Generating Idempotents of Quintic Residue Codes over the Binary Field

Xuedong Dong[1, a]

[1]College of Information Engineering, Dalian University, Dalian 116622, P. R. China

[a]dongxuedong@sina.com

Keywords: Generating idempotent; Residue code; Cyclic code

Abstract. It is well known that to construct the generating polynomials of higher power residue codes over finite fields is difficult. This paper gives explicit expressions of generating idempotents of quintic residue codes over the binary field. Using the result obtained, one can construct the generating polynomials of quintic residue codes over the binary field by computing the greatest common divisors of these generating idempotents and the polynomial x^n-1 with computer software such as Matlab and Maple.

Introduction

In many digital applications like computer memory, data storage media, satellite and deep space communications, error coding is used. Prange introduced the class of quadratic residue codes in 1958 [1]. It is a nice family of cyclic codes that has approximately 1/2 code rates, tends to have high minimum distance and includes some Hamming codes and Golay codes. Idempotents of quadratic residue codes were discussed in Chapter 16 of [2].Decoding algorithms for quadratic residue codes were still interesting [3]. There are various generalizations of quadratic residue codes. Charters [4] provided a generalization of binary quadratic residue codes to the cases of higher power prime residues over the finite field of the same order. Higher power residue codes and forms of generating polynomials of these codes were proposed in [5-9].Generating polynomials of higher power residue codes are factors of x^n-1. Generally speaking, it is difficult to factor the polynomial x^n-1 over finite fields. In [7-8], generating idempotents of cubic and quartic residue codes over the fields F_2 and F_3 were given. In [9], generating idempotents of cubic residue codes over the field F_4 were given. This paper gives generating idempotents of quintic residue codes over the binary field F_2. Thus, the generating polynomials of quintic residue codes over the binary field can be obtained by computing the greatest common divisors of these generating idempotents and the polynomial x^n-1 with computer software such as Matlab. The rest of this paper is organized as follows. In Section 2 we give some preliminaries. Generating idempotents of quintic residue codes over the binary field are given in Section 3. Finally, summary is given in Section 4.

Preliminaries

*Definition 1.*If there exists an integer x such that $x^5 \equiv a \left(\bmod p\right)$, where $a \in Z$ and $(a, p)=1$,then a is called a quintic residue modulo p.

In the following we assume that p is an odd prime and ρ is a primitive element of the finite field F_p. Let $R_0=\left\{\rho^{tk} \in F_P \mid k \in Z\right\}, R_1=\left\{\rho^{tk+1} \in F_P \mid k \in Z\right\}, \cdots, R_{t-1}=\left\{\rho^{tk+(t-1)} \in F_P \mid k \in Z\right\}$. Let m be the smallest positive integer such that $2^m \equiv 1 \left(\bmod p\right)$, α a primitive p-th root of unity in F_{2^m}, and

$$g_0(x)=\prod_{r_0 \in R_0}\left(x-\alpha^{r_0}\right) \quad g_1(x)=\prod_{r_1 \in R_1}\left(x-\alpha^{r_1}\right) \cdots, g_{t-1}(x)=\prod_{r_{t-1} \in R_{t-1}}\left(x-\alpha^{r_{t-1}}\right)$$

Lemma 1. $x^p-1=(x-1)g_0(x)\cdots g_{t-1}(x)$ and $g_j(x)=\prod_{r_j\in R_j}\left(x-\alpha^{r_j}\right)\in F_2[x]$ for $j=0,1,2,\cdots,t-1$.

Definition 2. [7] The t -th residue codes $C_0,\cdots,C_{t-1},\overline{C}_0,\cdots,\overline{C}_{t-1}$ are cyclic codes of $F_2[x]/(x^p-1)$ with generator polynomials $g_0(x),\cdots,g_{t-1}(x),(x-1)g_0(x),\cdots,(x-1)g_{t-1}(x)$ respectively.

Definition 3 .[10,p.132] An element $e(x)\in F_2[x]/\left(x^p-1\right)$ satisfying $e(x)^2\equiv e(x)\left(\bmod x^p-1\right)$ is called an idempotent. Each cyclic code contains a unique idempotent which generates the ideal. This idempotent is called the generating idempotent of the cyclic code.

Definition 4.[10, p.138] Let a be an integer such that $(a,n)=1$. The function μ_a defined on $\{0,1,\cdots,n-1\}$ by $i\mu_a\equiv ia(\bmod n)$ is a permutation of the coordinate positions $\{0,1,\cdots,n-1\}$ of a cyclic code of length n and is called a multiplier. μ_a acts on $F_p[x]/(x^n-1)$ by $f(x)\mu_a\equiv f(xa)$ $(\bmod x^n-1)$, where $f(x)\in F_p[x]/(x^n-1)$.

Lemma 2.[10, p.139] Let C be a cyclic code of length n over the finite field F_q with generating idempotent $e(x)$. Let a be an integer such that $(a,n)=1$. Then $e(x)$ μ_a is the generating idempotent of the cyclic code $C\mu_a$.

Lemma 3.[7] $C_0,\cdots,C_{t-1}$ are pairwise equivalent and $\overline{C}_0,\cdots,\overline{C}_{t-1}$ are pairwise equivalent.

In the following assume that $e_0(x)=\sum_{r_0\in R_0}x^{r_0}$ $e_1(x)=\sum_{r_1\in R_1}x^{r_1}$, $\cdots,e_{t-1}(x)=\sum_{r_{t-1}\in R_{t-1}}x^{r_{t-1}}$

Lemma 4. [7] $e_0(x)+e_1(x)+\cdots+e_{t-1}(x)+\sum_{i=0}^{p-1}x^i=1$

Lemma 5. [7] Let $E(x)$ be the generating idempotent of a t -th residue code C . Then $E(x)=a+\sum_{i=0}^{t-1}a_ie_i(x)$, where $a,a_0,a_1,\cdots,a_{t-1}\in F_2$.

Lemma 6. If $\overline{E}_0(x)$ is the generating idempotent of the quintic residue code $\overline{C}_0$, then $E_0(x)=\overline{E}_0(x)$ $+\sum_{i=0}^{p-1}x^i$ is the generating idempotent of C_0.

Proof. The proof is similar to that of Lemma 9 in [7].

*Lemma 7.*If $E_0(x)$ and $\overline{E}_0(x)$ are respectively the generating idempotents of the t -th residue codes C_0 and $\overline{C}_0$, and $d=\rho^{tk+t-1}\in R_{t-1}$, then

1. $E_0(x)\mu_d=E_1(x),E_1(x)\mu_d=E_2(x),\cdots,E_{t-2}(x)\mu_d=E_{t-1}(x)$ are respectively the generating idempotents of the t -th residue codes $C_1,\cdots,C_{t-1}$.

2. $\overline{E}_0(x)\mu_d=\overline{E}_1(x),\overline{E}_1(x)\mu_d=\overline{E}_2(x),\cdots,\overline{E}_{t-2}(x)\mu_d=\overline{E}_{t-1}(x)$ are respectively the generating idempotents of the t -th residue codes $\overline{C}_1,\cdots,\overline{C}_{t-1}$.

Proof. The proof is similar to that of Lemma 10 in [7].

Generating Idempotents of the Quintic Residue Codes

*Theorem 1.*Let $5\,|\left(p-1\right)$ and 2 be a quintic residue modulo p .Let $C_0,C_1,C_2,C_3,C_4,\overline{C}_0,\overline{C}_1,\overline{C}_2,\overline{C}_3,\overline{C}_4$

Be quintic residue codes. Then:

1) The set of generating idempotents of the quintic residue codes C_0, C_1, C_2, C_3, C_4 is $\{1+e_0(x), 1+e_1(x), 1+e_2(x), 1+e_3(x), 1+e_4(x)\}$ or $\{1+e_0(x)+e_1(x)+e_3(x),\ 1+e_1(x)+e_2(x)+e_4(x),$ $1+e_0(x)+e_2(x)+e_3(x),\quad 1+e_1(x)+e_3(x)+e_4(x),\quad 1+e_0(x)+e_2(x)+e_4(x)\}$ or $\{1+e_0(x)+e_1(x)+e_2(x),$ $1+e_1(x)+e_2(x)+e_3(x),\ 1+e_2(x)+e_3(x)+e_4(x),\ 1+e_0(x)+e_3(x)+e_4(x),\ 1+e_0(x)+e_1(x)+e_4(x)\}$.

2) The set of generating idempotents of the quintic residue codes $\overline{C}_0, \overline{C}_1, \overline{C}_2, \overline{C}_3, \overline{C}_3, \overline{C}_4$ is $\{e_1(x)+e_2(x)+e_3(x)+e_4(x),\ e_0(x)+e_2(x)+e_3(x)+e_4(x), e_0(x)+e_1(x)+e_3(x)+e_4(x),$ $e_0(x)+e_1(x)+e_2(x)+e_4(x), e_0(x)+e_1(x)+e_2(x)+e_3(x)\}$ or $\{e_2(x)+e_4(x),\ e_0(x)+e_3(x),$ $e_1(x)+e_4(x)\quad,\quad e_0(x)+e_2(x)\quad,\quad e_1(x)+e_3(x)\}$ or $\{e_3(x)+e_4(x),\ e_0(x)+e_4(x), e_0(x)+e_1(x), e_1(x)+e_2(x), e_2(x)+e_3(x)\}$.

Proof. Since $(p-1)/5$ is even, we have $(p-1)/5=0$ over the binary field F_2. By lemma 5 let $\overline{E}_0(x)=a+\sum_{i=0}^{4}a_ie_i(x)$ be the generating idempotent of the quintic residue code $\overline{C}_0$, where $a, a_i \in F_2$ and $0\le i\le 4$. From $0=\overline{E}_0(1)=a+\sum_{i=0}^{4}a_ie_i(1)=a+\left(\frac{p-1}{5}\right)\sum_{i=0}^{4}a_i\equiv a \pmod 2$ it follows that $\overline{E}_0(x)=\sum_{i=0}^{4}a_ie_i(x)$. Let α be a primitive p-th root of unity in F_{2^m} as before. Note that each $e_i(x)$ is an idempotent. Thus, we have $e_i(\alpha)=0$ or 1 and $e_0(\alpha)+e_1(\alpha)+e_2(\alpha)+e_3(\alpha)+e_4(\alpha)=1$. Thus the number of 1 among $e_0(\alpha), e_1(\alpha), e_2(\alpha), e_3(\alpha), e_4(\alpha)$ is odd. We have to consider three cases.

Case 1: $e_0(\alpha)=e_1(\alpha)=e_2(\alpha)=e_3(\alpha)=e_4(\alpha)=1$.

Since $0=\overline{E}_0(\alpha)=\sum_{i=0}^{4}a_ie_i(\alpha)=\sum_{i=0}^{4}a_i$, the number of 1 among a_0, a_1, a_2, a_3, a_4 is even. If $a_i=a_j=1, i\ne j$, and the others $a_k=0$, where $i,j,k\in\{0,1,2,3,4\}$, then $\overline{E}_0(x)=e_i(x)+e_j(x)$.

$\forall b=\rho^{5k+1}\in R_1$, $1=\overline{E}_0(\alpha^b)=e_{i+1(\mathrm{mod}\,5)}(\alpha)+e_{j+1(\mathrm{mod}\,5)}(\alpha)=1+1=0$, a contradiction, where the subscript is the smallest nonnegative residue modulo 5. If $a_i=a_j=a_k=a_l=1$ and the other $a_h=0$, where $\{i,j,k,l,h\}=\{0,1,2,3,4\}$, then $\overline{E}_0(x)=e_i(x)+e_j(x)+e_k(x)+e_l(x)$, $\forall b=\rho^{5k+1}\in R_1$ $1=\overline{E}_0(\alpha^b)=e_{i+1(\mathrm{mod}\,5)}(\alpha)+e_{j+1(\mathrm{mod}\,5)}(\alpha)+e_{k+1(\mathrm{mod}\,5)}(\alpha)+e_{l+1(\mathrm{mod}\,5)}(\alpha)=1+1+1+1=0$, a contradiction. Thus, Case 1 is impossible.

Case 2: One of $e_0(\alpha), e_1(\alpha), e_2(\alpha), e_3(\alpha), e_4(\alpha)$ is 1, the others are 0.

Let $e_i(\alpha)=1, e_{i+1(\mathrm{mod}\,5)}(\alpha)=e_{i+2(\mathrm{mod}\,5)}(\alpha)=e_{i+3(\mathrm{mod}\,5)}(\alpha)=e_{i+4(\mathrm{mod}\,5)}(\alpha)=0, 0\le i\le 4$, where the subscript is the smallest nonnegative residue modulo 5. Since $0=\overline{E}_0(\alpha)=a_i$, $\forall b=\rho^{5k+1}\in R_1$ $1=\overline{E}_0(\alpha^b)=a_{i+4(\mathrm{mod}\,5)}$, $\forall c=\rho^{5k+2}\in R_2$ $1=\overline{E}_0(\alpha^c)=a_{i+3(\mathrm{mod}\,5)}$, $\forall d=\rho^{5k+3}\in R_3$ $1=\overline{E}_0(\alpha^d)=a_{i+2(\mathrm{mod}\,5)}$, $\forall e=\rho^{5k+4}\in R_4$ $1=\overline{E}_0(\alpha^e)=a_{i+1(\mathrm{mod}\,5)}$, we have $a_i=0$, $a_{i+1(\mathrm{mod}5)}=a_{i+2(\mathrm{mod}5)}$ $=a_{i+3(\mathrm{mod}5)}=a_{i+4(\mathrm{mod}5)}=1$. Therefore $\overline{E}_0(x)=e_{i+1(\mathrm{mod}\,5)}(x)+e_{i+2(\mathrm{mod}\,5)}(x)+e_{i+3(\mathrm{mod}\,5)}(x)+e_{i+4(\mathrm{mod}\,5)}(x)$.

By lemma 6 we get that the generating idempotent of the quintic residue code C_0 is $E_0(x)=1+e_i(x)$. By lemma 7, the set of generating idempotents of the quintic residue codes C_0, C_1, C_2, C_3, C_4 is $\{1+e_0(x), 1+e_1(x), 1+e_2(x), 1+e_3(x), 1+e_4(x)\}$, the set of generating idempotents of

$\overline{C}_0,\overline{C}_1,\overline{C}_2,\overline{C}_3,\overline{C}_3,\overline{C}_4$ is $\{e_1(x)+e_2(x)+e_3(x)+e_4(x),\ e_0(x)+e_2(x)+e_3(x)+e_4(x),\ e_0(x)+e_1(x)+e_3(x)+e_4(x),$ $e_0(x)+e_1(x)+e_2(x)+e_4(x),\ e_0(x)+e_1(x)+e_2(x)+e_3(x)\}$.

Case 3: Three of $e_0(\alpha),e_1(\alpha),e_2(\alpha),e_3(\alpha),e_4(\alpha)$ are 1,and the other two are 0.

①Let $e_i(\alpha)=e_{i+1(\bmod 5)}(\alpha)=0,e_{i+2(\bmod 5)}(\alpha)=e_{i+3(\bmod 5)}(\alpha)=e_{i+4(\bmod 5)}(\alpha)=1,0\le i\le 4$.Then $0=\overline{E}_0(\alpha)=a_{i+2(\bmod 5)}+a_{i+3(\bmod 5)}+a_{i+4(\bmod 5)}$, $\forall b=\rho^{5k+1}\in R_1$ $1=\overline{E}_0(\alpha^b)=a_{i+1(\bmod 5)}+a_{i+2(\bmod 5)}$ $+a_{i+3(\bmod 5)}$, $\forall c=\rho^{5k+2}\in R_2$ $1=\overline{E}_0(\alpha^c)=a_{i(\bmod 5)}+a_{i+1(\bmod 5)}+a_{i+2(\bmod 5)}$, $\forall d=\rho^{5k+3}\in R_3$ $1=\overline{E}_0(\alpha^d)=a_{i(\bmod 5)}+a_{i+1(\bmod 5)}+a_{i+4(\bmod 5)}$, $\forall e=\rho^{5k+4}\in R_4$ $1=\overline{E}_0(\alpha^e)=a_{i(\bmod 5)}+a_{i+3(\bmod 5)}+a_{i+4(\bmod 5)}$. By solving system of linear equations in 5 unknowns $a_{i(\bmod 5)},a_{i+1(\bmod 5)},a_{i+2(\bmod 5)},a_{i+3(\bmod 5)},a_{i+4(\bmod 5)}$ we get $a_i=a_{i+1(\bmod 5)}=a_{i+3(\bmod 5)}=0,a_{i+2(\bmod 5)}=a_{i+4(\bmod 5)}=1$ and $\overline{E}_0(x)=e_{i+2(\bmod 5)}(x)+e_{i+4(\bmod 5)}(x)$.

By lemma 6 we get that the generating idempotent of the quintic residue code C_0 is $E_0(x)=1+e_i(x)+e_{i+1(\bmod 5)}(x)+e_{i+3(\bmod 4)}(x)$. By lemma 7,the set of generating idempotents of the quintic residue codes C_0,C_1,C_2,C_3,C_4 is $\{1+e_0(x)+e_1(x)+e_3(x),\ 1+e_1(x)+e_2(x)+e_4(x),$ $1+e_0(x)+e_2(x)+e_3(x),\ 1+e_1(x)+e_3(x)+e_4(x),\ 1+e_0(x)+e_2(x)+e_4(x)\}$ and the set of generating idempotents of $\overline{C}_0,\overline{C}_1,\overline{C}_2,\overline{C}_3,\overline{C}_3,\overline{C}_4$ is $\{e_2(x)+e_4(x),\ e_0(x)+e_3(x),e_1(x)+e_4(x),e_0(x)+e_2(x),e_1(x)+e_3(x)\}$.

② Let $e_i(\alpha)=e_{i+2(\bmod 5)}(\alpha)=0,e_{i+1(\bmod 5)}(\alpha)=e_{i+3(\bmod 5)}(\alpha)=e_{i+4(\bmod 5)}(\alpha)=1,0\le i\le 4$. Then $0=\overline{E}_0(\alpha)=a_{i+1(\bmod 5)}+a_{i+3(\bmod 5)}+a_{i+4(\bmod 5)}$, $\forall b=\rho^{5k+1}\in R_1$ $1=\overline{E}_0(\alpha^b)=a_{i(\bmod 5)}+a_{i+2(\bmod 5)}+$ $a_{i+3(\bmod 5)}$, $\forall c=\rho^{5k+2}\in R_2$ $1=\overline{E}_0(\alpha^c)=a_{i+1(\bmod 5)}+a_{i+2(\bmod 5)}+a_{i+4(\bmod 5)}$, $\forall d=\rho^{5k+3}\in R_3$ $1=\overline{E}_0(\alpha^d)=a_{i(\bmod 5)}+a_{i+1(\bmod 5)}+a_{i+3(\bmod 5)}$, $\forall e=\rho^{5k+4}\in R_4$ $1=\overline{E}_0(\alpha^e)=a_{i(\bmod 5)}+a_{i+2(\bmod 5)}+a_{i+4(\bmod 5)}$.

By solving system of linear equations in 5 unknowns $a_{i(\bmod 5)},a_{i+1(\bmod 5)},a_{i+2(\bmod 5)},a_{i+3(\bmod 5)},a_{i+4(\bmod 5)}$ we get $a_i=a_{i+1(\bmod 5)}=a_{i+2(\bmod 5)}=0,a_{i+3(\bmod 5)}=a_{i+4(\bmod 5)}=1$,and $\overline{E}_0(x)=e_{i+3(\bmod 5)}(x)+e_{i+4(\bmod 5)}(x)$. By lemma 6 we get that the generating idempotent of the quintic residue code C_0 is $E_0(x)=1+e_i(x)+e_{i+1(\bmod 5)}(x)+e_{i+2(\bmod 4)}(x)$.By lemma 7,the set of generating idempotents of the quintic residue codes C_0,C_1,C_2,C_3,C_4 is $\{1+e_0(x)+e_1(x)+e_2(x),\ 1+e_1(x)+e_2(x)+e_3(x),$ $1+e_2(x)+e_3(x)+e_4(x),\ 1+e_0(x)+e_3(x)+e_4(x),\ 1+e_0(x)+e_1(x)+e_4(x)\}$,the set of generating idempotents of $\overline{C}_0,\overline{C}_1,\overline{C}_2,\overline{C}_3,\overline{C}_3,\overline{C}_4$ is $\{e_3(x)+e_4(x),\ e_0(x)+e_4(x),e_0(x)+e_1(x),e_1(x)+e_2(x),e_2(x)+e_3(x)\}$.

③Let $e_i(\alpha)=e_{i+3(\bmod 5)}(\alpha)=0,e_{i+1(\bmod 5)}(\alpha)=e_{i+2(\bmod 5)}(\alpha)=e_{i+4(\bmod 5)}(\alpha)=1,0\le i\le 4$.Then $0=\overline{E}_0(\alpha)=a_{i+1(\bmod 5)}+a_{i+2(\bmod 5)}+a_{i+4(\bmod 5)}$, $\forall b=\rho^{5k+1}\in R_1$ $1=\overline{E}_0(\alpha^b)=a_{i(\bmod 5)}+a_{i+1(\bmod 5)}+$ $a_{i+3(\bmod 5)}$, $\forall c=\rho^{5k+2}\in R_2$ $1=\overline{E}_0(\alpha^c)=a_{i(\bmod 5)}+a_{i+2(\bmod 5)}+a_{i+4(\bmod 5)}$, $\forall d=\rho^{5k+3}\in R_3$ $1=\overline{E}_0(\alpha^d)$ $=a_{i+1(\bmod 5)}+a_{i+3(\bmod 5)}+a_{i+4(\bmod 5)}$, $\forall e=\rho^{5k+4}\in R_4$ $1=\overline{E}_0(\alpha^e)=a_{i(\bmod 5)}+a_{i+2(\bmod 5)}+a_{i+3(\bmod 5)}$.

By solving system of linear equations in 5 unknowns $a_{i(\bmod 5)},a_{i+1(\bmod 5)},a_{i+2(\bmod 5)},a_{i+3(\bmod 5)},a_{i+4(\bmod 5)}$ we get $a_i=a_{i+3(\bmod 5)}=a_{i+4(\bmod 5)}=0,a_{i+1(\bmod 5)}=a_{i+2(\bmod 5)}=1$ .Thus $\overline{E}_0(x)=e_{i+1(\bmod 5)}(x)+e_{i+2(\bmod 5)}(x)$. By lemma 7,the set of generating idempotents of the quintic residue codes C_0,C_1,C_2,C_3,C_4 is

$\{1+e_0(x)+e_1(x)+e_2(x),\ 1+e_1(x)+e_2(x)\ +e_3(x),\ 1+e_2(x)+e_3(x)+e_4(x),\ 1+e_0(x)+e_3(x)+e_4(x),$ $1+e_0(x)+e_1(x)+e_4(x)\}$,the set of generating idempotents of $\overline{C}_0,\overline{C}_1,\overline{C}_2,\overline{C}_3,\overline{C}_3,\overline{C}_4$ is $\{e_3(x)+e_4(x),\ e_0(x)+e_4(x), e_0(x)+e_1(x), e_1(x)+e_2(x), e_2(x)+e_3(x)\}$.

④Let $e_i(\alpha)=e_{i+4(\mathrm{mod}5)}(\alpha)=0, e_{i+1(\mathrm{mod}5)}(\alpha)=e_{i+2(\mathrm{mod}5)}(\alpha)=e_{i+3(\mathrm{mod}5)}(\alpha)=1, 0\le i\le 4$ .Then $0=\overline{E}_0(\alpha)=a_{i+1(\mathrm{mod}5)}+a_{i+2(\mathrm{mod}5)}+a_{i+3(\mathrm{mod}5)}$, $\forall b=\rho^{5k+1}\in R_1\ 1=\overline{E}_0(\alpha^b)=a_{i(\mathrm{mod}5)}+a_{i+1(\mathrm{mod}5)}+$ $a_{i+2(\mathrm{mod}5)}$, $\forall c=\rho^{5k+2}\in R_2\ 1=\overline{E}_0(\alpha^c)=a_{i(\mathrm{mod}5)}+a_{i+1(\mathrm{mod}5)}+a_{i+4(\mathrm{mod}5)}$, $\forall d=\rho^{5k+3}\in R_3\ 1=\overline{E}_0(\alpha^d)$ $=a_{i(\mathrm{mod}5)}+a_{i+3(\mathrm{mod}5)}+a_{i+4(\mathrm{mod}5)}$, $\forall e=\rho^{5k+4}\in R_4\ \ 1=\overline{E}_0(\alpha^e)=a_{i+2(\mathrm{mod}5)}+a_{i+3(\mathrm{mod}5)}+a_{i+4(\mathrm{mod}5)}$ .By solving system of linear equations in 5 unknowns $a_{i(\mathrm{mod}5)}, a_{i+1(\mathrm{mod}5)}, a_{i+2(\mathrm{mod}5)}, a_{i+3(\mathrm{mod}5)}, a_{i+4(\mathrm{mod}5)}$ we get $a_i=a_{i+2(\mathrm{mod}5)}=a_{i+4(\mathrm{mod}5)}=0, a_{i+1(\mathrm{mod}5)}=a_{i+3(\mathrm{mod}5)}=1$, $\overline{E}_0(x)=e_{i+3(\mathrm{mod}5)}(x)+e_{i+1(\mathrm{mod}5)}(x)$ .By lemma 7,the set of generating idempotents of the quintic residue codes C_0,C_1,C_2,C_3,C_4 is $\{1+e_0(x)+e_1(x)+e_3(x),\ 1+e_1(x)+e_2(x)\ \ +e_4(x),\ 1+e_0(x)+e_2(x)+e_3(x),\ 1+e_1(x)+e_3(x)+e_4(x),$ $1+e_0(x)+e_2(x)+e_4(x)\}$,and the set of generating idempotents of $\overline{C}_0,\overline{C}_1,\overline{C}_2,\overline{C}_3,\overline{C}_3,\overline{C}_4$ is $\{e_2(x)+e_4(x),\ e_0(x)+e_3(x), e_1(x)+e_4(x), e_0(x)+e_2(x), e_1(x)+e_3(x)\}$.

Summary

This paper gives generating idempotents of quintic residue codes over the binary field. The generating polynomials of quintic residue codes over the binary field can be obtained by computing the greatest common divisors of these generating idempotents and the polynomial x^n-1 with computer software such as Matlab and Maple.

Acknowledgements

This research was financially supported by the Research Project of Liaoning Education Bureau under Project Code L2014490.

References

[1] E.Prange, I.S.Reed and T.K.Truong, Air Force Cambridge Research Center, Cambridge, 2(1958)58-156.

[2] F.J.Macwilliams,N.J.A.Sloane, The Theory of Error-Correcting Codes ,Amsterdam,the Netherlands:North-Holland,1977.

[3] T.C.Lin, H.P.Lee, H.C.Chang, T.K.Truong, A cyclic weight algorithm of decoding the (47, 24, 11) quadratic residue code, Information Sciences, 197(2012)215-222.

[4] P. Charters, Generalizing binary quadratic residue codes to higher power residues over larger fields, Finite Fields and Their Applications, 15(2009)404-413.

[5] X.Dong,J.Gao and L.Yang, On cubic residue codes(in Chinese),Journal of Liaoning Normal University,25(2002)1-2.

[6] S.Zhu and A.Chen, On cubic residue codes over the binary field(in Chinese), Acta Electronic Sinica, 36(2008)2312-2314.

[7] X.Dong, W.Li and Y.Zhang, Generating idempotents of cubic and quartic residue codes over the binary field (in Chinese),Computer Engineering and Applications, 49(2013)41-44.

[8] X.Dong, Yao Zhang and Yan Zhang, Generating idempotents of cubic and quartic residue codes over the field F_3 (in Chinese), Computer Engineering and Applications,50(2014)113-117.

[9] X.Dong, Generating idempotents of cubic residue codes over the field F_4 , Applied Mechanics and Materials, 385-386 (2013)1797-1800.

[10] W.C.Huffman and V.Pless, Fundamentals of Error Correcting Codes,Cambridge University Press, 2003.