Advances in Computer Science Research (ACSR), volume 61
7th International Conference on Education, Management, Computer and Society (EMCS 2017)

Generating Idempotents of Sixth Residue Codes over the Binary Field (II)

Xuedong Dong[1, a*] and Yan Zhang [2]

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

[2]School of Mathematics, Liaoning Normal University, Dalian 116029, P.R China

[a]dongxuedong@sina.com

[*]The corresponding author

Keywords: Generating idempotent, Residue code, Cyclic code

Abstract. This paper gives explicit expressions of generating idempotents of sixth residue codes of length p over the binary field, where p is a prime with $p \equiv 7 \pmod{24}$. By computing the greatest common divisors of these generating idempotents and the polynomial $x^p - 1$ with computer software such as Matlab and Maple, one can get the generating polynomials of sixth residue codes over the binary field.

Introduction

Prange [1] introduced the class of quadratic residue codes in 1958. 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 [6-7], generating idempotents of cubic and quartic residue codes over the fields F_2 and F_3 were given. In [8], generating idempotents of quintic residue codes over the binary field F_2 were given. In [9], explicit expressions of generating idempotents of some sixth residue codes of length p over the binary field were given, where p is a prime with $p \equiv 1 \pmod{24}$. This paper gives explicit expressions of generating idempotents of sixth residue codes of length p over the binary field, where p is a prime with $p \equiv 7 \pmod{24}$. Thus, the generating polynomials of sixth residue codes over the binary field can be obtained by computing the greatest common divisors of these generating idempotents and the polynomial $x^p - 1$ 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 some sixth 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 $x^6 \equiv a \pmod{p}$, where $a \in Z$ and $(a, p) = 1$,then a is called a sixth residue modulo p.

In the following we assume that ρ is a primitive element of the finite field F_p. Let $R_0=\{\rho^{tk}\in F_P \mid k\in Z\}$, $R_1=\{\rho^{tk+1}\in F_P \mid k\in Z\}$, $\cdots, R_{t-1}=\{\rho^{tk+(t-1)}\in F_P \mid k\in Z\}$. Let m be the smallest positive integer such that $2^m\equiv 1(\bmod p)$, α a primitive p-th root of unity in F_{2^m}, and $g_0(x)=\prod_{r_0\in R_0}(x-\alpha^{r_0})$ $g_1(x)=\prod_{r_1\in R_1}(x-\alpha^{r_1})\cdots, g_{t-1}(x)=\prod_{r_{t-1}\in R_{t-1}}(x-\alpha^{r_{t-1}})$

Lemma 1. $x^p-1=(x-1)g_0(x)\cdots g_{t-1}(x)$ and $g_j(x)=\prod_{r_j\in R_j}(x-\alpha^{r_j})\in F_2[x]$ 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 $e(x)\in F_2[x]/(x^p-1)$ satisfying $e(x)^2\equiv e(x)(\bmod(x^p-1))$ 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 $e(x)\ \mu_a$ 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. [7] If $\overline{E}_0(x)$ is the generating idempotent of the sixth 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.

Lemma 7. [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 $\overline{C}_1, \cdots, \overline{C}_{t-1}$.

Generating Idempotents of Some Sixth Residue Codes

*Theorem 1.*Let $p \equiv 7 \pmod{24}$,and 2 be a sixth residue modulo p. Then the set of the generating idempotents of
$\overline{C}_0, \overline{C}_1, \overline{C}_2, \overline{C}_3, \overline{C}_3, \overline{C}_4, \overline{C}_5$ is $\{1+e_0(x), 1+e_1(x), 1+e_2(x), 1+e_3(x), 1+e_4(x), 1+e_5(x)\}$ or
$\{1+e_1(x)+e_2(x)+e_5(x), 1+e_0(x)+e_2(x)+e_3(x), 1+e_1(x)+e_3(x)+e_4(x), 1+e_2(x)+$
$e_4(x)+e_5(x), 1+e_0(x)+e_3(x)+e_5(x), 1+e_0(x)+e_1(x)+e_4(x)\}$ or
$\{1+e_0(x)+e_2(x)+e_5(x), 1+e_0(x)+e_1(x)+e_3(x), 1+e_1(x)+e_2(x)+e_4(x), 1+e_2(x)+e_3(x)+e_5(x),$
$1+e_0(x)+e_4(x)+e_5(x), 1+e_1(x)+e_4(x)+e_5(x)\}$ or $\{1+e_1(x)+e_2(x)+e_3(x)+e_4(x)+e_5(x),$
$1+e_0(x)+e_2(x)+e_3(x)+e_4(x)+e_5(x),$
$1+e_0(x)+e_1(x)+e_3(x)+e_4(x)+e_5(x), 1+e_0(x)+e_1(x)+e_2(x)+e_4(x)+e_5(x),$
$1+e_0(x)+e_1(x)+e_2(x)+e_3(x)+e_5(x), 1+e_0(x)+e_1(x)+e_2(x)+e_3(x)+e_4(x)\}$.

Proof: Since $p \equiv 7 \pmod{24}$ it is clear that $(p-1)/6$ is odd and therefore $(p-1)/6 = 1$ over F_2.

By Lemma 5 assume that $\overline{E}_0(x) = a + \sum_{i=0}^{5} a_i e_i(x)$ is the generating idempotent of the residue code $\overline{C}_0$, where $a, a_i \in F_2, 0 \le i \le 5$. It is clear that

$$0 = \overline{E}_0(1) = a + \sum_{i=0}^{5} a_i e_i(1) = a + \left(\frac{p-1}{6}\right)\sum_{i=0}^{5} a_i \equiv a + \sum_{i=0}^{5} a_i \pmod 2. \quad (1)$$

Let α a primitive p-th root of unity in F_{2^m} as before. Since 2 is a sixth residue modulo p ,we deduce that each $e_i(x)$is an idempotent.Thus we have that $e_i(\alpha) = 0$ or 1 and $e_0(\alpha)+e_1(\alpha)+e_2(\alpha)+e_3(\alpha)+e_4(x)+e_5(x) = 1$.Thus the number of 1 among $e_0(\alpha), e_1(\alpha), e_2(\alpha), e_3(\alpha), e_4(\alpha), e_5(x)$ is odd. We will consider three cases in the following.

Case 1: One of $e_0(\alpha), e_1(\alpha), e_2(\alpha), e_3(\alpha), e_4(\alpha), e_5(x)$ is 1 and the others are 0.

Let $e_i(\alpha) = 1, e_{i+1(\bmod 6)}(\alpha) = e_{i+2(\bmod 6)}(\alpha) = e_{i+3(\bmod 6)}(\alpha) = e_{i+4(\bmod 6)}(\alpha) = e_{i+5(\bmod 6)}(\alpha) = 0$, $0 \le i \le 5$, where the subscript is the smallest nonnegative residue modulo 6.Then

$$0 = \overline{E}_0(\alpha) = a + a_i \quad (2)$$

$$\forall b = \rho^{6k+1} \in R_1\ 1 = \overline{E}_0(\alpha^b) = a + a_{i+5(\bmod 6)} \quad (3)$$

$$\forall c = \rho^{6k+2} \in R_2\ 1 = \overline{E}_0(\alpha^c) = a + a_{i+4(\bmod 6)} \quad (4)$$

$$\forall d = \rho^{6k+3} \in R_3\ 1 = \overline{E}_0(\alpha^d) = a + a_{i+3(\bmod 6)} \quad (5)$$

$$\forall e = \rho^{6k+4} \in R_4\ 1 = \overline{E}_0(\alpha^e) = a + a_{i+2(\bmod 6)} \quad (6)$$

$$\forall f = \rho^{6k+5} \in R_5\ 1 = \overline{E}_0(\alpha^f) = a + a_{i+1(\bmod 6)} \quad (7)$$

From equations (1)-(7) it follows that $a = 1, a_i = 1, a_{i+1(\bmod 6)} = a_{i+2(\bmod 6)} = a_{i+3(\bmod 6)} = a_{i+4(\bmod 6)} = a_{i+5(\bmod 6)} = 0, 0 \le i \le 5$, $\overline{E}_0(x) = 1 + e_i(x)$. By lemma 7,the set of generating idempotents of the sixth residue codes $\overline{C}_0, \overline{C}_1, \overline{C}_2, \overline{C}_3, \overline{C}_3, \overline{C}_4, \overline{C}_5$ is $\{1+e_0(x), 1+e_1(x), 1+e_2(x), 1+e_3(x), 1+e_4(x), 1+e_5(x)\}$.

Case 2: Three of $e_0(\alpha), e_1(\alpha), e_2(\alpha), e_3(\alpha), e_4(\alpha), e_5(x)$ are 1 and the other three are 0.

1) .Let $e_i(\alpha)=e_{i+1(\bmod 6)}(\alpha)=e_{i+2(\bmod 6)}(\alpha)=1, e_{i+3(\bmod 6)}(\alpha)=e_{i+4(\bmod 6)}(\alpha)=e_{i+5(\bmod 6)}(\alpha)=0, 0\le i\le 5$,Then

$$0=\overline{E}_0(\alpha)=a+a_i+a_{i+1(\bmod 6)}+a_{i+2(\bmod 6)} \quad (8)$$

$$\forall b=\rho^{6k+1}\in R_1\ 1=\overline{E}_0(\alpha^b)=a+a_i+a_{i+1(\bmod 6)}+a_{i+5(\bmod 6)} \quad (9)$$

$$\forall c=\rho^{6k+2}\in R_2\ 1=\overline{E}_0(\alpha^c)=a+a_i+a_{i+4(\bmod 6)}+a_{i+5(\bmod 6)} \quad (10)$$

$$\forall d=\rho^{6k+3}\in R_3\ 1=\overline{E}_0(\alpha^d)=a+a_{i+3(\bmod 6)}+a_{i+4(\bmod 6)}+a_{i+5(\bmod 6)} \quad (11)$$

$$\forall e=\rho^{6k+4}\in R_4\ 1=\overline{E}_0(\alpha^e)=a+a_{i+2(\bmod 6)}+a_{i+3(\bmod 6)}+a_{i+4(\bmod 6)} \quad (12)$$

$$\forall f=\rho^{6k+5}\in R_5\ 1=\overline{E}_0(\alpha^f)=a+a_{i+1(\bmod 6)}+a_{i+2(\bmod 6)}+a_{i+3(\bmod 6)} \quad (13)$$

From (8)+(13)it follows that $a_i+a_{i+3(\bmod 6)}=1$, from(10)+(11) it follows that $a_i+a_{i+3(\bmod 6)}=0$,a contradiction.

2).Let $e_i(\alpha)=e_{i+1(\bmod 6)}(\alpha)=e_{i+3(\bmod 6)}(\alpha)=1, e_{i+2(\bmod 6)}(\alpha)=e_{i+4(\bmod 6)}(\alpha)=e_{i+5(\bmod 6)}(\alpha)=0$, $0\le i\le 5$. Then

$$0=\overline{E}_0(\alpha)=a+a_i+a_{i+1(\bmod 6)}+a_{i+3(\bmod 6)} \quad (14)$$

$$\forall b=\rho^{6k+1}\in R_1\ 1=\overline{E}_0(\alpha^b)=a+a_i+a_{i+2(\bmod 6)}+a_{i+5(\bmod 6)} \quad (15)$$

$$\forall c=\rho^{6k+2}\in R_2\ 1=\overline{E}_0(\alpha^c)=a+a_{i+1(\bmod 6)}+a_{i+4(\bmod 6)}+a_{i+5(\bmod 6)} \quad (16)$$

$$\forall d=\rho^{6k+3}\in R_3\ 1=\overline{E}_0(\alpha^d)=a+a_i+a_{i+3(\bmod 6)}+a_{i+4(\bmod 6)} \quad (17)$$

$$\forall e=\rho^{6k+4}\in R_4\ 1=\overline{E}_0(\alpha^e)=a+a_{i+2(\bmod 6)}+a_{i+3(\bmod 6)}+a_{i+5(\bmod 6)} \quad (18)$$

$$\forall f=\rho^{6k+5}\in R_5\ 1=\overline{E}_0(\alpha^f)=a+a_{i+1(\bmod 6)}+a_{i+2(\bmod 6)}+a_{i+4(\bmod 6)} \quad (19)$$

By solving system of linear equations in 6 unknowns $a_{i(\bmod 5)}, a_{i+1(\bmod 5)}, a_{i+2(\bmod 5)}, a_{i+3(\bmod 5)}, a_{i+4(\bmod 5)}$, $a_{i+5(\bmod 6)}$ from (1) and (14)-(19) we get that $a=1, a_i=0, a_{i+1(\bmod 6)}=1, a_{i+2(\bmod 6)}=1, a_{i+3(\bmod 6)}=0, a_{i+4(\bmod 6)}=0, a_{i+5(\bmod 6)}=1, 0\le i\le 5, \overline{E}_0(x)=1+e_{i+1(\bmod 6)}(x)+e_{i+2(\bmod 6)}(x)+e_{i+5(\bmod 6)}(x)$.

By lemma 7,the set of generating idempotents of the sixth residue codes $\overline{C}_0, \overline{C}_1, \overline{C}_2, \overline{C}_3, \overline{C}_3, \overline{C}_4, \overline{C}_5$ is

$\{1+e_1(x)+e_2(x)+e_5(x), 1+e_0(x)+e_2(x)+e_3(x), 1+e_1(x)+e_3(x)+e_4(x),$
$1+e_2(x)+e_4(x)+e_5(x), 1+e_0(x)+e_3(x)+e_5(x), 1+e_0(x)+e_1(x)+e_4(x)\}$

3).Let $e_i(\alpha)=e_{i+1(\bmod 6)}(\alpha)=e_{i+4(\bmod 6)}(\alpha)=1, e_{i+2(\bmod 6)}(\alpha)=e_{i+3(\bmod 6)}(\alpha)=e_{i+5(\bmod 6)}(\alpha)=0, 0\le i\le 5$. Then

$$0=\overline{E}_0(\alpha)=a+a_i+a_{i+1(\bmod 6)}+a_{i+4(\bmod 6)} \quad (20)$$

$$\forall b=\rho^{6k+1}\in R_1\ 1=\overline{E}_0(\alpha^b)=a+a_i+a_{i+3(\bmod 6)}+a_{i+5(\bmod 6)} \quad (21)$$

$$\forall c=\rho^{6k+2}\in R_2\ 1=\overline{E}_0(\alpha^c)=a+a_{i+2(\bmod 6)}+a_{i+4(\bmod 6)}+a_{i+5(\bmod 6)} \quad (22)$$

$$\forall d=\rho^{6k+3}\in R_3\ 1=\overline{E}_0(\alpha^d)=a+a_{i+1(\bmod 6)}+a_{i+3(\bmod 6)}+a_{i+4(\bmod 6)} \quad (23)$$

$$\forall e=\rho^{6k+4}\in R_4\ 1=\overline{E}_0(\alpha^e)=a+a_i+a_{i+2(\bmod 6)}+a_{i+3(\bmod 6)} \tag{24}$$

$$\forall f=\rho^{6k+5}\in R_5\ 1=\overline{E}_0(\alpha^f)=a+a_{i+1(\bmod 6)}+a_{i+2(\bmod 6)}+a_{i+5(\bmod 6)} \tag{25}$$

By solving system of linear equations in 6 unknowns $a_{i(\bmod 5)}, a_{i+1(\bmod 5)}, a_{i+2(\bmod 5)}, a_{i+3(\bmod 5)}, a_{i+4(\bmod 5)}$, $a_{i+5(\bmod 6)}$ from (1) and (20)-(25) we get that $a=1, a_i=1, a_{i+1(\bmod 6)}=0, a_{i+2(\bmod 6)}=1, a_{i+3(\bmod 6)}=0, a_{i+4(\bmod 6)}=0, a_{i+5(\bmod 6)}=1, 0\le i\le 5, \overline{E}_0(x)=1+e_i(x)+e_{i+2(\bmod 6)}(x)+e_{i+5(\bmod 6)}(x)$. By lemma 7,the set of generating idempotents of the sixth residue codes $\overline{C}_0, \overline{C}_1, \overline{C}_2, \overline{C}_3, \overline{C}_3, \overline{C}_4, \overline{C}_5$ is

$\{1+e_0(x)+e_2(x)+e_5(x), 1+e_0(x)+e_1(x)+e_3(x), 1+e_1(x)+e_2(x)+e_4(x),$
$1+e_2(x)+e_3(x)+e_5(x), 1+e_0(x)+e_4(x)+e_5(x), 1+e_1(x)+e_4(x)+e_5(x)\}$

4).Let $e_i(\alpha)=e_{i+2(\bmod 6)}(\alpha)=e_{i+4(\bmod 6)}(\alpha)=1, e_{i+1(\bmod 6)}(\alpha)=e_{i+3(\bmod 6)}(\alpha)=e_{i+5(\bmod 6)}(\alpha)=0$, $0\le i\le 5$.

$$0=\overline{E}_0(\alpha)=a+a_i+a_{i+2(\bmod 6)}+a_{i+4(\bmod 6)} \tag{26}$$

$$\forall b=\rho^{6k+1}\in R_1\ 1=\overline{E}_0(\alpha^b)=a+a_{i+1(\bmod 6)}+a_{i+3(\bmod 6)}+a_{i+5(\bmod 6)} \tag{27}$$

$$\forall c=\rho^{6k+2}\in R_2\ 1=\overline{E}_0(\alpha^c)=a+a_i+a_{i+2(\bmod 6)}+a_{i+4(\bmod 6)} \tag{28}$$

(26) and (28) contradict each other.

Case 3:Five of $e_0(\alpha), e_1(\alpha), e_2(\alpha), e_3(\alpha), e_4(\alpha), e_5(x)$ are 1 and the other is 0.

Let $e_i(\alpha)=0, e_{i+2(\bmod 6)}(\alpha)=e_{i+1(\bmod 6)}(\alpha)=e_{i+3(\bmod 6)}(\alpha)=e_{i+4(\bmod 6)}(\alpha)=e_{i+5(\bmod 6)}(\alpha)=1,\ 0\le i\le 5$.Then

$$0=\overline{E}_0(\alpha)=a+a_{i+1(\bmod 6)}+a_{i+2(\bmod 6)}+a_{i+3(\bmod 6)}+a_{i+4(\bmod 6)}+a_{i+5(\bmod 6)} \tag{29}$$

$$\forall b=\rho^{6k+1}\in R_1\ 1=\overline{E}_0(\alpha^b)=a+a_i+a_{i+1(\bmod 6)}+a_{i+2(\bmod 6)}+a_{i+3(\bmod 6)}+a_{i+4(\bmod 6)} \tag{30}$$

$$\forall c=\rho^{6k+2}\in R_2\ 1=\overline{E}_0(\alpha^c)=a+a_i+a_{i+1(\bmod 6)}+a_{i+2(\bmod 6)}+a_{i+3(\bmod 6)}+a_{i+5(\bmod 6)} \tag{31}$$

$$\forall d=\rho^{6k+3}\in R_3\ 1=\overline{E}_0(\alpha^d)=a+a_i+a_{i+1(\bmod 6)}+,a_{i+2(\bmod 6)}+a_{i+4(\bmod 6)}+a_{i+5(\bmod 6)} \tag{32}$$

$$\forall e=\rho^{6k+4}\in R_4\ 1=\overline{E}_0(\alpha^e)=a+a_i+a_{i+1(\bmod 6)}+a_{i+3(\bmod 6)}+a_{i+4(\bmod 6)}+a_{i+5(\bmod 6)} \tag{33}$$

$$\forall f=\rho^{6k+5}\in R_5\ 1=\overline{E}_0(\alpha^f)=a+a_i+a_{i+2(\bmod 6)}+a_{i+3(\bmod 6)}+a_{i+4(\bmod 6)}+a_{i+5(\bmod 6)} \tag{34}$$

By solving system of linear equations in 6 unknowns $a_{i(\bmod 5)}, a_{i+1(\bmod 5)}, a_{i+2(\bmod 5)}, a_{i+3(\bmod 5)}, a_{i+4(\bmod 5)}$, $a_{i+5(\bmod 6)}$ from (1) and (29)-(34) we get

that $a=1, a_i=0, a_{i+1(\bmod 6)}=a_{i+2(\bmod 6)}=a_{i+3(\bmod 6)}=a_{i+4(\bmod 6)}=a_{i+5(\bmod 6)}=1, 0\le i\le 5$.

$\overline{E}_0(x)=1+e_{i+1(\bmod 6)}(x)+e_{i+2(\bmod 6)}(x)+e_{i+3(\bmod 6)}(x)+e_{i+4(\bmod 6)}(x)+e_{i+5(\bmod 6)}(x)$. By lemma 7,the set of generating idempotents of the sixth residue codes $\overline{C}_0, \overline{C}_1, \overline{C}_2, \overline{C}_3, \overline{C}_3, \overline{C}_4, \overline{C}_5$ is

$\{1+e_1(x)+e_2(x)+e_3(x)+e_4(x)+e_5(x), 1+e_0(x)+e_2(x)+e_3(x)$
$+e_4(x)+e_5(x), 1+e_0(x)+e_1(x)+e_3(x)+e_4(x)+e_5(x), 1+e_0(x)+e_1(x)+e_2(x)+e_4(x)+e_5(x),$
$1+e_0(x)+e_1(x)+e_2(x)+e_3(x)+e_5(x), 1+e_0(x)+e_1(x)+e_2(x)+e_3(x)+e_4(x)\}$.

Summary

We have given explicit expressions of generating idempotents of some sixth residue codes of length p over the binary field**,** where p is a prime with $p \equiv 7 \pmod{24}$. One can get the generating polynomials of sixth residue codes over the binary field by computing the greatest common divisors of these idempotents and $x^p - 1$ 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, Information Sciences, 197(2012)215-222.

[4] P. Charters,Finite Fields and Their Applications, 15(2009)404-413.

[5] S.Zhu and A.Chen, Acta Electronic Sinica, 36(2008)2312-2314.

[6] X.Dong, W.Li and Y.Zhang, Computer Engineering and Applications, 49(2013)41-44.

[7] X.Dong, Yao Zhang and Yan Zhang, Computer Engineering and applications, 50 (2014) 113-117.

[8] X.Dong, Advances in Intelligent Systems Research, 135(2016)357-362.

[9] X.Dong, Y. Zhang, Generating idempotents of sixth residue codes over the binary field,to be published.

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