Rings of Low Multiplicative Complexity and Fast Multiplication in Finite Fields $\mathbb{F}_{2^N}$

Murat Cenk[1] and Ferruh Özbudak[2]

***Abstract*— We survey the rings of low multiplicative complexity and the redundant representation of finite fields. The construction is originally due to Ito and Tsujii [3]. We give the important results of Silverman's works in [1], [2]. Moreover, we note that the fields constructed with Silverman's method are not suitable for elliptic curve cryptography while Silverman suggests those curves can be used in elliptic curve cryptography.**

***Index Terms*— Finite fields, redundant representation**

I. Introduction

FINITE field multiplication is widely used in many areas such as cryptography and coding theory. For example, the field operations are used in key exchange, encryption, signing and authentication. The binary field $\mathbb{F}_{2^N}$ is especially used for computer implementation due to the binary structure of computers. In this paper, we give an overview of the important representation of finite fields so called redundant representation. Moreover, we discuss the application of the redundant representation in $\mathbb{F}_{2^N}$. This paper is a survey of papers [1], [2].

In section 2 we give the basic definitions and notations. Examples are given in Section 3 to show the concepts from Section 2. Fields and rings of low complexity are given in the next section. In Section 5 the application part, fast multiplication in finite fields $\mathbb{F}_{2^N}$ is given. Finally, selection of fields $\mathbb{F}_{2^N}$ is presented in Section 6.

II. Definitions and Notations

In this section we give the basic definitions and notations that are used throughout the paper.

Let k be a field and R be a k-algebra with a finite basis $\mathcal{B} = \{x_1, x_2, ..., x_r\}$ as k-vector space. The multiplication law in R is given by the equation

$$x_i x_j = \sum_{k=1}^{r} \lambda_{ij}^k x_k, \ 1 \leq i, j, k \leq r,$$

where $\lambda_{ij}^k \in k$. The complexity of the basis $\mathcal{B}$ is defined to be

$$C(\mathcal{B}) = \frac{1}{r} \#\{(i, j, k) : \lambda_{ij}^k \neq 0\}$$

and complexity of R is defined as

$$C(R) = \min\{C(\mathcal{B}) : \mathcal{B} \text{ is a } k\text{-basis for } R\}.$$

[1]Department of Mathematics and Computer Science, Çankaya University, Ankara, Turkey, E-mail: mcenk@cankaya.edu.tr

[2]Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey, E-mail: ozbudak@metu.edu.tr

For example, the normal basis $\mathcal{B}$ of the finite field $\mathbb{F}_{2^N}$ is well known to have the complexity $C(\mathcal{B}) \geq 2n-1$. For some certain fields the equality $C(\mathcal{B}) = 2n-1$ is obtained. In this case the normal basis $\mathcal{B}$ is called optimal normal basis or ONB. We refer to [6], [7] for the details.

An useful property of a basis is the symmetry so that the r^3 multipliers λ_{ij}^k are determined by the r^2 multipliers λ_{ij}^1 using a simple transformation. It is said that $\mathcal{B}$ is a permutation basis if there are permutations $\sigma_k, \tau_k \in \mathcal{S}_r, 1 \leq k \leq r$ such that

$$\lambda_{ij}^k = \lambda_{ij}^1 \quad \text{for all } i, j, k.$$

If $a = \sum a_i x_i$ and $b = \sum B_i x_i$ and if $\mathcal{B}$ is a permutation basis as above, then

$$ab = \sum_{i,j,k=1}^{r} a_i b_j \lambda_{ij}^k = \sum_{k=1}^{r} \left(\sum_{i,j=1}^{r} a_{\sigma_k^{-1}} b_{\tau_k^{-1}} \lambda_{ij}^1 \right) x_k.$$

Note that if $\mathcal{B}$ is permutation basis, then its complexity is determined by the λ_{ij}^1's,

$$C(\mathcal{B}) = \#\{(i, j) : \lambda_{ij}^1 \neq 0\}.$$

In order to obtain smaller multiplicative complexity than ONB complexity one can begin with a quotient field K of R and lift the elements of K to elements of R. All computations can be operated in R and go back to K if the complexity of R is smaller than K. Let $\rho(R)$ be defined as

$$\rho(R) = \dim_k R - \max\{\dim_k K : K \text{ is a quotient field of } R\}.$$

It would be better $\rho(R)$ to be small for practical applications, which means that R has a large quotient field. Obviously, $\rho(R) = 0$ if and only if $K = R$.

III. Examples

In this section a number of examples are given to show the concepts from Section II.

Example 3.1: Consider the ring $R = k[x]/(x^r)$. Let the set $\mathcal{B} = \{1, x, x^2, ..., x^{r-1}\}$ be a basis of R. The multiplication law is given by $x^i x^j = x^{i+j}$ if $i + j < r$, and $x^i x^j = 0$ if $i + j \geq r$, so

$$\lambda_{ij}^k = \begin{cases} 1 & \text{if} \quad i + j = k < r, \\ 0 & \text{otherwise.} \end{cases}$$

So one can obtain the complexity

$$C(\mathcal{B}) = \frac{1}{r} \sum_{0 \leq i,j < r, i+j < r} 1 = \frac{r+1}{2}.$$

It is seen that complexity can be rational. Note that the only field of R is k. Hence $\rho(R) = r - 1$.

Example 3.2: Let $A \in k$, $A \neq 0$, and $R = k[x]/(x^r - A)$ with basis $\mathcal{B} = \{1, x, x^2, ..., x^{r-1}\}$. Then

$$x^i x^j = \begin{cases} x^{i+j} & \text{if} \quad i+j < k \\ Ax^{i+j-r} & \text{if} \quad i+j \geq r, \end{cases}$$

$$\lambda_{ij}^k = \begin{cases} 1 & \text{if} \quad i+j = k, \\ A & \text{if} \quad k = i+j-r, \\ 0 & \text{otherwise.} \end{cases}$$

Then the complexity of $\mathcal{B}$ becomes

$$C(\mathcal{B}) = r,$$

because there is only one k with $\lambda_{ij}^k \neq 0$ for each (i, j). Now, $\rho(R)$ can be computed. Let $x^r - 1 = f_1 f_2 ... f_s$ be irreducible factors and let $d_i = \deg f_i$. Since $k[x]/(f_i)$ is a quotient field of R of dimension d_i, it is seen that

$$\rho(R) = r - \max d_i.$$

Note that if $A = 1$ then

$$x^r - 1 = (x-1)(x^{r-1} + x^{r-2} + ... + x + 1).$$

If the polynomial $\Phi(x) = x^{r-1} + x^{r-2} + ... + x + 1$ is irreducible in $k[x]$ then $\rho(R) = 1$. Moreover, we know that $\Phi(x)$ is irreducible in $k[x]$ if and only if r is prime and q, number of elements in k, is a primitive root in $\mathbb{Z}/r\mathbb{Z}$. We will see details of this situation for $k = \mathbb{F}_2$ in next section.

Example 3.3: Consider the ring $R = k[x]/(x^r - \alpha x - \beta)$ for some $\alpha, \beta \in k^*$ and the basis $\mathcal{B} = \{1, x, x^2, ..., x^{r-}\}$. Then

$$x^i x^j = \begin{cases} x^{i+j} & \text{if} \quad i+j < r \\ \alpha x^{i+j-r+1} + \beta x^{i+j-r} & \text{if} \quad i+j \geq r. \end{cases}$$

So one can obtain the complexity as

$$C(\mathcal{B}) = \frac{3r-1}{2}.$$

Note that this result is better than a normal basis which has multiplicative complexity greater than or equal $(2r-1)$. However normal basis has many advantages such as squaring complexity and permutability.

Example 3.4: Consider $k = \mathbb{F}_2$, $\Phi(x) = x^{r-1} + x^{r-2} + ... + x + 1$, and the ring $R = \mathbb{F}_2[x]/(\Phi(x))$. Note that R is subring of $\mathbb{F}_2/(x^{r+1} - 1)$ for which standard basis has complexity $r+1$. Multiplication rule in R is given by the rules

$$x^i x^j = \begin{cases} x^{i+j} & \text{if} \quad i+j < r \\ 1 + x + ... + x^{r-1} & \text{if} \quad i+j = r \\ x^{i+j-r-1} & \text{if} \quad i+j \geq r. \end{cases}$$

The r pairs (i, j) for which r of the λ_{ij}^k are non-zero and the remaining $r^2 - r$ pairs (i, j) have exactly one non-zero λ_{ij}^k and therefore

$$C(\mathcal{B}) = \frac{1}{r}(r^2 + r^2 - r) = 2r - 1.$$

As it is seen the multiplicative complexity of $\mathcal{B}$ is twice as large as the ring of dimension one higher that contains R.

Example 3.5: Let R_1 and R_2 be rings of dimensions r_1 and r_2 over k, respectively. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be k-bases with $C(\mathcal{B}_i) = C(R_i)$ for $i = 1, 2$. Then the product ring $R = R_1 \times R_2$ of dimension $r = r_1 + r_2$ has a natural product basis

$$\mathcal{B} = \{(y, 0) : y \in \mathcal{B}_1\} \cup \{(0, z) : z \in \mathcal{B}_2\}.$$

Since $(y, 0)(0, z) = (0, 0)$, the complexity of the basis $\mathcal{B}$ is given by the formula

$$rC(\mathcal{B}) = r_1 C(\mathcal{B}_1) + r_2 C(\mathcal{B}_2) = r_1 C(R_1) + r_2 C(R_2).$$

Then it follows that

$$C(R_1 \times R_2) \leq \frac{r_1 C(R_1) + r_2 C(R_2)}{r_1 + r_2}.$$

Example 3.6: The product basis of $R_1 \times R_2$ described in Example 3.5 has the property $x_i x_j = 0$. In the case where $R_1 = k$, this property is eliminated by forming twisted product basis

$$\mathcal{B} = \{(1, 1) : y \in \mathcal{B}_1\} \cup \{(0, z) : z \in \mathcal{B}_2\}.$$

This gives

$$C(R) = \left(1 - \frac{1}{r}\right)(C(R_2) - r_2) + r.$$

The intermediate steps can be seen in [2].

IV. Fields and Rings of Low Complexity

In this section, the main result in [2] will be given. Firstly the theorem which describes all field extensions of a finite field for which the complexity is equal to the dimension. Next a complete classification of all rings R/k with low complexity $C(R) \leq \dim_k R$ and a quotient field of dimension $\dim_k R - 1$ are presented. The proof of theorems are in [2].

Theorem 4.1: Let k be a field with q elements and let K/k be afield extension of degree r. Then $C(K) = r$ if and only if the following two conditions are true:

(i) Every prime dividing r also divides $q - 1$.
(ii) Either $4 \nmid r$ or $4 \mid q - 1$.

Further, if (i) and (ii) are true, then K is isomorphic to $k[x]/(x^r - A)$ for some $A \in k$ such that $x^r - A$ is irreducible in $k[x]$.

Theorem 4.2: Let k be a field with q elements and let R be a k-algebra of dimension r satisfying

$$\rho(R) = 1 \text{ and } C(R) \leq r.$$

Then R has one of the following forms:

(i) $R \cong k[x]/(x^r - 1)$ where r is a prime and q is a primitive root modulo r. The basis $\mathcal{B} = \{1, x, x^2, ..., x^{r-1}\}$ is a permutation basis for R satisfying $C(\mathcal{B}) = C(R)$.
(ii) There is a field K/k so that $R \cong k \times K$, and the basis $\mathcal{B}$ for R satisfying $C(\mathcal{B}) = r$ is a twisted product basis as given in Example 3.6. Further $C(K) = \dim_k K$, so in particular $K \cong k[x]/(x^{r-1} - A)$ is a field extension of the type described in Theorem 4.1.
(iii) There is a field K/k so that $R \cong k \times K$, and the basis $\mathcal{B}$ for R satisfying $C(\mathcal{B}) \leq r$ is a product basis as in the Example 3.5.
(iv) r=2 and $R \equiv k[x]/(x^2)$.

Only in case (i) does R have a permutation basis $\mathcal{B}$ satisfying $C(\mathcal{B}) \leq r$.

Note that the rings in Theorem 4.2 (i) are of the particular interest for practical implementations. In the next section, the case $k = \mathbb{F}_2$ and $R = \mathbb{F}_2 \times \mathbb{F}_{2^{r-1}}$ is analyzed.

V. Fast Multiplication in Finite Fields $\mathbb{F}_{2^N}$

In this section we give an application of Theorem 4.2. It is described for performing computations in a finite field $\mathbb{F}_{2^N}$ by embedding it a larger ring R where multiplicative complexity of R is $N+1$ which is approximately twice as efficient as optimal normal basis multiplication.

The field $\mathbb{F}_{2^N}$ can be generated as a quotient $\mathbb{F}_2[x]/(\Phi(x))$, where

$$\Phi(x) = x^N + x^{N-1} + x^{N-2} ... + x + 1.$$

It is known that the polynomial $\Phi(x)$ over $\mathbb{F}_2$ is irreducible if and only if

- $p = N + 1$ is prime,
- 2 is a primitive root modulo p.

The second condition says that

$$2^{N/\ell} \not\equiv 1 \mod p, \text{ for every prime } \ell \text{ dividing } N.$$

When the field $\mathbb{F}_{2^N}$ represented in standard way as the set of polynomials modulo $\Phi(x)$ it is seen that $\mathbb{F}_2[x]/(\Phi(x))$ is a subring of the ring of polynomials modulo $x^p - 1$, where $N = p - 1$. In other words,

$$\frac{\mathbb{F}_2[x]}{(x^p - 1)} \cong \mathbb{F}_{2^N} \times \mathbb{F}_2.$$

Note that this is an isomorphism of rings, not fields. Let R_p denote the ring of polynomials modulo $x^p - 1$,

$$R_p = \frac{\mathbb{F}_2[x]}{(x^p - 1)}.$$

An element of R_p can be represented by

$$a = a_N x^N + a_{N-1} x^{N-1} + ... + a_x + a_0$$

and it can be also represented by a list

$$a = [a_N, a_{N-1}, ..., a_1, a_0]$$

where $a_i \in \mathbb{F}_2$ for $0 \leq i \leq N$.

Remark 5.1: Note that the method constructed above can be generalized for fields $\mathbb{F}_{q^N}$ for any prime power q provided $p = N + 1$ is prime and q is primitive root modulo p. The generalization is given in [4].

Now it is given the multiplicative complexity of the ring R_p. The complexity of the basis $\mathcal{B} = \{1, x, x^2, ..., x^{p-1}\}$ for the ring R_p is clearly $C(\mathcal{B}) = p$ since $\lambda_{ij}^k = 1$ where λ_{ij}^k is given in Section II. Therefore R_p has complexity $p = N + 1$ while the complexity of optimal normal basis for F_{2^N} is $2N - 1$. Therefore, it is better to perform $\mathbb{F}_{2^N}$ multiplication by first moving to R_p and then doing the multiplications in R_p.

The lift operations between $\mathbb{F}_{2^N}$ and R_p are performed as follows: An element of $\mathbb{F}_{2^N}$ and R_p are represented by

$$[a_{N-1}, ..., a_1, a_0], \quad [a_N, a_{N-1}, ..., a_1, a_0].$$

The extra bit in R_p is called ghost bit. In order to do a computation in $\mathbb{F}_{2^N}$ we first move R_p then do all computations in R_p and finally go back to $\mathbb{F}_{2^N}$. Note that movement between $\mathbb{F}_{2^N}$ and R_p is fast, at most a single complement operation.

More clearly, the map between $\mathbb{F}_{2^N}$ and R_p is given by

$$\begin{array}{ccc} \mathbb{F}_{2^N} & \longrightarrow & R_p \\ a = [a_{N-1}, ..., a_1, a_0] & \longrightarrow & [0, a_{N-1}, ..., a_1, a_0]. \end{array}$$

Inverse map is given by

$$R_p \longrightarrow \mathbb{F}_{2^N}$$

$$[a_N, a_{N-1}, ..., a_1, a_0] \longrightarrow \begin{cases} [a_{N-1}, ..., a_1, a_0] & \text{if} \quad a_N = 0 \\ \sim [a_{N-1}, ..., a_1, a_0] & \text{if} \quad a_N = 1 \end{cases}$$

where $\sim$ means take the complement of every bit.

VI. Selection of Fields $\mathbb{F}_{2^N}$

The first condition in choosing $\mathbb{F}_{2^N}$ is that 2 is a primitive root modulo p and $p = N + 1$ is prime since this ensures that the cyclotomic polynomial

$$\Phi(x) = x^N + x^{N-1} + ... + x^2 + x + 1 = \frac{x^{N+1} - 1}{x - 1}$$

is irreducible in $\mathbb{F}_2[x]$.

Some of the values of p, where $N = p - 1$ are $\{101, 107, 131, 139, 149, 163, 173, 179, 181, 197, 211, 227, 269, 193, 653, 659, 661, 677, 701, 709, 757, 773, 787, 821, 829, 1019, 1061, 1091, 1109, 1117, 1123, 1171, 1187\}$. As it is seen there are limited value of N. In paper [1] it is said that for elliptic curve cryptography one might take N to be one of the values $162, 172, 178, 180$ or 196. However we want to note that those values are not secure since the composite extension fields are weak due to weil-descent attack [5]. In fact, since the value p is prime and $N = p - 1$ is always even, the fields constructed in this method are not suitable for elliptic curve cryptography.

On the other hand, one can use the field in $\mathbb{F}_{2^N}$ in Diffie-Hellman key exchange or ElGamal system. In this case, the multiplicative group $\mathbb{F}_{2^N}^*$ is a cyclic group of order $2^N - 1$ and if $2^N - 1$ is the product of small primes then Pohlig-Hellman algorithm solves the discrete logarithm problem which provides the security of Diffie-Hellman key exchange or ElGamal system.

To find the prime divisors od $2^N - 1$, one can start with the factorization of $X^N - 1$ as a product of cyclotomic polynomials

$$x^N - 1 = \prod_{d|N} \Phi_d(x),$$

where $\Phi_d(x)$ is d^{th} cyclotomic polynomial. That is, the roots of $\Phi_d(x)$ are primitive d^{th} roots of unity,

$$\Phi_d(x) = \prod_{1 \leq k \leq d, \ \gcd(k,d)=1} (x - e^{2\pi k/d}).$$

Therefore we have the following relation:

$$2^N - 1 = \prod_{d|N} \Phi_d(2),$$

so one should find the large prime divisors of $\Phi_d(x)$. For example, consider the situation, $p = 787$ and $N = 786$. Since 786 is divisible by 393 it is seen that $2^{786} - 1$ is divisible by

$$\Phi_{393}(2) = \frac{2^{393} - 1}{(2^3 - 1)(2^{131} - 1)}.$$

One can find the value of $\Phi_{393}(2)$ as

$$\Phi_{393}(2) = 36093121 \cdot 51118297 \cdot 58352641 \cdot q,$$

where $q \approx 2^{183}$ is a prime. Hence $2^{786} - 1$ is divisible by the large prime q.

REFERENCES

[1] J.H. Silverman, "Fast Multiplication in Finite Fields $GF(2^N)$," Cryptographic Hardware and Embedded Systems, Proc. First Intl Workshop, CHES 99, C K. Koc and C. Paar, eds. pp. 122-134, 1999.
[2] J. H. Silverman, "Rings of Low Multiplicative Complexity", *Finite Fields and Their Applications*, vol. 6, no. 2, pp. 175-191, 2000.
[3] T. Itoh and S. Tsujii, "Structure of Parallel Multipliers for a Class of Fields $GF(2^m)$," Information and Computation, vol. 83, no. 1, pp. 21-40, 1989.
[4] W. Geiselmann and S. Rainer, "A Redundant Representation of $GF(q^n)$ for Designing Arithmetic Circuits, IEEE Trans. Computers, 52(7):848-853, 2003.
[5] P. Gaudry, F. Hess and N. P. Smart, "Constructive and Destructive Facets of Weil Descent on Elliptic Curves", J. Cryptology, 15(1):19-46, 2002.
[6] Gao, S., Vanstone, S.A., "On orders of optimal normal basis generators", Mathema- tics of Computation,64 (1995), 1227-1233.
[7] Mullin, R., Onyszchuk, I., Vanstone, S., Wilson, R., "Optimal normal bases in $GF(p^n)$", Discrete Applied Mathematics., 22, (1988), 149-161.