Efficient Multiplication in $\mathbb{F}_{3^{\ell m}}$, $m \geq 1$ and $5 \leq \ell \leq 18$

M.Cenk and F. Özbudak

June 12, 2008

Problem

Finite field multiplication plays an important role in public key cryptography and coding theory. Public key cryptographic applications accomplished in very large finite fields. For example, one needs a finite field of at least $\sim 2^{163}$ elements for elliptic curve cryptography. For that reason efficient finite field multiplication has become a crucial part of such applications. A finite field with q^n elements is denoted by $\mathbb{F}_{q^n}$ where q is a prime power and $n \geq 1$. The elements of $\mathbb{F}_{q^n}$ can be represented by n-term polynomials over $\mathbb{F}_q$. Field elements can be multiplied firstly in terms of ordinary multiplication of polynomials and then the result product is reduced by the defining polynomial of the finite field. The reduction step has no multiplicative complexity (S. Winograd). So finite field multiplication is directly related to the polynomial multiplication. Therefore the problem that we have studied is finding efficient polynomial multiplication over finite fields.

Background

The elements of $\mathbb{F}_{3^m}$ can be represented by at most $(m-1)$ degree polynomials over $\mathbb{F}_3$. To multiply elements of $\mathbb{F}_{3^m}$ one can use Karatsuba method or Montgomery formulae , which are among the main algorithms used in every finite fields. On the other hand, for finite fields of fixed characteristics, there are other methods that give more efficient algorithms for polynomial multiplication than Karatsuba and Montgomery in some cases. Some of those methods are Chinese Remainder Theorem (CRT) method and Discrete Fourier Transform (DFT) method. J. Shokrollahi et al. improved the multiplication formula given recently by T. Kerins et al. for $\mathbb{F}_{3^{6m}}$ using DFT method.

Our Contribution

Using a method based on CRT for polynomial multiplication over $\mathbb{F}_3$, we obtained an efficient multiplication method for finite fields of characteristic 3. For $5 \leq \ell \leq 18$, we show that our method gives canonical multiplication formulae over $\mathbb{F}_{3^{\ell m}}$ for any $m \geq 1$ with the best multiplicative complexity improving the bounds in given by P. L. Montgomery. Moreover, we give explicit formula in the case $\mathbb{F}_{3^{6\cdot 97}}$.

Basic Definitions and Notations

- Let $\mathbb{F}_q$ be the field with q elements where $q = 3^n$.
- Let $n \geq 1$ be an integer. A polynomial $A(x)$ of the form

$$A(x) = a_0 + a_1 x + ... + a_{n-1} x^{n-1},$$

  is called an n-term polynomial.
- $M(n)$ denotes the minimum number of multiplications needed in $\mathbb{F}_3$ in order to multiply two arbitrary n-term polynomials. We note that $M(n)$ is also called multiplicative complexity of n-term polynomials.

- Let $M_{f,\ell}(n)$ denote the minimum number of multiplications needed in $\mathbb{F}_q$ in order to obtain the product $A(x) \cdot B(x)$ modulo $f(x)^\ell$.
- Let $M_{(x-\infty),w}(n)$ denote the minimum number of multiplications needed in $\mathbb{F}_q$ in order to obtain $c_{2n-2}, c_{2n-3}, ..., c_{2n-1-w}$ from given n-term polynomials $A(x)$ and $B(x)$ where

$$\begin{aligned} A(x) \cdot B(x) &= (a_0 + ... + a_{n-1}x^{n-1}) \cdot (b_0 + ... + b_{n-1}x^{n-1}) \\ &= c_0 + c_1 x + ... + c_{2n-3}x^{2n-3} + c_{2n-2}x^{2n-2} \end{aligned}$$

Chinese Remainder Theorem for Polynomial Multiplication

CRT method for finite field polynomial multiplication can be summarized as follows. For $1 \leq i \leq t$, let $m_i(x) = f_i(x)^{\ell_i}$ be the ℓ_i-th power ($\ell_i \geq 1$) of an irreducible polynomial $f_i(x)$ such that $deg(m(x)) \geq 2n-1$ where $m(x) = \prod_{i=1}^{t} m_i(x)$. Assume that $f_1(x), ..., f_t(x)$ are distinct. Let $w \geq 1$ be an integer which corresponds to multiplication modulo $(x-\infty)^w$. It follows from CRT algorithm that if

$$w + \sum_{i=1}^{t} \ell_i \; deg(f_i(x)) \geq 2n-1 \tag{1}$$

then

$$M(n) \leq M_{(x-\infty),w}(n) + \sum_{i=1}^{t} M_{f,\ell}(n). \tag{2}$$

Improvements

The value of $M_{f,\ell}(n)$ can be taken as $M(\ell \cdot deg(f))$. For example in the recent paper by Fan and Hasan, $M_{f,\ell}(n) \leq M(\ell \cdot deg(f))$ is used for binary fields. Then we improved the estimate of $M_{f,\ell}(n)$ for the binary field $\mathbb{F}_2$. The same techniques also work for any finite field $\mathbb{F}_q$, in particular for $\mathbb{F}_3$. Before giving the improvement, we give the following definition.

Definition

Let $R = \mathbb{F}_q[x]$ be the ring of polynomials over $\mathbb{F}_q$ in variable x, $\ell \geq 1$ be an integer and

$$A(Y) = a_0(x) + a_1(x)Y + ... + a_{\ell-1}(x)Y^{\ell-1}$$

$$B(Y) = b_0(x) + b_1(x)Y + ... + b_{\ell-1}(x)Y^{\ell-1}$$

be two ℓ-term polynomials in the polynomial ring $R[Y]$ over R. Let $c_0(x), ..., c_{2\ell-2}(x) \in R$ be given by

$$c_0(x) + c_1(x)Y + ... + c_{2\ell-2}(x)Y^{2\ell-2} = A(Y)B(Y).$$

Let $\lambda(\ell)$ denote the minimum number of multiplications needed in R in order to obtain $c_0(x), c_1(x), ..., c_{\ell-1}(x)$.

Theorem

Let $f(x)$ be an irreducible polynomial and $\ell \geq 1$ be an integer such that $\ell\ deg(f(x)) < 2n-1$. We have

$$M_{f,\ell}(n) \leq \lambda(\ell) M(deg(f)). \tag{3}$$

Some effective upper bounds of $\lambda(\ell)$ is given in the following proposition which contributes to improvements on $M_{f,\ell}(n)$.

Proposition

$\lambda(3) \leq 5,\ \lambda(4) \leq 8,\ \lambda(5) \leq 11,\ \lambda(6) \leq 15,\ \lambda(7) \leq 19,\ \lambda(8) \leq 24,$ *and* $\lambda(9) \leq 29.$

Table 1: Upper Bounds for $M_{f,\ell}(n)$.

f	ℓ	Old $M_{f,\ell}(n)$	New $M_{f,\ell}(n)$
f_{11}, f_{12}, f_{13}	3	6	5
f_{11}, f_{12}, f_{13}	4	9	8
f_{11}, f_{12}, f_{13}	5	13	11
f_{11}, f_{12}, f_{13}	6	17	15
f_{11}, f_{12}, f_{13}	7	22	19
f_{11}, f_{12}, f_{13}	8	27	24
f_{11}, f_{12}, f_{13}	9	34	29
f_{21}, f_{22}, f_{23}	3	17	15
f_{21}, f_{22}, f_{23}	4	27	24
f_{21}, f_{22}, f_{23}	5	39	33
$f_{31}, ..., f_{38}$	3	34	30

where f_{ij} denotes an irreducible polynomial of degree i over $\mathbb{F}_3$ which are defined as follows:

$f_{11} = x, f_{12} = x+1, f_{13} = x+2, f_{21} = x^2+1, f_{22} = x^2+x+2, f_{23} = x^2+2x+2, f_{31} = x^3+2x+1, f_{32} = x^3+2x+2, f_{33} = x^3+2x^2+2x+2, f_{34} = x^3+x^2+x+2, f_{35} = x^3+x^2+2, f_{36} = x^3+2x^2+x+1, f_{37} = x^3+x^2+2x+1, f_{38} = x^3+2x^2+1.$

Table 2: Upper Bounds for $M(n)$.

n	Old $M(n)$	New $M(n)$	Modulus polynomials
2	3	3	$(x-\infty), f_{11}, f_{12}$
3	6	6	$(x-\infty), f_{11}^2, f_{12}, f_{13}$
4	9	9	$(x-\infty), f_{11}^2, f_{12}, f_{13}, f_{21}$
5	13	12	$(x-\infty), f_{11}^2, f_{12}, f_{13}, f_{21}, f_{22}$
6	17	15	$(x-\infty)^2, f_{11}, f_{12}, f_{13}, f_{21}, f_{22}, f_{23}$
7	22	19	$(x-\infty)^2, f_{11}^2, f_{12}^2, f_{13}, f_{21}, f_{22}, f_{23}$
8	27	23	$(x-\infty)^3, f_{11}^3, f_{12}^2, f_{13}, f_{21}, f_{22}, f_{23}$
9	34	27	$(x-\infty)^3, f_{11}^3, f_{12}^3, f_{13}^2, f_{21}, f_{22}, f_{23}$
10	39	31	$(x-\infty)^3, f_{11}^3, f_{12}^2, f_{13}^2, f_{21}, f_{22}, f_{23}, f_{31}$
11	46	35	$(x-\infty)^3, f_{11}^3, f_{12}^3, f_{13}^3, f_{21}, f_{22}, f_{23}, f_{31}$
12	51	39	$(x-\infty)^3, f_{11}^3, f_{12}^3, f_{13}^2, f_{21}, f_{22}, f_{23}, f_{31}, f_{32}$
13	60	43	$(x-\infty)^3, f_{11}^3, f_{12}^2, f_{13}^2, f_{21}, f_{22}, f_{23}, f_{31}, f_{32}, f_{33}$
14	66	47	$(x-\infty)^3, f_{11}^2, f_{12}^2, f_{13}^2, f_{21}, f_{22}, f_{23}, f_{31}, f_{32}, f_{33}, f_{34}$
15	75	51	$(x-\infty)^2, f_{11}^2, f_{12}^2, f_{13}^2, f_{21}, f_{22}, f_{23}, f_{31}, f_{32}, f_{33}, f_{34}, f_{35}$
16	81	55	$(x-\infty)^3, f_{11}^3, f_{12}^2, f_{13}^2, f_{21}, f_{22}, f_{23}, f_{31}, f_{32}, f_{33}, f_{34}, f_{35}$
17	94	59	$(x-\infty)^3, f_{11}^3, f_{12}^3, f_{13}^3, f_{21}, f_{22}, f_{23}, f_{31}, f_{32}, f_{33}, f_{34}, f_{35}$
18	102	63	$(x-\infty)^3, f_{11}^3, f_{12}^3, f_{13}^2, f_{21}, f_{22}, f_{23}, f_{31}, f_{32}, f_{33}, f_{34}, f_{35}, f_{36}$

Theorem

The formulae for multiplication of two arbitrary n-term polynomials over $\mathbb{F}_3$ are also valid for multiplication of two arbitrary n-term polynomials over $\mathbb{F}_{3^m}$, where m is any positive integer.

Application

The finite fields of $\mathbb{F}_{3^{6m}}$, where m is prime are used in id-based cryptography for efficient computation of the Tate pairing. T. Kerins et al. showed that multiplication in $\mathbb{F}_{3^{6m}}$ requires 18 multiplications in $\mathbb{F}_{3^m}$. Then J. Shokrollahi et al. found an algorithm for multiplication in $\mathbb{F}_{3^{6m}}$ with 15 multiplications in $\mathbb{F}_{3^m}$. Our method also gives a formula for 6 term polynomial multiplication over $\mathbb{F}_3$ which requires 15 multiplications in $\mathbb{F}_3$. Since the formula for multiplication of two arbitrary n-term polynomials over $\mathbb{F}_3$ is also valid for multiplication of two arbitrary n-term polynomials over $\mathbb{F}_{3^m}$, where m is any positive integer, the formula given in the Appendix A can be used for the multiplication in $\mathbb{F}_{3^{6m}}$ with 15 multiplications in $\mathbb{F}_{3^m}$. The following example compares our formula and the formula given by J. Shokrollahi et al.

Example

We will show that multiplication in $\mathbb{F}_{3^{6\cdot 97}}$ can be done with 15 multiplications in $\mathbb{F}_{3^{97}}$. Let us construct,

$$\begin{aligned} \mathbb{F}_{3^{97}} &\cong \mathbb{F}_3[x]/(x^{97}+x^{16}+2), \\ \mathbb{F}_{3^{6\cdot 97}} &\cong \mathbb{F}_{3^{97}}[y]/(y^6+y-1). \end{aligned}$$

Let $\alpha, \beta, \gamma \in \mathbb{F}_{3^{6\cdot 97}}$ such that $\alpha = \sum_{i=0}^{5} a_i y^i$, $\beta = \sum_{i=0}^{5} b_i y^i$ and $\gamma = \alpha \cdot \beta = \sum_{i=0}^{5} c_i y^i$. Then the coefficients of γ can be found as follows: First compute the coefficients of $\left(\sum_{i=0}^{5} a_i y^i\right)\left(\sum_{i=0}^{5} b_i y^i\right)$ and then reduce it modulo y^6+y-1. Therefore, using the formula in Appendix A we get

$$
\begin{aligned}
c_0 &= -m_{15} - m_1 + m_{10} - m_6 - m_5 + m_7 - m_8 - m_9 - m_{12} - m_{11};\\
c_1 &= m_{15} + m_2 - m_3 - m_4 + m_5 - m_7 - m_8 + m_{10} - m_{11} + m_{12} + m_{13} + m_{14};\\
c_2 &= -m_3 + m_5 + m_4 - m_6 - m_1 - m_2 - m_8 + m_9 - m_{13};\\
c_3 &= -m_3 - m_5 + m_7 - m_1 - m_8 - m_9 - m_{13} - m_{15};\\
c_4 &= m_6 + m_{13} - m_{12} - m_{11} - m_8 - m_{10} - m_5 - m_7 + m_2 - m_3 - m_4;\\
c_5 &= m_{14} - m_8 + m_9 - m_{10} - m_6 + m_{13} - m_1 + m_3 - m_{11} + m_{12};
\end{aligned}
$$

where m_i's are given in Appendix A of our paper.

The explicit formula for multiplication in $\mathbb{F}_{3^{6\cdot 97}}$ given by J. Shokrollahi et al. can be seen in Appendix B of our paper. $\mathbb{F}_{3^{6\cdot 97}}$ is constructed in their paper by using tower field representation, i.e.

$$\begin{aligned}
\mathbb{F}_{3^{97}} &\cong \mathbb{F}_3[x]/(x^{97}+x^{16}+2),\\
\mathbb{F}_{3^{2\cdot 97}} &\cong \mathbb{F}_{3^{97}}[y]/(y^2+1),\\
\mathbb{F}_{3^{6\cdot 97}} &\cong \mathbb{F}_{3^{2\cdot 97}}[z]/(z^3-z-1).
\end{aligned}$$

In our formula the only nonzero coefficients are ∓ 1 and we do not need to introduce intermediate field extensions like $\mathbb{F}_{3^{2\cdot 97}}$.

Conclusion

For each $5 \leq \ell \leq 18$ we obtain a canonical multiplication formula in $\mathbb{F}_{3^{\ell m}}$ which is valid for any $m \geq 1$. To the best of our knowledge, these formulae have the best known multiplication complexity in the literature. Moreover, we give explicit formula in the case $\mathbb{F}_{3^{6 \cdot 97}}$.

Thanks...