On Multiplication in Finite Fields

F. Özbudak, Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey

Joint work with M. Cenk

Let $\mathbb{F}_q$ be a finite field and $n > 1$ be an integer. Let $\mathbb{F}_{q^n}^{\perp}$ be dual of $\mathbb{F}_{q^n}$ as a vector space over $\mathbb{F}_q$. Then the rank $R(\mathbb{F}_{q^n}/\mathbb{F}_q)$ over $\mathbb{F}_q$ is defined to be

$$R(\mathbb{F}_{q^n}/\mathbb{F}_q) = min\left\{ \ell \in \mathbb{N} \;\middle|\; \exists u_i, v_i \in \mathbb{F}_{q^n}^{\perp}, w_i \in \mathbb{F}_{q^n} \text{ such that } \forall a, b \in \mathbb{F}_{q^n}, ab = \sum_{i=1}^{\ell} u_i(a)v_i(b)w_i \right\}.$$

$R(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is also denoted by $\mu_q(n)$ and it is called *the bilinear complexity of multiplication in* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$. It corresponds to the minimum number of $\mathbb{F}_q$ multiplications in order to multiply two arbitrary elements of $\mathbb{F}_{q^n}$. Winograd [15] showed that this complexity is $\geq 2n-1$ and it is equal to $2n-1$ if and only if $n \leq \frac{1}{2}q+1$. Algorithms obtaining the lower bound are based on interpolation algorithms on the rational function field [15]. D. V. Chudnovsky and G. V. Chudnovsky [6] generalized this idea to algebraic function fields (of one variable) over $\mathbb{F}_q$. Shokrollahi [11] obtained optimal algorithms for the multiplication in certain finite fields using the principle of D. V. and G. V. Chudnovsky algorithm and the elliptic curves. Shparlinski, Tsfasman and Vladut [12] gave the asymptotic bounds for multiplication in finite fields by using curves with many points. Ballet [1],[2] generalized Shokrollahi's work to the algebraic function fields of genus g. Ballet and Rolland [3] gave a generalization of D. V. Chudnovsky and G. V. Chudnovsky multiplication algorithm by interpolating not only degree one places but also interpolating on degree two places. In [4], new upper bounds of the bilinear complexity of multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ are obtained by proving the existence of certain types of non-special divisors of $g-1$ in the algebraic function fields of genus g defined over $\mathbb{F}_q$.

There is a related but different complexity notion. Let $M_q(n)$ denote the number of multiplications needed in $\mathbb{F}_q$ in order to multiply two arbitrary n-term polynomials in $\mathbb{F}_q[x]$ (cf. [15], [14], [13], [8], [7], [5]). Here a polynomial is called an n-term polynomial in $\mathbb{F}_q[x]$ if it is of the form

$$a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathbb{F}_q[x].$$

As reduction modulo an irreducible polynomial in $\mathbb{F}_q[x]$ can be performed without multiplications in $\mathbb{F}_q$, we have

$$\mu_q(n) \leq M_q(n). \tag{1}$$

However $\mu_q(n)$ and $M_q(n)$ are not necessarily equal in general. Using a polynomial basis $\{1, \xi, \xi^2, \ldots, \xi^{n-1}, \ldots, \xi^{2n-2}\}$ for $\mathbb{F}_{q^{2n-1}}$ over $\mathbb{F}_q$, it is easy to show that

$$M_q(n) \leq \mu_q(2n-1).$$

In this extended abstract we present a new method for multiplication in finite fields improving $\mu_q(n)$ for certain values of q and n. We use local expansions, the length of which is a further parameter that can be used to optimize the bounds on the bilinear complexity, instead of evaluation into residue class field. Our basic principle is still based on the method of D. V. Chudnovsky and G. V. Chudnovsky. The main idea in the new method can be summarized as follows. We use algebraic function fields of one variable with places of arbitrary degrees and moreover we use some places not only once but also many times. Here many times refers to using first $u_i > 1$ coefficients instead of the first ($u_i = 1$) coefficient in the local expansion of a place P_i (see the map φ below).

Before stating our results we need to introduce another complexity notion. For a positive integer ℓ, let $\widehat{M}_q(\ell)$ denote the minimum number of multiplications needed in $\mathbb{F}_q$ in order to obtain the first ℓ coefficients of the product of two arbitrary ℓ-term polynomials in $\mathbb{F}_q[x]$. It is not difficult to obtain useful upper bounds on $\widehat{M}_q(\ell)$ for certain values ℓ. For example we have $\widehat{M}_q(2) \leq 3$, $\widehat{M}_q(3) \leq 5$, $\widehat{M}_q(4) \leq 8$ and $\widehat{M}_q(5) \leq 11$ for any prime power q (cf. [5, Proposition 1]).

Let $F/\mathbb{F}_q$ be an algebraic function field with full constant field $\mathbb{F}_q$. Let $P_1, P_2, \ldots, P_N$ be distinct places of arbitrary degrees. Assume that Q is a place of degree n. Let $\mathcal{O}_Q$ be the valuation ring of the place Q. Note that the residue field $\mathcal{O}_Q/Q$ is isomorphic to $\mathbb{F}_{q^n}$. Let D be a divisor such that $\mathrm{supp}D \cap \{Q, P_1, P_2, \ldots, P_N\} = \emptyset$. Let $\mathcal{L}(D)$ be the Riemann-Roch space of D. Assume also that the evaluation map Ev_Q from $\mathcal{L}(D)$ into the residue field $\mathcal{O}_Q/Q$ is onto. For $1 \le i \le N$, let t_i be a local parameter at P_i. For $f \in \mathcal{L}(2D)$, let

$$f = \alpha_{i,0} + \alpha_{i,1} t_i + \alpha_{i,2} t_i^2 + \cdots$$

be the local expansion at P_i with respect to t_i, where $\alpha_{i,0}, \alpha_{i,1}, \ldots \in \mathbb{F}_{q^{\deg(P_i)}}$. Let u_i be a positive integer and consider the $\mathbb{F}_q$-linear map

$$\begin{array}{rcl} \varphi_i : \mathcal{L}(2D) & \to & \left(\mathbb{F}_{q^{\deg(P_i)}}\right)^{u_i} \\ f & \mapsto & (\alpha_{i,0}, \alpha_{i,1}, \ldots, \alpha_{i,u_i-1}) . \end{array}$$

Let φ be the $\mathbb{F}_q$-linear map given by

$$\begin{array}{rcl} \varphi : \mathcal{L}(2D) & \to & \left(\mathbb{F}_{q^{\deg(P_1)}}\right)^{u_1} \times \left(\mathbb{F}_{q^{\deg(P_2)}}\right)^{u_2} \times \cdots \times \left(\mathbb{F}_{q^{\deg(P_N)}}\right)^{u_N} \\ f & \mapsto & (\varphi_1(f), \varphi_2(f), \ldots, \varphi_N(f)) . \end{array}$$

Finally we assume that the map φ is injective.

Theorem 1. *Under the notation and assumptions as above we have*

$$\mu_q(n) \le \sum_{i=1}^{N} \mu_q(\deg(P_i)) \widehat{M}_{q^{\deg(P_i)}}(u_i).$$

Using Theorem 1 we obtain explicit algorithms for multiplications in $\mathbb{F}_{q^n}$. The conditions of the following theorem guarantee that the assumptions of Theorem 1 are satisfied.

Theorem 2. *Let $F/\mathbb{F}_q$ be an algebraic function field with full constant field $\mathbb{F}_q$. Let g be the genus of F. Let $P_1, P_2, \ldots, P_N$ be distinct places of arbitrary degrees of F. Let $u_1, u_2, \ldots, u_N$ be arbitrary positive integers. Assume that*

(1) *there exists a non-special divisor of degree $g-1$,*
(2) *there exists a place of degree n,*
(3) *$\sum_{i=1}^{n} \deg(P_i) u_i \ge 2n + g - 1$.*

Then we have

$$\mu_q(n) \le \sum_{i=1}^{N} \mu_q(\deg(P_i)) \widehat{M}_{q^{\deg(P_i)}}(u_i).$$

Remark 1. *Under the notation and assumptions of Theorem 2, consider the subcase that $N = N_1 + N_2$, P_i is a degree one place for $1 \le i \le N_1$, P_i is a degree two place for $N_1 + 1 \le i \le N_1 + N_2$. Moreover let $u_i = 1$ for $1 \le i \le N_1 + N_2$. Note that $\mu_q(1) = 1$, $\mu_q(2) \le 3$, and $\widehat{M}_{q^{\deg(P_i)}}(1) = 1$ for any $\deg(P_i)$. Therefore the condition (3) of Theorem 2 becomes*

$$N_1 + 2N_2 \ge 2n + g - 1,$$

and the bound of Theorem 2 on $\mu_q(n)$ becomes

$$\mu_q(n) \le N_1 + 3N_2.$$

These coincide with the corresponding result of [3] *(see also* [4, Theorem 1.1]*).*

Remark. *By Theorem 2, in order to obtain better upper bounds on $\mu_q(n)$, we need algebraic function fields with full constant field $\mathbb{F}_q$, with small genus g, and with enough number of rational places of suitable degrees. It is well known that finding algebraic function fields over $\mathbb{F}_q$ with fixed small genus g and many rational places is not easy (cf.* [10, Chapter 4]*). In Theorem 2, as $\deg(P_i)$ and u_i are further parameters to be chosen, the condition (3) is weaker than the corresponding condition in* [3, Theorem 2.2] *(see also* [4, Theorem 2.1]*). Therefore we obtain improved bounds on $\mu_q(n)$ using Theorem 2. We also illustrate our improvements by an example below.*

Using $u = 2$ for degree one places and $u = 1$ for degree two places in Theorem 2, we obtain the following corollary.

Corollary 1. *Let $F/\mathbb{F}_q$ be an algebraic function field with full constant field $\mathbb{F}_q$. Let g be the genus of F. Assume there exist at least N_1 degree one and at least N_2 degree two places of F. If*

(1) *there exists a non-special divisor of degree $g-1$,*
(2) *there exists a place of degree n,*
(3) $2N_1 + 2N_2 \geq 2n + g - 1$,

then we have

$$\mu_q(n) \leq 3n + 3\left\lceil \frac{g-1}{2} \right\rceil.$$

We compare Corollary 1 with the corresponding results in [3] and [4]. The bound of Corollary 1 is at least as good as the bounds of [3, Theorem 2.2] and [4, Theorem 2.1]. The condition (3) of Corollary 2 is weaker as the corresponding condition of [3] and [4] is $N_1 + 2N_2 \geq 2n + g - 1$. The other conditions of Corollary 1 are the same as the ones in [3] and [4]. Therefore Corollary 1 gives improved bounds on $\mu_q(n)$.

Example 1. *Let $q = 3$ and $n = 9$. Using the results in the literature, to the best of our knowledge, the best upper bound is $\mu_3(9) \leq 27$, which can be derived by two alternative methods as follows. Using* [14], [8], *and* [5], *we obtain the upper bounds on $M_3(9)$ as* 36, 34 *and* 27, *respectively. Hence by* [5] *and (1) we get $\mu_3(9) \leq 27$. For the method in* [3], *we have considered all algebraic function fields of genus* 0 *and* 1. *Let E be elliptic curve $y^2 = x^3 + x + 2$ over $\mathbb{F}_3$. It has* 4 *degree one places,* 6 *degree two places and* 8 *degree three places. As $4 + 2 \cdot 6 < 2 \cdot 9 + 1 - 1$, the method of* [3] *cannot be applied directly. Using* 3 *degree one places,* 6 *degree two places, and* 1 *degree three places, all with $u = 1$ as in* [3], *we obtain that $\mu_3(9) \leq 3 \cdot 1 + 6 \cdot 3 + 6 \cdot 1 = 27$. Now we improve this to $\mu_3(9) \leq 26$ using Theorem 2 together with $u = 2$ for some places. We take* 2 *degree one places with $u = 2$,* 2 *degree one places with $u = 1$, and* 6 *degree two places with $u = 1$. Therefore we obtain that $\mu_3(9) \leq 2 \cdot 3 + 2 \cdot 1 + 6 \cdot 3 = 26$. We also find an explicit formula of such an algorithm via Theorem 1, which can be found in* `http://www.metu.edu.tr/~ozbudak/formula3-9.pdf` .

Finite field multiplication is widely used in many areas such as cryptography and coding theory. For example, in elliptic curve cryptography finite fields of large number of elements are used. Some of suitable finite fields are proposed by NIST (National Institute of Standards and Technology) [9]. In that list it is suggested to use the field with 2^{163} elements. Now we will compute the complexity for multiplication in $\mathbb{F}_{2^{163}}$ using proposed method. The most suitable elliptic curve for our method over $\mathbb{F}_2$ (up to isomorphism) is $y^2 + y = x^3 + x + 1$ which has 1 degree one places, 2 degree two places, 4 degree three places, 5 degree four places, 8 degree five places, 8 degree six places, 16 degree seven places and 25 degree eight places. We take 1 degree one places with $u = 5$, 2 degree two places with $u = 2$, 4 degree three places with $u = 1$, 5 degree four places with $u = 1$, 8 degree five places with $u = 1$, 8 degree six places with $u = 1$, 15 degree seven places with $u = 1$ and 11 degree eight places with $u = 1$. Therefore we obtain

$$\mu_2(163) \leq 11 + 2 \cdot 9 + 5 \cdot 9 + 8 \cdot 13 + 8 \cdot 15 + 15 \cdot 22 + 12 \cdot 24 = 916,$$

where we take $\widehat{M}_2(5) \leq 11$, $\widehat{M}_4(2) \leq 3$ [5] and $\mu_2(4) \leq 9$, $\mu_2(5) \leq 13$, $\mu_2(6) \leq 15$, $\mu_2(7) \leq 22$ and $\mu_2(8) \leq 24$. In the full paper, how the latter bounds are obtained will be explained in detail. On the other hand, the best we can expect from Karatsuba algorithm (together with (1)) is $\mu_2(163) \leq N$, where N is an integer with $N > 2187$, since it is given in [14] that $M_2(128) \leq 2187$.

Acknowledgments. The authors would like to thank the anonymous referees for their useful suggestions. This work was supported by TÜBİTAK under Grant No. TBAG-107T826.

References

[1] S. Ballet, *Curves with many points and multiplication complexity in any extension of $\mathbb{F}_q$*, Finite Fields Their Appl. 5, 1999, 364 - 377.
[2] S. Ballet, *Quasi-optimal algorithms for multiplication in the extension of degree 13, 14, and 15*, J. Pure Appl. Algebra, 171, 2002, 149 -164.
[3] S. Ballet, R. Rolland, *Multiplication algorithm in a finite field and tensor rank of the multiplication*, J. Algebra 272/1, 2004, 173 - 185.

[4] S. Ballet, *On the tensor rank of the multiplication in the finite fields*, J. Number Theory (2007), in press, available at doi:10.1016/j.jnt.2007.06.010
[5] M. Cenk, F. Özbudak, *Efficient multiplication in* $\mathbb{F}_{3^{\ell m}}$, $m \geq 1$ *and* $5 \leq \ell \leq 18$, in Africacrypt 2008 volume 5023 of Lecture Notes in Computer Science, Springer - Verlag, in press.
[6] D.V. Chudnovsky, G.V. Chudnovsky, *Algebraic complexities and algebraic curves over finite fields*, J. Complexirty 4 1988, 285 - 316.
[7] H. Fan and M. Anwar Hasan, *Comments on "Five, Six, and Seven-Term Karatsuba-Like Formulae"*, IEEE Transactions on Computers, vol. 56, no. 5, pp. 716-717, 2007.
[8] P. L. Montgomery, *Five, six, and seven-term Karatsuba-like formulae*, IEEE Transactions on Computers, 54(3), 362-369, March 2005.
[9] National Institute of Standards and Technology, Digital Signature Standard, FIPS Publication 186-2, February 2000.
[10] H. Niederreiter and C. Xing, *Rational Points on Curves over Finite Fields: Theory and Applications*, Cambridge University Press, Cambridge, UK, 2001.
[11] M. A. Shokrollahi, *Optimal algortihms for multiplication in certain finite fields using algebraic curves*, SIAM J. Comput., 21 (6), 1992, 1193 - 1198.
[12] I.E. Shparlinski, M. A. Tsfasman, S.G. Vladut, *Curves with many points and multiplication in finite fields*, Lecture Notes in Mathematics, Vol. 1518, Springer, Berlin, 1992, pp. 145 - 169.
[13] B. Sunar, *A generalized method for constructing subquadratic complexity* $GF(2^k)$ *multipliers*, IEEE Transactions on Computers, vol. 53, no. 9, pp. 1097-1105, 2004.
[14] A. Weimerskirch and C. Paar, *Generalizations of the Karatsuba algorithm for polynomial multiplication*, Technical Report, Ruhr-Universität Bochum, Germany, 2003.
`http://www.crypto.ruhr-uni-bochum.de/imperia/md/content/texte/publications/tecreports/kaweb.pdf`
[15] S. Winograd, *Arithmetic Complexity of Computations,* SIAM, 1980.