Counting Prime Divisors on Elliptic Curves and Multiplication in Finite Fields

M. Amin Shokrollahi

Bell Labs, Rm. 2C-353, 700 Mountain Ave, Murray Hill, NJ 07974, USA

Abstract Let $K/\mathbb{F}_q$ be an elliptic function field. For every natural number n we determine the number of prime divisors of degree n of $K/\mathbb{F}_q$ which lie in a given divisor class of K.

1 Introduction

If K is a number field it is well known that there exist infinitely many prime divisors which belong to a fixed divisor class and that the (Dirichlet-)density of the set of such prime divisors is $1/h$ where h is the class number of K [6, §9]. The proof of this theorem is similar to the proof of the theorem on the number of primes in an arithmetic progression and proceeds roughly as follows: One first separates the prime divisors in the different classes by the characters of the class group and uses then orthogonality relations of the characters together with the non-vanishing of the L-series at 1 (which constitutes the deep part of the theorem). In fact, one of the approaches to class field theory is based on the investigation of the Dirichlet-density of the set of prime divisors lying in a given (ray-) class [6].

If K is an algebraic function field over a finite field, then we might similarly ask for the number of prime divisors belonging to a fixed class. In this situation there exist only finitely many prime divisors in each class since there are only finitely many integral divisors in each divisor class. However, as it will be shown in this paper, the method outlined above will prove successful in answering this question for the case K is an elliptic function field over the finite field $\mathbb{F}_q$.

Let $K/\mathbb{F}_q$ be an elliptic function field and C be a divisor class of K. Denoting by $a(C)$ the number of prime divisors in the class C, we are thus asking for the exact value of $a(C)$ for all C. If C is a class of degree one for example, $a(C) = 1$, since no two distinct prime divisors of degree one are equivalent in K.

The group $\mathcal{C}$ of divisor classes of K is the direct product of the group $\mathcal{C}_0$ of divisor classes of degree zero and the infinite cyclic group generated by $[Q]$ where $[Q]$ is the class of an arbitrary divisor Q of degree one [5, pp. 64]. Let us define $a_{n,Q}(C_0)$ for a class C_0 of degree zero and an integer n by

$$a_{n,Q}(C_0) := a(C_0[Q]^n).$$

For the ease of notation we shall suppress the dependency of $a_{n,Q}$ on Q and write simply a_n instead. We can thus equivalently ask for the value of $a_n(C_0)$ for all n and all classes C_0 of degree zero (where we can of course confine ourselves to the case $n \geq 1$). This question will be answered in this paper (Theorem 6).

Our question can be translated to the language of elliptic curves: let E be an elliptic curve over the field $\mathbb{F}_q$. Denote by $E(\mathbb{F}_{q^n})$ the group of $\mathbb{F}_{q^n}$-rational points of E. Let σ denote the Frobenius automorphism of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. We define the trace map by

$$\begin{aligned} \mathrm{Tr}\colon E(\mathbb{F}_{q^n}) &\to E(\mathbb{F}_q) \\ P &\mapsto \textstyle\sum_{i=0}^{n-1} P^{\sigma^i} \end{aligned}$$

where $\sum$ denotes the summation in the group $E(\mathbb{F}_q)$. Denote the restriction of Tr on $E(\mathbb{F}_{q^n}) \setminus \cup_{d|n,\, d<n} E(\mathbb{F}_{q^d})$ by tr. Suppose that Q is the neutral element of $E(\mathbb{F}_q)$. Let C be an arbitrary class of degree 0 of the function field K of E. As a consequence of the Riemann-Roch theorem there exists a unique $P \in E(\mathbb{F}_q)$ such that $C = [P - Q]$. Then $a_n(C)$ is equal to the cardinality of the fiber of tr at P.

The method for obtaining a formula for $a_n(C)$ (which resembles Dirichlet's proof of the existence of infinitely many primes in an arithmetic progression) can be described as follows: First we introduce appropriate characters of the class group $\mathcal{C}$ of $K/\mathbb{F}_q$ which will "separate" the prime divisors belonging to different classes. Then the corresponding L-functions are constructed. Taking logarithms of the L-functions and applying the inversion formula for the characters we will be able to obtain a recursion formula for $a_n(C)$ (Section 2). Next we apply the principle of inclusion and exclusion to solve the recursion (Section 3). The final formula for $a_n(C)$ involves the numbers Π_d of prime divisors of degree d of $K/\mathbb{F}_q$ for different d (or equivalently the numbers N_d of divisors of degree one of $K\mathbb{F}_{q^d}/\mathbb{F}_{q^d}$) and the number of classes C' some power of which equal C (Theorem 6). The next sections deal with the problem of determining extremal values of a_n for given n. It turns out that a_n is constant if n and the number h of classes of degree 0 of K, are coprime (Lemma 7). Further a_n attains its minimum value at $\mathcal{H}$, the principal class of K (Theorem 17). The techniques developed in Section 5 can be utilized to prove several results on the distribution of the numbers $a_n(C_0)$ for a fixed n. We have confined ourselves to mention some of the more interesting results (compare also Theorems 30 and 33).

The interest of the author in the numbers $a_n(C)$ arouse in the context of optimal bilinear algorithms for multiplication in finite fields. For instance, the results of this paper have been used in [9] to construct an efficient randomized algorithm which produces optimal bilinear algorithms for multiplication in certain finite fields (see also [10]). An example in this direction is given in the final section of the paper.

2 L-Functions

Let $K/\mathbb{F}_q$ be an elliptic function field. By $\mathcal{C}$ we denote the class group and by $\mathcal{C}_0$ the group of classes of degree 0 of $K/\mathbb{F}_q$. Let P be a prime divisor of degree one of $K/\mathbb{F}_q$ and denote by $[P]$ its class. It is well known (see the introduction) that $\mathcal{C} = \mathcal{C}_0 \times [P]^{\mathbb{Z}}$. Any character χ of $\mathcal{C}_0$ can be extended to a character $\tilde{\chi}$ of $\mathcal{C}$ by setting $\tilde{\chi}(A) := \chi(A - \deg(A)P)$. By abuse of notation we shall denote $\tilde{\chi}$ by χ.

The **L-function** of a character χ of $\mathcal{C}$ is defined by

$$L(s,\chi) := \sum_A \chi(A)N(A)^{-s}$$

where the sum is over all integral divisors of $K/\mathbb{F}_q$, and $N(A)$ denotes the norm of the divisor A, i.e., $N(A) = q^{\deg(A)}$. $L(s,\chi)$ has an **Euler-product-expansion** [5, §24]

$$L(s,\chi) = \prod_P (1 - \chi(P)N(P)^{-s})^{-1} \tag{1}$$

where the product extends over all prime divisors of $K/\mathbb{F}_q$. If ε denotes the principal character of $\mathcal{C}$, we call $L(s,\varepsilon)$ the **ζ-function** of $K/\mathbb{F}_q$ and denote it by $\zeta(s)$.

For the rest of this paper we assume that $\mathrm{Re}(s) > 1$ which implies that the series encountered converge absolutely [5, Lecture 11].

While the ζ-function of an elliptic function field plays a great role in the arithmetic theory, the L-functions attached to extensions of non-principal characters of $\mathcal{C}_0$ to C are trivial:

Lemma 1. *Let $K/\mathbb{F}_q$ be an elliptic function field. Further let χ be a non-principal character of $\mathcal{C}_0$. Then $L(s,\chi) = 1$.*

Proof. In [5, pp. 66, §25] it is proved that

$$(q-1)L(s,\chi) = \sum_{C \in \mathcal{C}_0} \chi(C) q^{\dim(C)}.$$

Now observe that $\dim(C) = 0$ if C is not the principal class and $\dim(C) = 1$ if C is the principal class. Since χ is not the principal character, we have $\sum_{C \in \mathcal{C}_0} \chi(C) = 0$, hence

$$(q-1)L(s,\chi) = q - 1$$

which yields the assertion. □

In order to get a formula for the numbers $a_n(C)$ we first take the logarithm of $L(s,\chi)$ using formula (1):

$$\log L(s,\chi) = \sum_P \sum_{m \geq 1} \frac{\chi(P)^m}{mN(P)^{-sm}}.$$

Taking into account that $N(P) = q^{\deg(P)}$ this yields

$$\log L(s,\chi) = \sum_P \sum_{m\geq 1} \frac{\chi(P)^m}{m} u^{\deg(P)m}$$

where we have followed the customary convention $u := q^{-s}$. Now we divide the above sum into sums over prime divisors belonging to a fixed class:

$$\log L(s,\chi) = \sum_{C\in\mathcal{C}} \sum_{\substack{P \\ [P]=C}} \sum_{m\geq 1} \frac{\chi(C)^m}{m} u^{\deg(P)m}.$$

The isomorphism $\mathcal{C} = \mathcal{C}_0 \times [Q]^{\mathbb{Z}}$ allows to classify the classes according to their degree:

$$\log L(s,\chi) = \sum_{C\in\mathcal{C}_0} \sum_{n\geq 1} \sum_{m\geq 1} a_n(C) \frac{\chi(C)^m}{m} u^{nm}.$$

The above sum is a power series in u. A trivial computation yields the following normal representation of this power series:

$$\log L(s,\chi) = \sum_{\nu\geq 1} \frac{1}{\nu} \Big(\sum_{d|\nu} \sum_{C\in\mathcal{C}_0} a_d(C)\, d\, \chi(C)^{\frac{\nu}{d}} \Big) u^\nu. \tag{2}$$

Now let $C_0 \in \mathcal{C}_0$ be a fixed class and X denote the character group of $\mathcal{C}_0$. We have:

$$\sum_{\chi\in X} \chi(C_0^{-1}) \log L(s,\chi) = \sum_{\nu\geq 1} \frac{1}{\nu} \Big(\sum_{d|\nu} \sum_{C\in\mathcal{C}_0} a_d(C) d \sum_{\chi\in X} \chi(C_0^{-1} C^{\frac{\nu}{d}}) \Big) u^\nu.$$

It is well known that if a is an element of a finite abelian group A and X denotes the character group of A, then $\sum_{\chi\in X} \chi(a) = 0$ if a is not equal to the identity-element of A, whereas this sum equals the cardinality of A if a is the identity element of A. Applying this we get

$$\sum_{\chi\in X} \chi(C_0^{-1}) \log L(s,\chi) = \sum_{\nu\geq 1} \frac{1}{\nu} \Big(\sum_{d|\nu} \sum_{\substack{C\in\mathcal{C}_0 \\ C^{\nu/d}=C_0}} a_d(C)\, d\, h \Big) u^\nu \tag{3}$$

where $h = |\mathcal{C}_0|$ is the number of classes of degree 0 of $K/\mathbb{F}_q$ (i.e., the number of $\mathbb{F}_q$-rational points of the corresponding elliptic curve).

By Lemma 1, $\log L(s,\chi) = 0$ for non-principal χ. Hence, taking into account Equation (2) and the fact that $\sum_{C_0\in\mathcal{C}_0} a_n(C_0) = \Pi_n$, the above sum equals

$$\log L(s,\varepsilon) = \sum_{\nu\geq 1} \frac{1}{\nu} \Big(\sum_{d|\nu} \Pi_d d \Big) u^\nu. \tag{4}$$

Since the right hand sides of Equation (3) and Equation (4) are equal power series we get

$$\forall C_0 \in \mathcal{C}_0 \, \forall \nu \geq 1 : \sum_{d|\nu} \Pi_d d = \sum_{d|\nu} \Big(\sum_{\substack{C \in \mathcal{C}_0 \\ C^{\nu/d} = C_0}} a_d(C) \Big) dh.$$

This proves the following recursion formula:

Lemma 2. *Let n be an arbitrary positive integer and C_0 be an arbitrary class of degree zero of the elliptic function field $K/\mathbb{F}_q$. We have*

$$a_n(C_0) = \frac{1}{h}\Pi_n + \sum_{\substack{d|n \\ d<n}} \Big(\frac{1}{h}\Pi_d - \sum_{\substack{C \in \mathcal{C}_0 \\ C^{n/d} = C_0}} a_d(C) \Big) \frac{d}{n}. \tag{5}$$

In the next section we shall solve this recursion.

3 Resolution of the Recursion

The principle of inclusion and exclusion is applied in this section to solve the recursion (5).

For $n \in \mathbb{N}$ and $C_0 \in \mathcal{C}_0$ define

$$A(d; n, C_0) = A(d) := \begin{cases} \Big(\frac{1}{h}\Pi_d - \sum_{\substack{C \in \mathcal{C}_0 \\ C^{n/d} = C_0}} a_d(C) \Big) \frac{d}{n} & \text{if } d|n \\ 0 & \text{otherwise.} \end{cases}$$

Further, let $f(m; n, C_0) = f(m) := \sum_{d|\gcd(m,n)} A(d)$. Our first aim is to prove the following:

Lemma 3. *If $m|n$, we have*

$$f(m) = \frac{1}{hn} \sum_{d|m} d \, \Pi_d \, (1 - |\{ C \mid C^{n/m} = C_0 \}|).$$

Proof. We have

$$f(m) = \Big(\frac{1}{h}\Pi_m - \sum_{\substack{C \in \mathcal{C}_0 \\ C^{n/m} = C_0}} a_m(C) \Big) \frac{m}{n} + \sum_{\substack{d|m \\ d<m}} \Big(\frac{1}{h}\Pi_d - \sum_{\substack{C \in \mathcal{C}_0 \\ C^{n/d} = C_0}} a_d(C) \Big) \frac{d}{n}.$$

By Equation (5) we obtain

$$\begin{aligned} f(m) &= \Big(\frac{1}{h}\Pi_m - \sum_{\substack{C\in\mathcal{C}_0\\(C^{n/m}=C_0)}} \Big(\frac{1}{h}\Pi_m + \sum_{\substack{d|m\\d<m}} \Big(\frac{1}{h}\Pi_d - \sum_{\substack{C'\in\mathcal{C}_0\\(C'^{m/d}=C)}} a_d(C')\Big)\frac{d}{n}\Big)\Big)\frac{m}{n} \\ &\quad + \sum_{\substack{d|m\\d<m}} \Big(\frac{1}{h}\Pi_d - \sum_{\substack{C\in\mathcal{C}_0\\(C^{n/d}=C_0)}} a_d(C)\Big)\frac{d}{n} \\ &= \frac{1}{h}\sum_{d|m} d\,\Pi_d\,(1 - |\{\, C \mid C^{n/m} = C_0 \,\}|) \\ &\quad - \sum_{\substack{d|m\\d<m}} \Big(\sum_{\substack{C\in\mathcal{C}_0\\(C^{n/m}=C_0)}} \sum_{\substack{C'\in\mathcal{C}_0\\(C'^{m/d}=C)}} a_d(C') - \sum_{\substack{C\in\mathcal{C}_0\\(C^{n/d}=C_0)}} a_d(C)\Big). \end{aligned}$$

Now note that

$$\sum_{\substack{C\in\mathcal{C}_0\\(C^{n/m}=C_0)}} \sum_{\substack{C'\in\mathcal{C}_0\\(C'^{m/d}=C)}} a_d(C') = \sum_{\substack{C\in\mathcal{C}_0\\(C^{n/d}=C_0)}} a_d(C).$$

Hence the assertion follows. □

Denote by N_m the number of prime divisors of degree one of $K\mathbb{F}_{q^m}/\mathbb{F}_{q^m}$. It is well known that $N_m = \sum_{d|m} \Pi_d d$. Thus the following corollary follows:

Corollary 4. *We have*

$$f(m) = \frac{1}{hn} N_m (1 - |\{\, C \mid C^{n/m} = C_0 \,\}|).$$

Now we apply the principle of inclusion and exclusion:

Lemma 5. *Let S be a finite set, $S_1, \ldots, S_k$ subsets of S and $A\colon S \to \mathbb{Z}$ a mapping. For $T \subseteq S$ let $A_\Sigma(T) := \sum_{t\in T} A(t)$. Then we have*

$$\begin{aligned} A_\Sigma(S \setminus \cup_{i=1}^k S_i) = A_\Sigma(S) &- \sum_{i=1}^k A_\Sigma(S_i) + \sum_{1\le i<j\le k} A_\Sigma(S_i \cap S_j) \\ &- \sum_{1\le i<j<l\le n} A_\Sigma(S_i \cap S_j \cap S_l) + \cdots \\ &+ (-1)^k A_\Sigma(S_1 \cap S_2 \cap \cdots \cap S_k). \end{aligned}$$

Proof. This is a straightforward generalization of [1, Theorem 5.31]. □

Theorem 6. *Let $K/\mathbb{F}_q$ be an elliptic function field, $\mathcal{C}_0$ be the group of divisor classes of degree zero of K, $C_0 \in \mathcal{C}_0$ and n an integer greater or equal to zero.*

Then

$$a_n(C_0) = \frac{1}{h}\Big(\Pi_n - \frac{1}{n}\sum_{\substack{d|n\\ d<n}} \mu\Big(\frac{n}{d}\Big) N_d(1 - \big|\{\, C \mid C^{n/d} = C_0 \,\}\big|)\Big)$$
$$= \frac{1}{hn}\sum_{d|n} \mu\Big(\frac{n}{d}\Big) N_d \big|\{\, C \mid C^{n/d} = C_0 \,\}\big|.$$

Proof. Let $n = \prod_{i=1}^{k} p_i^{a_i}$ be the prime factor decomposition of n. Set $S := \{d \mid d|n\}$ and $S_i := \{d \mid d|\frac{n}{p_i}\}$ for $i = 1, \ldots, k$. Then $S \setminus \cup_{i=1}^{k} S_i = \{n\}$. Applying Lemma 5 with $A(.) = A(.; n, C_0)$ we get

$$\frac{1}{h}\Pi_n - a_n(C_0) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big) f(d).$$

Now note that $f(n) = 0$. So applying Lemma 3 we get the first equality. The second equality follows from the first by observing that application of Möbius-inversion to $\sum_{d|n} \Pi_d d = N_n$ yields $\Pi_n = \frac{1}{n}\sum_{d|n} N_d\, \mu(n/d)$. □

Before going into elaborate estimates of the above sums, let us derive first a simple lemma from Theorem 6. Let $C_0 \in \mathcal{C}_0$ and consider $a_1(C_0)$. As was remarked in the introduction $a_1(C_0) = 1 = \Pi_1/h$ for all C_0 in $\mathcal{C}_0$. Can we expect $a_n(C_0) = \Pi_n/h$ for all n and all $C_0 \in \mathcal{C}_0$ (at least as long as Π_n is a multiple of h)? The following lemma gives a sufficient condition for this to be the case.

Lemma 7. *Suppose that n and h are coprime. Then $a_n(C_0) = \Pi_n/h$ for all $C_0 \in \mathcal{C}_0$.*

Proof. Since $(n, h) = 1$, the homomorphism $C_0 \mapsto C_0^n$ is an automorphism of $\mathcal{C}_0$. Hence $\big|\{\, C \mid C^{n/d} = C_0 \,\}\big| = 1$ for all $C_0 \in \mathcal{C}_0$. The assertion follows now from Theorem 6. □

The following example shows that the condition in the preceding lemma is not necessary:

Example 8. The elliptic function field $K = \mathbb{F}_4(x, y), y^2 + y = x^3 + 1$ has 9 prime divisors of degree one [2]. The group of divisors of degree 0 of K is easily computed to be the direct product of two cyclic groups of order 3 (note that $\mathcal{C}_0$ is isomorphic to the group of $\mathbb{F}_4$-rational points of the corresponding elliptic curve). K has $\Pi_6 = 648$ prime divisors of degree 6. Further, $N_2 = N_1 = 9$ and $|\{C \mid C^2 = C_0\}| = 1$ since $(2, 9) = 1$, and $|\{C \mid C^3 = C_0\}| = |\{C \mid C^6 = C_0\}|$ for all $C_0 \in \mathcal{C}_0$. Applying Theorem 6 we get

$$a_6(C_0) = \frac{1}{9}\Pi_6 = 72 \qquad \text{for all } C_0 \in \mathcal{C}_0.$$

Example 8 is actually an exception. In Section 5 we will prove a partial converse to Lemma 7 (see Theorem 33).

In the next sections we investigate the extremal values of the function a_n.

4 Some Tools

In this section we shall gather some well known results about abelian groups and elliptic function fields. This will serve as a toolbox for the computations in the next section.

To begin with, let us introduce a notation: If A is an abelian group and n an integer, we define $A^n := \{a^n \mid a \in A\}$. The following lemma is almost trivial:

Lemma 9. *Let A be a finite abelian group and n, m integers. Then $A^n \cap A^m = A^{\mathrm{lcm}(n,m)}$ and $A^n A^m = A^{\gcd(n,m)}$.*

Proof. Let A be the direct product of B and C. Then $A^n \cap A^m = (B^n \times C^n) \cap (B^m \times C^m)$, so $A^n \cap A^m = (B^n \cap B^m) \times (C^n \cap C^m)$. Analogously $A^n A^m = (B^n B^m) \times (C^n C^m)$. Since the assertion of the lemma is easily verified for cyclic groups, the general case follows by decomposition of A into cyclic factors. □

Let A be a finite abelian group, n an integer and $\pi_n^A \colon A \to A^n, a \mapsto a^n$.

Lemma 10. *If A is a finite abelian group, m, n are integers and π_n^A is as above, we have:*

$$|\ker \pi^A_{\mathrm{lcm}(m,n)}| = \frac{|\ker \pi_n^A||\ker \pi_m^A|}{|\ker \pi^A_{\gcd(n,m)}|}.$$

Proof. Application of Lemma 9 yields:

$$\begin{aligned}
|\ker \pi^A_{\mathrm{lcm}(m,n)}| &= \frac{|A|}{|A^{\mathrm{lcm}(m,n)}|} \\
&= \frac{|A|}{|A^n|}\frac{|A^n|}{|A^{\mathrm{lcm}(m,n)}|} \\
&= \frac{|A|}{|A^n|}\frac{|A^{\gcd(m,n)}|}{|A^m|} \\
&= \frac{|A|}{|A^n|}\frac{|A|}{|A^m|}\frac{|A^{\gcd(n,m)}|}{|A|} \\
&= \frac{|\ker \pi_n^A||\ker \pi_m^A|}{|\ker \pi^A_{\gcd(n,m)}|}. \quad \square
\end{aligned}$$

We immediately get the following corollaries whose proofs are obvious.

Corollary 11. *If A is a finite abelian group and m, n are coprime integers, we have*

$$|\ker \pi^A_{mn}| = |\ker \pi_n^A||\ker \pi_m^A|.$$

Corollary 12. *Let A be a finite abelian group and n, m coprime integers. Then*

$$H_{A^{nm}} = H_{A^n} H_{A^m},$$

where H_M is denotes the characteristic function of the set M.

Now we want to investigate some elementary problems related to elliptic function fields.

Lemma 13. *Let $K/\mathbb{F}_q$ be an elliptic function field, $q \geq 5$, and n, k be positive integers, $k \geq 2$. Then*

$$q^{n(k-2)} N_n \leq N_{nk} \leq q^{nk} N_n.$$

Proof. We apply the well known **Hasse-Weil-inequality**

$$|N_n - q^n - 1| \leq 2\sqrt{q^n}$$

to get

$$\frac{(\sqrt{q^{nk}} - 1)^2}{(\sqrt{q^n} + 1)^2} \leq \frac{N_{nk}}{N_n} \leq \frac{(\sqrt{q^{nk}} + 1)^2}{(\sqrt{q^n} - 1)^2}$$

Now note that if $a \geq \sqrt{5}$ is a real number and k is as above, we have

$$\frac{(a^k - 1)^2}{(a+1)^2} \geq a^{2(k-2)}$$
$$\frac{(a^k + 1)^2}{(a-1)^2} \leq a^{2k}.$$

Putting $a = \sqrt{q^n}$ we get the assertion. □

Remark 14. (1) The first inequality in the above lemma is also valid for $q = 4$. It is even sharp for $q = 4, n = 1, k = 2$ (as can be seen in the case of the function field $K = \mathbb{F}_4(x, y),\ x^3 + y^3 = 1$).

(2) The inequalities given are very crude for big q. Nevertheless we shall not need more refined estimates for the computations in the next section.

Now let $K/\mathbb{F}_q$ be an elliptic function field and $\mathcal{C}_0$ denote the group of divisor classes of degree 0 of K. For a nonnegative integer n we denote the homomorphism $\pi_n^{\mathcal{C}_0}$ simply by π_n. The kernel of π_n (also called the **group of n-division points**) plays an important role in the formulas of Theorem 6 as is apparent from the following

Lemma 15. *Let $C_0 \in \mathcal{C}_0$ and n be a positive integer. Then*

$$|\{C \mid C^n = C_0\}| = H_{\mathcal{C}_0^n}(C_0) |\ker \pi_n|.$$

Proof. Trivial. □

The order of $\ker \pi_n$ depends on n and the structure of $\mathcal{C}_0$. However, since $\mathcal{C}_0$ is always of the type $C_l \times C_m$ with $l|m$ (See e.g. [8]), we get the following (well known) estimate:

Lemma 16. *With the above notation we have* $|\ker \pi_n| \leq n^2$.

Proof. If $\mathcal{C}_0 = C_l \times C_m$ we have $|\ker \pi_n| = \gcd(n,l)\gcd(n,m) \leq n^2$. □

With these tools at hand, we are now able to derive some lower and upper bounds for the numbers $a_n(C_0)$. This will be done in the next section.

5 Some Estimates for $a_n(C_0)$

The aim of this section is to prove the following

Theorem 17. *Let $K/\mathbb{F}_q$ be an elliptic function field, $q \geq 7$, and n be an integer satisfying $n \leq 2^{q^{12}}$. Denote by $\mathcal{C}_0$ the group of divisor classes of degree 0 and by $\mathcal{H}$ the principal class of K. For $C_0 \in \mathcal{C}_0$ let $a_n(C_0)$ be defined as above. Then we have*

(1) $a_n(\mathcal{H}) = \min_{C_0 \in \mathcal{C}_0} a_n(C_0)$.
(2) *Let $\overline{n}$ denote the squarefree part of n. Then $a_n(C_0) = a_n(\mathcal{H})$ if and only if $C_0 \in \mathcal{C}_0^{\overline{n}}$.*
(3) *Suppose there exists $C_0 \in \mathcal{C}_0$ such that $C_0 \notin \mathcal{C}_0^p$ for all $p|n$. Then $a_n(C_0) = \max_{C_0 \in \mathcal{C}_0} a_n(C_0) = \frac{1}{hn} N_n$.*

Before starting with the proof of this theorem, let us state an immediate corollary:

Corollary 18. *With the same notation as above we have $a_n(\mathcal{H}) \leq \Pi_n/h$.*

Proof. We have

$$\Pi_n = \sum_{C_0 \in \mathcal{C}_0} a_n(C_0) \geq \sum_{C_0 \in \mathcal{C}_0} a_n(\mathcal{H}) = h a_n(\mathcal{H}). \quad \square$$

The proof of Theorem 17 requires some preliminary discussions. It is based on the investigation of $a_n(\mathcal{H}) - a_n(C_0)$ for arbitrary $C_0 \in \mathcal{C}_0$. Application of Theorem 6 and Lemma 15 yields the following formula for this difference

$$a_n(\mathcal{H}) - a_n(C_0) = \frac{1}{hn} \sum_{d|n} N_d \, \mu\Big(\frac{n}{d}\Big) \, |\ker \pi_{n/d}| (1 - H_{\mathcal{C}_0^{n/d}}(C_0)). \qquad (6)$$

Let us agree upon the following notation for the rest of this section:

Notation 51. *$K/\mathbb{F}_q$ is always assumed to be an elliptic function field. $\mathcal{C}_0$ is the group of divisor classes of degree 0 of K and h denotes its order. For an integer m, N_m is the number of prime divisors of degree one of $K\mathbb{F}_{q^m}/\mathbb{F}_{q^m}$ and Π_m is the number of prime divisors of degree m of K; the homomorphism $\pi_m^{\mathcal{C}_0}$ of the last section is simply denoted by π_m.*

n is always a positive integer which satisfies $n \leq 2^{q^{12}}$ (for technical reasons). $\mathrm{P} = \{p_1, \ldots, p_r\}$ is the set of distinct *prime divisors of n; for $0 \leq l \leq r-1$ we set $v_l := p_1 \ldots p_l$ and $u_l := p_{l+1} \ldots p_r$ (note that $v_0 = 1$). If $P \subseteq \mathrm{P}$ we denote by n_P the number $\prod_{q \in P} q$ ($n_\emptyset = 1$). For a non-negative integer i, $\binom{\mathrm{P}}{i}$ denotes the set of subsets of P of order i.*

The following lemma is the heart of the estimates following.

Lemma 19. *Let m be an integer such that $q^m \geq 7$. Further let l be an integer satisfying $0 \leq l \leq r-2$. Then we have*

$$\sum_{k=l+1}^{r} q^{m u_l/p_k} p_k^2 < q^{m(u_l-2)}.$$

Proof. Let us first replace q^m by t. Observe that the function $f(x) = t^{a/x}x^2$ decreases monotonically for $x < a\ln(t)/2$, hence also for $x \leq a$ (note that $t \geq 7$). The proof is divided in two cases:

CASE 1. $l \leq r-3$. In this case $u_l \geq 2 \cdot 3 \cdot 5 = 30$. Further $p_k < u_l/2 < u_l$, hence $t^{u_l/p_k} p_k^2 \leq 4t^{u_l/2}$ by the above observation. So we get

$$\begin{aligned}
\sum_{k=l+1}^{r} t^{u_l/p_k} p_k^2 &\leq 4rt^{u_l/2} \\
&\leq 4\log_2(n) t^{u_l/2} \\
&\leq 4q^{12} t^{u_l/2} \\
&\leq q^{13} t^{u_l/2} \quad (q \geq 7) \\
&\leq t^{u_l-2} \quad (t \geq q, u_l \geq 30).
\end{aligned}$$

CASE 2. $l = r-2$. This condition implies $u_l \geq 2 \cdot 3 = 6$. Hence we get

$$\begin{aligned}
\sum_{k=l+1}^{r} t^{u_l/p_k} p_k^2 &\leq 4t^{u_l/2} + 9t^{u_l/3} \\
&= t^{u_l/2}(4 + 9t^{-u_l/6}) \\
&\leq t^{u_l/2}(4 + \frac{9}{t}) \qquad (u_l \geq 7) \\
&< t^{u_l/2+1} \qquad (t \geq 7) \\
&\leq t^{u_l-2} \qquad (u_l \geq 7). \ \square
\end{aligned}$$

Lemma 20. *Let $q \geq 7$.*

(1) *If $0 \leq l \leq r-2$, we have*

$$-N_{n/v_l} + \sum_{k=l+1}^{r} N_{n/(v_l p_k)} p_k^2 < 0.$$

(2) $-N_{n/v_{r-1}} + N_{n/v_r} p_r^2 < 0$.

Proof. (1) Applying Lemma 13 we get

$$-N_{n/v_l} + \sum_{k=l+1}^{r} N_{n/(v_l p_k)} p_k^2 \leq N_{n/v_r} \Big(-q^{\frac{n}{v_r}(u_l - 2)} + \sum_{k=l+1}^{r} q^{\frac{n u_l}{v_r p_k}} p_k^2 \Big).$$

The right hand side of the inequality is less than zero by Lemma 19.

(2) Let $\mu := v_r$. Then $N_{n/v_{r-1}} = N_{\mu p_r}$. Applying the Hasse-Weil-inequality we obtain

$$\begin{aligned} \frac{N_{\mu p_r}}{N_\mu} &\geq \frac{q^{\mu p_r} + 1 - 2q^{\mu p_r/2}}{q^\mu + 1 + 2q^{\mu/2}} \\ &> \frac{q^{\mu(p_r-1)} - 2q^{\mu(p_r/2-1)}}{1 + q^{-\mu} + 2q^{-\mu/2}} \\ &\geq \frac{2}{3} q^{\mu(p_r/2-1)} (q^{\mu p_r/2} - 2) \qquad (q \geq 7) \\ &\geq \frac{2}{3}(q^{p_r} - 2) \qquad (\mu \geq 2) \\ &\geq p_r^2 \qquad (q \geq 5). \ \square \end{aligned}$$

Lemma 21. *Let $q \geq 7$ and $0 \leq l \leq r-1$. Then*

$$-N_{n/v_l} |\ker \pi_{v_l}| + \sum_{k=l+1}^{r} N_{n/(v_l p_k)} |\ker \pi_{v_l p_k}| < 0.$$

Proof. We have

$$\begin{aligned} &-N_{n/v_l} |\ker \pi_{v_l}| + \sum_{k=l+1}^{r} N_{n/(v_l p_k)} |\ker \pi_{v_l p_k}| = \\ &= |\ker \pi_{v_l}| \Big(-N_{n/v_l} + \sum_{k=l+1}^{r} N_{n/(v_l p_k)} |\ker \pi_{p_k}| \Big) \quad \text{(by Corollary 11)} \\ &\leq |\ker \pi_{v_l}| \Big(-N_{n/v_l} + \sum_{k=l+1}^{r} N_{n/(v_l p_k)} p_k^2 \Big) \quad \text{(by Lemma 16)} \\ &< 0 \quad \text{(by Lemma 20). } \square \end{aligned}$$

Corollary 22. *Let i be an integer satisfying $0 \le i \le r-1$ and $\emptyset \neq \mathcal{P} \subseteq \binom{\mathrm{P}}{i}$ (note that $\mathcal{P} = \{\emptyset\} \neq \emptyset$ if $i = 0$). Then we have*

$$\sum_{P \in \mathcal{P}} \left(-N_{\frac{n}{n_P}} |\ker \pi_{n_P}| + \sum_{\binom{P' \in \binom{\mathrm{P}}{i+1}}{P \subseteq P'}} N_{\frac{n}{n_{P'}}} |\ker \pi_{n_{P'}}| \right) < 0.$$

Proof. Let $P \in \binom{\mathrm{P}}{i}$. Rearranging P if necessary, we can assume that $v_l = n_P$. Further, for every $P' \in \binom{\mathrm{P}}{i+1}$ with $P \subseteq P'$ there exists a unique p_k with $k \ge l+1$ such that $n_{P'} = v_l p_k$. Now the assertion follows from Lemma 21. □

Corollary 23. *Assumptions being as in Lemma 21, let $C_0 \in \mathcal{C}_0$ we have*

$$- \sum_{\binom{P \in \binom{\mathrm{P}}{i}}{H_{\mathcal{C}_0^{n_P}}(C_0)=1}} N_{\frac{n}{n_P}} |\ker \pi_{n_P}| + \sum_{\binom{P' \in \binom{\mathrm{P}}{i+1}}{H_{\mathcal{C}_0^{n_{P'}}}(C_0)=1}} N_{\frac{n}{n_{P'}}} |\ker \pi_{n_{P'}}| \le 0$$

with equality holding if and only if both sums are empty.

Proof. First of all note that by Corollary 12 we have

$$H_{\mathcal{C}_0^{n_{P'}}}(C_0) = 1 \Rightarrow \forall\, P \subseteq P' :\ H_{\mathcal{C}_0^{n_P}}(C_0) = 1.$$

Hence, if the left sum is empty, both sums are empty and so the given term equals 0. If the left sum is not empty and the right sum is empty, the given term is trivially < 0. So assume that the right sum is not empty (which implies that the left sum is non-empty as well). We get

$$\text{Given term} \le \sum_{\binom{P \in \binom{\mathrm{P}}{i}}{H_{\mathcal{C}_0^{n_P}}(C_0)=1}} \left(-N_{\frac{n}{n_P}} |\ker \pi_{n_P}| + \sum_{\binom{P' \in \binom{\mathrm{P}}{i+1}}{P \subseteq P'}} N_{\frac{n}{n_{P'}}} |\ker \pi_{n_{P'}}| \right) < 0$$

by the previous corollary. □

Lemma 24. *For all $1 \le i \le r-1$ we have*

$$\begin{aligned} &- \textstyle\sum_{P \in \binom{\mathrm{P}}{i}} N_{\frac{n}{n_P}} |\ker \pi_{n_P}| (1 - H_{\mathcal{C}_0^{n_P}}(C_0)) \\ &+ \textstyle\sum_{P' \in \binom{\mathrm{P}}{i+1}} N_{\frac{n}{n_{P'}}} |\ker \pi_{n_{P'}}| (1 - H_{\mathcal{C}_0^{n_{P'}}}(C_0)) \le 0 \end{aligned}$$

with equality holding if and only if $C_0 \in \mathcal{C}_0^p$ for all $p|n$.

Proof. Of course the given sum equals 0 if $C_0 \in \mathcal{C}_0^p$ for all $p|n$. So suppose that there exists $p|n$ such that $C_0 \notin \mathcal{C}_0^p$. It follows that for all k there exists $P \in \binom{\mathrm{P}}{k}$ such that $C_0 \notin \mathcal{C}_0^{n_P}$. Let

$$\{P'_1, \ldots, P'_m\} = \{P' \subseteq \mathrm{P} \mid |P'| = i+1, C \notin \mathcal{C}_0^{n_{P'}}\}.$$

So by Corollary 12 there exist pairwise distinct $P_1, \dots, P_k$ such that $|P_l| = i$ for $1 \le l \le k$ and such that each P_l is a subset of at least one of the P'_t, $1 \le t \le m$. Hence the sum in question is less or equal to

$$\sum_{l=1}^{k}(-N_{\frac{n}{n_{P_l}}}|\ker \pi_{n_{P_l}}| + \sum_{\substack{P' \in \binom{\mathrm{P}}{i+1} \\ P_l \subseteq P'}} N_{\frac{n}{n_{P'}}}|\ker \pi_{n_{P'}}|) < 0$$

by Corollary 22. □

Remark 25. Note that the condition $i \ge 1$ is crucial in this proof. It is easily seen that the assertion of Lemma 24 is false for $i = 0$.

Lemma 26. *With the assumptions of Lemma 24 we have*

$$\begin{aligned} &- \sum_{P \in \binom{\mathrm{P}}{i}} N_{\frac{n}{n_P}}|\ker \pi_{n_P}|(1 - H_{\mathcal{C}_0^{n_P}}(C_0)) \\ &+ \sum_{P' \in \binom{\mathrm{P}}{i+1}} N_{\frac{n}{n_{P'}}}|\ker \pi_{n_{P'}}|(1 - H_{\mathcal{C}_0^{n_{P'}}}(C_0)) \\ &\quad \ge -\sum_{P \in \binom{\mathrm{P}}{i}} N_{\frac{n}{n_P}}|\ker \pi_{n_P}| + \sum_{P' \in \binom{\mathrm{P}}{i+1}} N_{\frac{n}{n_{P'}}}|\ker \pi_{n_{P'}}| \end{aligned}$$

with equality holding if and only if $C_0 \notin \mathcal{C}_0^{n_P}$ *for all* $P \in \binom{\mathrm{P}}{i} \cup \binom{\mathrm{P}}{i+1}$.

Proof. The left hand side of the inequality equals

$$\sum_{\substack{P \in \binom{\mathrm{P}}{i} \\ H_{\mathcal{C}_0^{n_P}}(C_0)=0}} N_{\frac{n}{n_P}}|\ker \pi_{n_P}| + \sum_{\substack{P' \in \binom{\mathrm{P}}{i+1} \\ H_{\mathcal{C}_0^{n_{P'}}}(C_0)=0}} N_{\frac{n}{n_{P'}}}|\ker \pi_{n_{P'}}| =: A.$$

By Corollary 23 we have

$$\begin{aligned} A &\ge A - \overbrace{\sum_{\substack{P \in \binom{\mathrm{P}}{i} \\ H_{\mathcal{C}_0^{n_P}}(C_0)=1}} N_{\frac{n}{n_P}}|\ker \pi_{n_P}| + \sum_{\substack{P' \in \binom{\mathrm{P}}{i+1} \\ H_{\mathcal{C}_0^{n_{P'}}}(C_0)=1}} N_{\frac{n}{n_{P'}}}|\ker \pi_{n_{P'}}|}^{} \\ &= -\sum_{P \in \binom{\mathrm{P}}{i}} N_{\frac{n}{n_P}}|\ker \pi_{n_P}| + \sum_{P' \in \binom{\mathrm{P}}{i+1}} N_{\frac{n}{n_{P'}}}|\ker \pi_{n_{P'}}| \end{aligned}$$

with equality holding if and only if the sums under the bracket are empty, i.e., if and only if $C_0 \notin \mathcal{C}_0^{n_P}$ for all $P \in \binom{\mathrm{P}}{i} \cup \binom{\mathrm{P}}{i+1}$. □

Lemma 27. *Assumptions being as above, we have*

$$\sum_{d|n} N_d\,\mu\Big(\frac{n}{d}\Big)\,|\ker \pi_{n/d}|(1-H_{\mathcal{C}_0^{n/d}}(C_0)) \le 0$$

with equality holding if and only if $H_{\mathcal{C}_0^p}(C_0)=1$ *for all* $p|n$.

Proof. The above sum equals

$$\sum_{i=1}^{\lfloor r/2\rfloor}\Big(-\sum_{P\in\binom{\mathrm{P}}{2i-1}} N_{\frac{n}{n_P}}|\ker \pi_{n_P}|(1-H_{\mathcal{C}_0^{n_P}}(C_0)) + \sum_{P\in\binom{\mathrm{P}}{2i}} N_{\frac{n}{n_P}}|\ker \pi_{n_P}|(1-H_{\mathcal{C}_0^{n_P}}(C_0))\Big)-\delta$$

where $\delta = N_{n/v_r}|\ker \pi_{v_r}|(1-H_{\mathcal{C}_0^{n/v_r}})$ if r is odd and $\delta=0$ if r is even. So by Lemma 24

$$\text{Given sum} \le -\delta \le 0$$

with equality if and only if $\delta=0$ and for all $\emptyset \ne P \subseteq \mathrm{P}$ we have $C_0 \in \mathcal{C}_0^{n_P}$, i.e., if and only if $C_0 \in \mathcal{C}_0^p$ for all $p|n$. □

Lemma 28. *Assumptions being as above we have*

$$\sum_{d|n} N_d\,\mu\Big(\frac{n}{d}\Big)\,|\ker \pi_{n/d}|(1-H_{\mathcal{C}_0^{n/d}}(C_0)) \ge \sum_{\binom{d|n}{d<n}} N_d\,\mu\Big(\frac{n}{d}\Big)\,|\ker \pi_{n/d}|$$

with equality holding if and only if $C_0 \notin \mathcal{C}_0^p$ *for all* $p|n$.

Proof. Resolving the sum on the left hand side of the above inequality as in the proof of the preceding lemma and applying Lemma 26 we get

$$\begin{aligned}\text{Given sum} &\ge \sum_{i=1}^{\lfloor r/2\rfloor}\Big(-\sum_{\binom{P}{|P|=2i-1}} N_{\frac{n}{n_P}}|\ker \pi_{n_P}| + \sum_{\binom{P}{|P|=2i-1}} N_{\frac{n}{n_P}}|\ker \pi_{n_P}|\Big)-\delta\\ &= \sum_{\binom{d|n}{d<n}} N_d\,\mu\Big(\frac{n}{d}\Big)\,|\ker \pi_{n/d}|\end{aligned}$$

with equality holding if and only if

$$\forall\,\emptyset \ne P \subseteq \mathrm{P}: \quad C_0 \notin \mathcal{C}_0^{n_P} \iff C_0 \notin \mathcal{C}_0^p \text{ for all } p|n.\ \square$$

Now we are able to prove Theorem 17:

Proof. (Of Theorem 17) (1) and (2) follow from Lemma 27 and Equation (6), (3) follows from Lemma 28, Equation (6) and Theorem 6. □

Remark 29. The assertion of Theorem 17 can be extended to $q = 4, 5$ by more careful estimations.

With the tools developed in this section we are able to prove several properties of the function a_n. The next two theorems serve as examples in this direction.

Theorem 30. *Notation and conditions being as in 12 we have* $a_n(C_0) > 0$.

Proof. In view of Theorem 17 it suffices to show that $a_n(\mathcal{H}) > 0$ for the principal class $\mathcal{H}$ of K. Now

$$a_n(\mathcal{H}) = \frac{1}{hn} \sum_{d|n} N_d \, \mu\Big(\frac{n}{d}\Big) \, |\ker \pi_{n/d}|.$$

The above sum equals

$$\frac{1}{hn} \sum_{i=0}^{\lfloor (r-1)/2 \rfloor} \Big(\sum_{P \in \binom{\mathrm{P}}{2i}} N_{\frac{n}{nP}} |\ker \pi_{nP}| - \sum_{P \in \binom{\mathrm{P}}{2i+1}} N_{\frac{n}{nP}} |\ker \pi_{nP}| \Big) + \frac{1}{hn} \delta'$$

where $\delta' = 0$ if r is odd and $\delta' = N_{n/v_r} |\ker \pi_{v_r}|$ if r is even. But

$$\sum_{P \in \binom{\mathrm{P}}{2i}} N_{\frac{n}{nP}} |\ker \pi_{nP}| - \sum_{P \in \binom{\mathrm{P}}{2i+1}} N_{\frac{n}{nP}} |\ker \pi_{nP}|$$

is greater than zero by Lemma 24 (if $i > 0$) and Lemma 22 (if $i = 0$). □

Remark 31. The above theorem states in other words that under the conditions stated the mapping tr defined in the introduction is surjective.

The following example shows that the assertion of Theorem 30 need not be true for $q \leq 5$:

Example 32. We consider again the elliptic function field

$$K = \mathbb{F}_4(x, y), \quad y^2 + y = x^3 + 1.$$

Let $n = 3$ and $\mathcal{H}$ be the principal class of K. An easy computation shows that $N_3 = 24$. Application of Theorem 6 yields

$$a_3(\mathcal{H}) = \frac{1}{9}\Big(24 - \frac{1}{3} \cdot 9 \cdot 8\Big) = 0.$$

The next theorem is a partial converse to Lemma 7.

Theorem 33. *Notation and conditions being as in 12 we have:* $a_n(C_0) = \Pi_n/h$ *for all* $C_0 \in \mathcal{C}_0$ *if and only if* $\gcd(n,h) = 1$.

Proof. In view of Lemma 7 we have to prove that for $\gcd(n,h) \neq 1$ there exists a class $C_0 \in \mathcal{C}_0$ such that $a_n(C_0) \neq a_n(\mathcal{H})$ where $\mathcal{H}$ is as usual the principal class of K. Now if $\gcd(n,h) \neq 1$, there exists a prime number p such that $p|\gcd(n,h)$. Hence there exists a class $C_0 \notin \mathcal{C}_0^p$. Lemma 27 implies now $a_n(\mathcal{H}) - a_n(C_0) < 0$. □

Example 8 shows that the assertion of Theorem 33 need not be true for $q \leq 5$.

6 An Optimal Algorithm for Multiplication in $\mathbb{F}_{27}/\mathbb{F}_3$

This section gives an application of the results of this paper to the problem of determining optimal bilinear multiplication algorithms for finite extensions of finite fields. For a background on the bilinear complexity theory, we refer the reader to [2, Chap. 14].

A bilinear algorithm of length r for the multiplication in a finite dimensional k-algebra A consists of r triples (f_i, g_i, w_i) where f_i and g_i are k-linear forms on the vector space A, and $w_i \in A$, such that

$$\forall a, b \in A: \quad a \cdot b = \sum_{i=1}^{r} f_i(a) g_i(b) w_i.$$

($a \cdot b$ is the product of a and b in A.) The aim is to obtain for an algebra A a bilinear algorithm of minimal length.

As an example, consider the algebra $A := k[x]/(x^2 - a)$, for some $a \in k$. A basis for this algebra is given by $(1, x)$, where we identify polynomials with their residue classes modulo $x^2 - a$. The naive way of multiplying elements in this algebra is by implementing the following formula:

$$(A + Bx)(C + Dx) = (AC + aBD) + (AD + BC)x.$$

Let $f_1(\alpha + \beta x) = g_1(\alpha + \beta x) = \alpha$, $f_2(\alpha + \beta x) = g_2(\alpha + \beta x) = \beta$, $w_1 := 1$, $w_2 := x$, and $w_3 := a$. Then, it is easily verified that

$$(f_1, g_1, w_1), (f_1, g_2, w_2), (f_2, g_1, w_2), (f_2, g_2, w_3)$$

is a bilinear computation for A of length 4. Another, more efficient algorithm is derived from

$$(A + Bx)(C + Dx) = (AB + aBD) + ((A + B)(C + D) - AC - BD)x$$

which gives rise to a bilinear algorithm of length 3: let f_i, g_i, $i = 1, 2$ be as above, and let $f_3(\alpha + \beta x) = g_3(\alpha + \beta x) := \alpha + \beta$. Further, let $w_1 := 1 - x$, $w_2 := a - x$, and $w_3 := x$. Then

$$(f_1, g_1, w_1), (f_2, g_2, w_2), (f_3, g_3, w_3)$$

is a bilinear computation for A of length 3.

The bilinear complexity does not measure the number of additions/subtractions, or scalar multiplications. (This is expressed by the fact that the additions and scalar multiplications necessary for evaluating f_i and g_i are not counted.) However, for many important problems like the matrix multiplication, the asymptotic complexity can be measured in terms of the bilinear complexity only [2, Chap. 15]. Furthermore, in some situations, using bilinear algorithms recursively leads to overall savings in the running time. For instance, the Toom-Karatsuba method of multiplication [7, Chap. 4.3.3] can be seen as recursively using the multiplication algorithm of length 3 in the algebra A above (for suitable A).

An important class of k-algebras are simple field extensions. Multiplication in these algebras can be reduced to polynomial multiplication, which in turn can be accomplished using Lagrange interpolation. One can prove that if $|k| \geq 2n - 2$, then the bilinear complexity of multiplication in a simple field extension of degree n over k is exactly $2n - 1$, and that it is larger than $2n - 1$ otherwise [2, Th. 17.29 and Rem. 17.30].

In [4] the authors describe an algorithm for multiplication in extensions of small finite fields, i.e., in extensions of degree n of a finite field k with $|k| < 2n - 2$. In a nutshell, Goppa's idea is used to replace the Lagrange interpolation by interpolation on algebraic curves. The algorithm was slightly modified in [10] for elliptic curves. In particular, it was proved there that the bilinear complexity of multiplication in $\mathbb{F}_{q^n}$ is $2n$ if $\frac{1}{2}q + 1 < n < \frac{1}{2}m(q)$ where $m(q)$ is the maximum number of points of an elliptic curve over $\mathbb{F}_q$. In a subsequent work [9], it was described how to obtain these algorithms using arithmetic properties of elliptic curves.

In this section, we apply by way of an example some of the results of this paper to obtain an optimal algorithm for multiplication in the field extension $\mathbb{F}_{27}$ of $\mathbb{F}_3$. Note that this case is not covered by [9]. The similar case of $\mathbb{F}_{256}/\mathbb{F}_4$ was solved in [2].

For the following computations we present $\mathbb{F}_3$ as $\mathbb{F}_3 = \{0, 1, 2\}$. We assume familiarity with [9].

In order to compute the optimal algorithm we are looking for, we follow [9, Algorithm IV–B] with minor modifications. In particular, we will compute two matrices $A \in \mathbb{F}_3^{3\times 6}$ and $B \in \mathbb{F}_3^{6\times 3}$ and a basis (f_0, f_1, f_2) of $\mathbb{F}_{27}/\mathbb{F}_3$ with the following properties: the multiplication of $x_0 f_0 + x_1 f_1 + x_2 f_2$ and $y_0 f_0 + y_1 f_1 + y_2 f_2$ is given as $z_0 f_0 + z_1 f_1 + z_2 f_2$ where

$$(z_0, z_1, z_2) = (X_0 Y_0, \ldots, X_5 Y_5) B,$$

and

$$\begin{pmatrix} X_0 \dots X_5 \\ Y_0 \dots Y_5 \end{pmatrix} = \begin{pmatrix} x_0, x_1, x_2 \\ y_0, y_1, y_2 \end{pmatrix} A.$$

Hence, A and B completely determine the multiplication in $\mathbb{F}_{27}$.

To obtain these two matrices, we first compute an elliptic curve E over $\mathbb{F}_3$ having 7 $\mathbb{F}_3$-rational and compute its set of points $E(\mathbb{F}_3)$. Next we determine prime divisors $\mathfrak{D}$ and $\mathfrak{p}$, both of degree 3, such that $L(\mathfrak{D} - \mathfrak{p}) = 0$, where by $L(A)$ we denote the linear space of the divisor A. Notice that this is equivalent to requiring $[\mathfrak{D}] \neq [\mathfrak{p}]$, where $[A]$ denotes the class of the divisor A. Afterwards we compute a basis $\{f_1, \dots, f_6\}$ of $L(2\mathfrak{D})$ such that $\{f_1, f_2, f_3\}$ is a basis of $L(\mathfrak{D})$. In order to compute the matrices Γ and A of Step (v) of [9, Algorithm IV–B], we first need to compute a set of points $P_1, \dots, P_6$ of $E(\mathbb{F}_3)$ such that

$$[P_1 \oplus \cdots \oplus P_6 - Q] \neq [\mathfrak{D} - 3Q]$$

where Q is the neutral element of $E(\mathbb{F}_3)$. Next we perform Steps (vi) and (vii) of [9, Algorithm IV–B] to obtain the matrices A and B which are the final outputs.

It is easily verified that the curve $E : y^2 = x^3 - x + 1$ has 7 $\mathbb{F}_3$-rational points and $E(\mathbb{F}_3) = \{Q, P_1, \dots, P_6\}$, where

$$P_1 := (0, 2), P_2 := (0, 1), P_3 := (1, 2),$$
$$P_4 := (1, 1), P_5 := (2, 2), P_6 := (2, 1).$$

For the sake of simplicity we choose for $\mathfrak{D}$ a prime divisor of degree 3. The representation of prime divisors is the same as described in [9, Section 3.6], i.e., a prime divisor is given by (g, h) where g is an irreducible polynomial of degree 3 and h is a polynomial of degree at most 2 such that $h^2 \equiv x^3 - x + 1 \bmod g$. We use [9, Algorithm III–F] to compute two random prime divisors $\mathfrak{D}$ and $\mathfrak{p}$. This is the place where we use the results of this paper. Namely, for a random choice of $\mathfrak{D}$ and $\mathfrak{p}$, the probability that they belong to the same divisor class is $\frac{1}{7}$ by Theorem 33. Hence, with high probability, we will pick two prime divisors that do not belong to the same class. In fact, after one guess we obtain

$$\mathfrak{D} = (x^3 + 2x^2 + 2x + 2, 2x^2 + x), \qquad \mathfrak{p} = (x^3 + 2x^2 + 1, 2x^2 + 2x).$$

The class finding algorithm [9, Algorithm III–E] gives

$$[\mathfrak{D} - 3Q] = [P_5 - Q], \qquad [\mathfrak{p} - 3Q] = [P_3 - Q], \tag{7}$$

which shows that $\mathfrak{D}$ and $\mathfrak{p}$ belong to different classes. The function $(x + 1)$ has the divisor $P_5 + P_6 - 2Q$. Hence (7) implies that $\mathfrak{D} + P_6 - 4Q$ is a principal divisor, i.e., the divisor of a function, say u. Observe first that $u \in L(4Q)$. Since $1, x, y, x^2$ is a basis of $L(4Q)$, u is a linear combination of these functions. Further, $\mathrm{ord}_Q(u) = -4$, hence w.l.o.g. we may assume

that $u = x^2 + ax + by + c$ with some constants $a, b, c \in \mathbb{F}_3$. Now $u(\mathfrak{D}) = 0$, hence computing with x as $X \bmod (X^3 + 2X^2 + 2X + 2)$ and with y as $(2X^2 + X) \bmod (X^3 + 2X^2 + 2X + 2)$, we obtain

$$(1 + 2b)X^2 + (a + b)X + C = 0.$$

This gives $u = x^2 + 2x + y$. We claim that

$$\mathsf{B} := \left\{1, \frac{x+1}{u}, \frac{(x+1)^2}{u}, \frac{(x+1)^2}{u^2}, \frac{(x+1)^3}{u^2}, \frac{(x+1)^4}{u^2}\right\}$$

is a basis of $L(2\mathfrak{D})$ and that the first three elements of B form a basis of $L(\mathfrak{D})$: first, $\mathsf{B} \subset L(2\mathfrak{D})$ and the first three elements of B belong to $L(\mathfrak{D})$ (simply compute their divisors!). In order to prove linear independence, we evaluate the representation matrix of the linear morphism

$$\begin{aligned} \gamma\colon \langle \mathsf{B} \rangle &\to \mathbb{F}_3^6 \\ v &\mapsto (v(P_1), \ldots, v(P_6)). \end{aligned}$$

We will show that $\mathrm{rk}\,(\gamma) = 6$, which implies that B is a basis of $L(2\mathfrak{D})$. For this, it is sufficient to show that

$$\Gamma := (v(P_i))_{v \in \mathsf{B}, 1 \le i \le 6}$$

has full rank. First, we have to explain how to evaluate the function in B at the point P_6, since $u(P_6) = 0$. Observe that

$$\mathrm{ord}_{P_6}((x+1)^2/u), \mathrm{ord}_{P_6}((x+1)^3/u^2), \mathrm{ord}_{P_6}((x+1)^4/u^2) \ge 1,$$

which implies that these functions vanish at P_6. Setting $v := (x+1)/u$, we thus have to compute $v(P_6)$. Note that $t := (x+1)$ is a local parameter for P_6, i.e., $\mathrm{ord}_{P_6}(t) = 1$. We obtain the following power series expansion for v in $\mathbb{F}_3[[t]]$:

$$v = \frac{t}{t^2 + 2 + \sqrt{t^3 + 2t + 1}} = 1 + t + 2t^2 + \cdots.$$

Hence $v(P_6)$ (which equals the constant term of $v \in \mathbb{F}_3[[t]]$) is 1. Thus,

$$\Gamma = \begin{pmatrix} 1&1&1&1&1&1 \\ 2&1&1&2&0&1 \\ 2&1&2&1&0&0 \\ 1&1&1&1&0&1 \\ 1&1&2&2&0&0 \\ 1&1&1&1&0&0 \end{pmatrix}.$$

It is easily seen that Γ is invertible. Hence B is a basis of $L(2\mathfrak{D})$.

Let us denote the elements of the basis B by $v_1 \ldots, v_6$ (in the order given above). We first compute a matrix T such that

$$\begin{pmatrix} v_1 \bmod \mathfrak{p} \\ \vdots \\ v_6 \bmod \mathfrak{p} \end{pmatrix} = T \begin{pmatrix} 1 \\ x \\ x^2 \end{pmatrix} \bmod (x^3 + 2x^2 + 1).$$

Now $u \bmod \mathfrak{p} = x \bmod (x^3 + 2x^2 + 1)$, hence $1/u \bmod \mathfrak{p} = 2x^2 + x \bmod (x^3 + 2x^2 + 1)$. Hence,

$$T = \begin{pmatrix} 1\,0\,0 \\ 1\,1\,2 \\ 2\,2\,2 \\ 2\,1\,1 \\ 1\,0\,0 \\ 1\,1\,0 \end{pmatrix}.$$

Let T' be the matrix consisting of the first three rows of T. As is shown in [9, Section 4.4] T' is non-singular and $C = T(T')^{-1}$. Further, $B = \Gamma^{-1}C$. This yields

$$B = \begin{pmatrix} 2\,2\,1 \\ 0\,2\,1 \\ 1\,2\,2 \\ 0\,2\,0 \\ 0\,0\,1 \\ 1\,1\,1 \end{pmatrix}.$$

Finally, the matrix A is given by the first three rows of Γ, i.e.,

$$A = \begin{pmatrix} 1\,1\,1\,1\,1\,1 \\ 2\,1\,1\,2\,0\,1 \\ 2\,1\,2\,1\,0\,0 \end{pmatrix}.$$

The multiplication algorithm is thus as follows: to compute the product of (x_0, x_1, x_2) and (y_0, y_1, y_2), first compute

$$\begin{array}{lll} X_0 := x_0 + 2x_1 + 2x_2 & X_1 := x_0 + x_1 + x_2 & X_2 := x_0 + x_1 + 2x_2 \\ X_3 := x_0 + 2x_1 + x_2 & X_4 := x_0 & X_5 := x_0 + x_1 \\ Y_0 := y_0 + 2y_1 + 2y_2 & Y_1 := y_0 + y_1 + y_2 & Y_2 := y_0 + y_1 + 2y_2 \\ Y_3 := y_0 + 2y_1 + y_2 & Y_4 := y_0 & Y_5 := y_0 + y_1. \end{array}$$

The product is given by (z_0, z_1, z_2), where

$$\begin{aligned} z_0 &:= 2X_0Y_0 + X_2Y_2 + X_5Y_5, \\ z_1 &:= 2X_0Y_0 + 2X_1Y_1 + 2X_2Y_2 + 2X_3Y_3 + X_5Y_5, \\ z_2 &:= X_0Y_0 + X_1Y_1 + 2X_2Y_2 + X_4Y_4 + X_5Y_5. \end{aligned}$$

Acknowledgement

The research on this paper was done while the author was visiting the department of mathematics of the university of Brasília. The author wants to thank the GMD for a travel grant, the FINEP for financial support, the department of mathematics of the university of Brasília, especially Prof. S. Shokranian, for their hospitality during his visit in Brasília.

References

1. T.M. Apostol. **Introduction to Analytic Number Theory**. Undergraduate Texts in Mathematics. Springer Verlag, 1979.
2. U. Baum and M.A. Shokrollahi. An optimal algorithm for multiplication in $\mathbb{F}_{256}/\mathbb{F}_4$. *AAECC*, 2:15–20, 1991.
3. P. Bürgisser, M. Clausen, and M.A. Shokrollahi. **Algebraic Complexity Theory**, volume 315 of *Grundlehren der Mathematischen Wissenschaften*. Springer Verlag, Heidelberg, 1996.
4. D.V. Chudnovsky and G.V. Chudnovsky. Algebraic complexity and algebraic curves over finite fields. *J. Compl.*, 4:285–316, 1988.
5. M. Deuring. **Lectures on the Theory of Algebraic Functions of One Variable**, volume 314 of *Lecture Notes in Mathematics*. Springer Verlag, 1973.
6. H. Hasse. **Vorlesungen über Klassenkörpertheorie**. Physica-Verlag, Würzburg, 1967.
7. D.E. Knuth. **The Art of Computer Programming**, volume 2: seminumerical algorithms. Addison-Wesley, 1981.
8. H. G. Rück. A note on elliptic curves over finite fields. *Math. Comp.*, 49:301–304, 1987.
9. M.A. Shokrollahi. Efficient randomized generation of algorithms for multiplication in certain finite fields. *Comp. Compl.*, 2:67–96, 1992.
10. M.A. Shokrollahi. Optimal algorithms for multiplication in certain finite fields using elliptic curves. *SIAM J. Comp.*, 21:1193–1198, 1992.