + \mathfrak{p}_2 - \mathfrak{o}$ clearly belong to two different classes of degree n. ∎

With the foregoing two lemmas at hand we can prove the existence of the divisor $\mathfrak{B}$ of Theorem 3.

Theorem 4 *Let q be a prime power, $q \geq 4$, and n be an integer with $n > \frac{1}{2}q + 1$. Further let $K/\mathbf{F}_q$ be an elliptic function field with at least two prime*

divisors of degree one. Then K contains a prime divisor $\mathfrak{p}$ of degree n and a divisor $\mathfrak{B}$ of degree n not belonging to the class of $\mathfrak{p}$ such that for all $\mathfrak{P} \in \mathbf{P}_1(K/\mathbf{F}_q)$ we have $\mathrm{ord}_{\mathfrak{P}}(\mathfrak{B}) = 0$.

Proof. The existence of $\mathfrak{p}$ follows from Lemma 1. Let C_1 denote the class of $\mathfrak{p}$. By Lemma 2 K contains a class C_2 of divisors of degree n with $C_1 \neq C_2$. By [5, Lemma 1, pp. 71] C_2 contains a divisor $\mathfrak{B}$ such that $\mathrm{ord}_{\mathfrak{P}}(\mathfrak{B}) = 0$ for all $\mathfrak{P} \in \mathbf{P}_1(K/\mathbf{F}_q)$. This proves the theorem. ∎

5 The main result

This section is devoted to the formulation and proof of the main theorem of this paper.

Theorem 5 *Let q be a prime power and n an integer satisfying $\frac{1}{2}q + 1 < n < \frac{1}{2}(q + 1 + \epsilon(q))$. Then we have*

$$R(\mathbf{F}_{q^n}/\mathbf{F}_q) = 2n.$$

Proof. Since for $q \in \{2, 3\}$ the assertion of the theorem is empty, let us suppose that $q \geq 4$. Let $K/\mathbf{F}_q$ be an elliptic function field with $q + 1 + \epsilon(q)$ prime divisors of degree one. (The existence of K follows from Theorem 2.) Since $q \geq 4$, the function field $K/\mathbf{F}_q$ contains more than two prime divisors of degree one. Applying Lemma 1 and Lemma 2 we get the existence of a prime divisor $\mathfrak{p}$ of degree n as well as the existence of the divisor $\mathfrak{B}$ with the conditions stated in Theorem 3. Further the assumption on n implies $2n < q + 1 + \epsilon(q)$. Hence, Theorem 3 yields the assertion $R(\mathbf{F}_{q^n}/\mathbf{F}_q) \leq 2n$.

Now by [6, Theorem 1.4], if $q < 2n - 2$ we have $R(\mathbf{F}_{q^n}/Fq) > 2n - 1$. So the assertion of the theorem follows. ∎

As a corollary to the above theorem we get the following:

Corollary 1 *Let q be a prime power which is a perfect square. Further let n be an integer satisfying $\frac{1}{2}q + 1 < n < \frac{1}{2}(q + 1 + 2\sqrt{q})$. Then we have*

$$R(\mathbf{F}_{q^n}/\mathbf{F}_q) = 2n.$$

Acknowledgement. The author wants to thank *Michael Clausen* for many helpful discussions during the research on this paper.

References

[1] *E. Artin*: *Algebraic Numbers and Algebraic Functions.* Gordon and Breach Science Publishers, 1977.

[2] *C. Chevalley*: *Introduction to Algebraic Functions of one Variable.* Am. Math. Society, New York, 1958.

[3] *D.V. Chudnovsky, G.V. Chudnovsky*: Algebraic Complexities and Algebraic Curves over Finite Fields. *Proc. Natl. Acad. Sci. USA*, **84**, 1739–1743, (1987).

[4] *D.V. Chudnovsky, G.V. Chudnovsky*: Algebraic Complexities and Algebraic Curves over Finite Fields. Research Report RC 12065, IBM Research Center, Yorktown Heights, (1987).

[5] *M. Deuring*: *Lectures on the Theory of Algebraic Functions of One Variable.* Lecture Notes in Mathematics **314**. Springer-Verlag, Heidelberg, New York, Tokyo, 1973.

[6] *H.F. de Groote*: Characterization of Division Algebras of Minimal Rank and the Structure of their Algorithm Varieties. *SIAM Journal of Computing*, **12**, 101–117, (1983).

[7] *H.F. de Groote*: *Lectures on the Complexity of Bilinear Problems.* Lecture Notes in Computer Science, **245**, Springer-Verlag, New York, Berlin, Heidelberg, Tokyo, 1985.

[8] *H. Hasse*: Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F.K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen. *Nachr. der math. Gesellschaft zu Göttingen*, 253–262, (1933).

[9] *J. H. Silverman*: *The Arithmetic of Elliptic Curves.* Springer-Verlag, New York, Berlin, Heidelberg, Tokyo, 1986.

[10] *W.C. Waterhouse*: Abelian Varieties over Finite Fields. *Ann. scient. Ec. Norm. Sup.*, **4**, 521–560, (1969).

[11] *S. Winograd*: On Multiplication in Algebraic Extension Fields. *Theoretical Computer Science*, **8**, 359–377, (1979).