Charlier Polynomial Representation for Finite Fields of Characteristic Three

Sedat Akleylek[1,2], **Ferruh Özbudak**[2,3], **Canan Özel**[2]

[1] *Department of Computer Engineering, Ondokuz Mayıs University, Samsun,*
sedat.akleylek@bil.omu.edu.tr
[2] *Institute of Applied Mathematics, METU, Ankara, Turkey*
ozbudak@metu.edu.tr, ccimen@metu.edu.tr
[3] *Department of Mathematics, METU, Ankara, Turkey*

1 Introduction

Finite field arithmetic is widely studied in cryptographic applications, coding theory and computer algebra [6]. In recent years, there has been an interest on the implementation of cryptographic systems based on odd characteristic finite fields $\mathbb{F}_{p^n}$, where p is a prime, as a result of the applications in areas such as elliptic curve cryptography and pairing based cryptography. The progress in the pairing based cryptography increase the importance of arithmetic of finite fields in characteristic three [4], [5].

In this paper, we focus on the multiplication of elements in certain extension fields of $\mathbb{F}_3$. In [2], Hermite polynomials are used to represent finite fields $\mathbb{F}_{3^n}$. In this study, we use Charlier polynomials as basis elements of finite fields $\mathbb{F}_{3^n}$. In [1], multiplication of elements of the binary fields in Charlier polynomial representation is presented and the total arithmetic complexity is given. We modify this idea for the finite fields of characteristic three. We obtain binomial irreducible polynomials in Charlier polynomial representation to get faster modular reduction. We give the general method to multiply two elements of $\mathbb{F}_{3^n}$ in Charlier polynomial representation and give the total arithmetic complexity. All computations are done by using Maple [7].

2 Preliminaries

In this section, we give preliminaries about Charlier polynomial representation of finite fields of characteristic three. The Charlier polynomials are $C_0(x) = 1$, $C_1(x) = x$ and for $n \geq 2$

$$C_n(x) = (x - n + 1) \cdot C_{n-1}(x)$$

The multiplication of Charlier polynomials in $\mathbb{F}_3[x]$ is given in Theorem 1.

Theorem 1. *Let $C_n(x) = \beta_n$ be the n-th Charlier polynomial in $\mathbb{F}_3[x]$, where $n \geq 0$. Then for all $i, j \geq 0$ the Charlier polynomials $\{\beta_0, \beta_1, ..., \beta_{n-1}, ..\}$ satisfies the following equation*

$$\beta_i \cdot \beta_j = \beta_{i+j} + l \cdot (k \cdot \beta_{i+j-1} + 2 \cdot m \cdot \beta_{i+j-2}) \tag{1}$$

where $l, k, m \in \mathbb{F}_3$ is defined as

$$l = \begin{cases} 0 & \text{if } i \text{ or } j \equiv 0 \text{ mod } 3 \\ 1 & \text{otherwise.} \end{cases}$$

$$k = \begin{cases} 1 & \text{if } i \equiv j \text{ mod } 3 \\ 2 & \text{otherwise.} \end{cases}$$

$$m = \begin{cases} 1 & \text{if } i, j \equiv 2 \text{ mod } 3 \\ 0 & \text{otherwise.} \end{cases}$$

3 Multiplication of Polynomials in Charlier Representation

In this section, we describe the multiplication of field elements represented by Charlier polynomials and explore the complexity of the multiplication. It is well-known that multiplication of finite field elements can be performed in two steps: first multiplication of polynomials and then modular reduction with respect to the irreducible polynomial that is chosen before [6]. We give the multiplication and the reduction operations, respectively. Theorem 2 gives the required number of multiplications and additions to multiply polynomials in Charlier basis where $M(n)$ and $A(n)$ denote the minimum number of multiplications and the minimum number of additions for corresponding algorithm for two n-term polynomials multiplication.

Theorem 2. *Let $a = a_{n-1}\beta_{n-1} + ... + a_0\beta_0$ and $b = b_{n-1}\beta_{n-1} + ... + b_0\beta_0$ be n-term polynomials over $\mathbb{F}_3$ and $a \cdot b = c_{2n-2}\beta_{2n-2} + ... + c_0\beta_0$. By using any multiplication method, the coefficients of the polynomial c are computed with*

$$M(n) \quad + \quad M(n - \lceil \frac{n}{3} \rceil - \lfloor \frac{n - \lceil \frac{n}{3} \rceil}{2} \rfloor) + 3 \cdot M(\lfloor \frac{n - \lceil \frac{n}{3} \rceil}{2} \rfloor)$$

$$+ \quad 4 \cdot \lfloor \frac{n - \lceil \frac{n}{3} \rceil}{2} \rfloor \cdot (n - \lceil \frac{n}{3} \rceil - \lfloor \frac{n - \lceil \frac{n}{3} \rceil}{2} \rfloor)$$

multiplications and

$$A(n) \quad + \quad A(n - \lceil \frac{n}{3} \rceil - \lfloor \frac{n - \lceil \frac{n}{3} \rceil}{2} \rfloor) + A(\lfloor \frac{n - \lceil \frac{n}{3} \rceil}{2} \rfloor) + \lfloor \frac{(2n-3) - \lceil \frac{2n-4}{3} \rceil}{2} \rfloor$$

$$+ \quad 2 \cdot \lfloor \frac{n - \lceil \frac{n}{3} \rceil}{2} \rfloor \cdot (n - \lceil \frac{n}{3} \rceil - \lfloor \frac{n - \lceil \frac{n}{3} \rceil}{2} \rfloor) + 2 \cdot \lceil \frac{2n-4}{3} \rceil$$

additions.

Then, we perform the reduction operations with respect to the irreducible Charlier binomials, $\beta_n + \beta_0$ where $n > 0$. In this paper, we give the multiplication and reduction complexities and we compare these results with the arithmetic complexity results in [2].

Acknowledgement

Sedat Akleylek and Ferruh Özbudak are partially supported by TUBITAK under the Grant No. TBAG-109T672.

References

[1] S. Akleylek, M. Cenk, F. Özbudak, *Polynomial Multiplication over Binary Fields Using Charlier Polynomial Representation with Low Space Complexity*, INDOCRYPT 2010: 227-237.

[2] S. Akleylek, F. Özbudak, C. Özel, *Hermite Polynomial Representation for Finite Fields of Characteristic Three*, 5th International Information Security and Cryptology Conference (ISCTURKEY 2012), Ankara, 2012.

[3] H. Cohen, G. Frey, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Discrete Math. Appl., Chapman Hall/CRC, 2006.

[4] R. Granger, D. Page and M. Stam. Hardware and software normal basis arithmetic for pairing based cryptography in characteristic three. *IEEE Transactions on Computers*, 54 (2005), 852-860.

[5] K. Harrison, D. Page and N. Smart. Software implementation of finite fields of characteristic three, for use in pairing-based cryptosystems.*LMS Journal of Computation and Mathematics*, 5 (2002), 181-193.

[6] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*. Cambridge University, 1997.

[7] www.maplesoft.com