Generating Idempotents of Sixth Residue Codes over the Binary Field

Xue-dong DONG¹,∗ and Yan ZHANG²

¹College of Information Engineering, Dalian University, Dalian 116622, P.R. China
²School of Mathematics, Liaoning Normal University, Dalian 116029, P.R. China

*Corresponding author

Keywords: Generating idempotent, Residue code, Cyclic code.

Abstract. Higher power residue codes over finite fields are generated by factors of the polynomial \( x^n - 1 \). Unfortunately, to decompose the polynomial \( x^n - 1 \) over finite fields is difficult. Generating idempotents can also generate higher power residue codes. Thus it is important to get generating idempotents of cyclic codes. We find precise expressions of generating idempotents of some sixth residue codes of length over the binary field, where \( p \) is a prime such that \( p \equiv 1 \pmod{24} \).

Introduction

There are many papers on quadratic residue codes and their generalizations [1-3]. In [4-9] higher power residue codes and forms of generating polynomials of these codes were investigated. Higher power residue codes are generated by factors of \( x^n - 1 \). Unfortunately, to decompose \( x^n - 1 \) over finite fields is difficult. We have to get the generating idempotents of higher power residue codes since generating polynomials of cyclic codes can be obtained by computing the GCD (greatest common divisors) of generating idempotents and \( x^n - 1 \) without factoring \( x^n - 1 \) over finite fields. Precise expressions of generating idempotents of cubic and quartic residue codes over the fields \( F_2 \) and \( F_3 \) were obtained respectively in [6] and [7]. Precise expressions of generating idempotents of quintic residue codes over \( F_2 \) were obtained in [9]. This paper gives generating idempotents of some sixth residue codes of length \( p \) over the binary field, where \( p \) is a prime such that \( p \equiv 1 \pmod{24} \).

The paper is organized as follows. We give preliminary results in Section 2. Generating idempotents of some sixth residue codes over the binary field are given in Section 3. Conclusions are given in Section 4.

Preliminaries

Definition 2.1. If \( x \) is an integer such that \( x^6 \equiv a \pmod{p} \), where \( a \in \mathbb{Z} \) and \( (a, p) = 1 \), then \( a \) is called a sixth residue modulo \( p \).

Let \( p \) be an odd prime and \( \rho \) a primitive element of the finite field \( F_p \) in the following.

\[
R_0 = \{ \rho^k \in F_p \mid k \in \mathbb{Z} \}, \quad R_1 = \{ \rho^{k+1} \in F_p \mid k \in \mathbb{Z} \}, \ldots, \quad R_{t-1} = \{ \rho^{k+(t-1)} \in F_p \mid k \in \mathbb{Z} \}.
\]

Assume that \( m \) is the smallest positive integer such that \( 2^m \equiv 1 \pmod{p} \), \( \alpha \) is a primitive \( p \)-th root of unity in \( F_{2^m} \), and

\[
g_0(x) = \prod_{i \in R_0} (x - \alpha^i), \quad g_1(x) = \prod_{i \in R_0} (x - \alpha^i), \ldots, \quad g_{t-1}(x) = \prod_{i \in R_{t-1}} (x - \alpha^i).
\]

Lemma 2.1. \( x^{p^j} - 1 = (x - 1) g_0(x) \cdots g_{t-1}(x) \) and \( g_j(x) = \prod_{i \in R_j} (x - \alpha^i) \in F_2[x] \) for \( j = 0, 1, 2, \ldots, t - 1 \).
Definition 2.2. [6] The $t$-th residue codes $C_0, \cdots, C_{t-1}, \bar{C}_0, \cdots, \bar{C}_{t-1}$ are cyclic codes of $F_q[x]/(x^p-1)$ 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 2.3. [10] If $E(x) \in F_2[x]/(x^p-1)$ and $E(x)^2 \equiv E(x) \pmod{(x^p-1)}$, then it is called an idempotent.

Definition 2.4. [10] The function $\mu_a$ is defined on $\{0, 1, \cdots, n-1\}$ by $i \mu_a \equiv ia \pmod{n}$, where $a$ is an integer with $(a, n) = 1$. $\mu_a$ acts on $F_p[x]/(x^n-1)$ by $f(x) \mu_a \equiv f(xa) \pmod{x^n-1}$, where $f(x) \in F_p[x]/(x^n-1)$.

Lemma 2.2. [10] If $C$ is a cyclic code of length $n$ over the finite field $F_q$ with generating idempotent $e(x)$, then the cyclic code $C \mu_a$ is generated by the generating idempotent $e(x) \mu_a$.

Lemma 2.3. [6] $C_0, \cdots, C_{t-1}$ are pairwise equivalent and $\bar{C}_0, \cdots, \bar{C}_{t-1}$ are pairwise equivalent.

In the following assume that $e_0(x) = \sum_{i=0}^{n-1} x^i e_i(x) = \sum_{i=0}^{n-1} x^i e_{r-1}(x) = \sum_{i=0}^{n-1} x^{i-r}$

Lemma 2.4. [6] $e_0(x) + e_1(x) + \cdots + e_{t-1}(x) + \sum_{i=0}^{n-1} x^i = 1$

Lemma 2.5. [6] Let $E(x)$ be the generating idempotent of a $t$-th residue code $C$. Then $E(x) = a + \sum_{i=0}^{t-1} a_i e_i(x)$, where $a, a_0, a_1, \cdots, a_{t-1} \in F_2$.

Lemma 2.6. [6] If $\bar{E}_0(x)$ is the generating idempotent of $\bar{C}_0$, then $E_0(x) = \bar{E}_0(x) + \sum_{i=0}^{n-1} x^i$ is the generating idempotent of $C_0$.

Lemma 2.7. [6] If $E_0(x)$ and $\bar{E}_0(x)$ are respectively the generating idempotents of $C_0$ and $\bar{C}_0$, and $d = \rho^{d_{t-1}} \in R_{t-1}$, then

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

2. $\bar{E}_0(x) \mu_d = \bar{E}_1(x), \bar{E}_1(x) \mu_d = \bar{E}_2(x), \cdots, \bar{E}_{r-2}(x) \mu_d = \bar{E}_{t-1}(x)$ are respectively generating idempotents of $\bar{C}_1, \cdots, \bar{C}_{t-1}$.

Generating Idempotents of Some Sixth Residue Codes

Let 2 be a sixth residue modulo $P$. Then there exists an integer $x$ such that $x^6 \equiv 2 \pmod{p}$. Thus, 2 is a quadratic residue modulo $P$. We have $p \equiv \pm 1 \pmod{8}$. If $p \equiv 1 \pmod{8}$ and $61 \equiv p-1$, then $p \equiv 1 \pmod{24}$. If $p \equiv -1 \pmod{8}$ and $61 \equiv p-1$, then $p \equiv 7 \pmod{24}$. The following theorem will determine the set of the generating idempotents of $\bar{C}_0, \bar{C}_1, \bar{C}_2, \bar{C}_3, \bar{C}_4, \bar{C}_5$. By Lemma 2.6 and Lemma 2.7 one can easily determine the set of the generating idempotents of $C_0, C_1, C_2, C_3, C_4, C_5$.

Theorem 3.1. Let $p \equiv 1 \pmod{24}$ and 2 be a sixth residue modulo $P$. Then the set of the generating idempotents of $\bar{C}_0, \bar{C}_1, \bar{C}_2, \bar{C}_3, \bar{C}_4, \bar{C}_5$ over $F_2$ is:

\[
\{e_1(x) + e_2(x) + e_3(x) + e_4(x) + e_5(x), e_0(x) + e_2(x) + e_4(x) + e_5(x), e_0(x) + e_1(x) + e_3(x),
+ e_2(x) + e_5(x), e_0(x) + e_1(x) + e_3(x) + e_5(x), e_0(x) + e_1(x) + e_4(x) + e_5(x), e_0(x) + e_2(x) + e_3(x) + e_4(x), e_0(x) + e_2(x) + e_3(x) + e_5(x) + e_1(x) + e_2(x) + e_3(x) + e_4(x) \}
\] or
\[
\{e_0(x) + e_3(x) + e_4(x), e_1(x) + e_4(x) + e_5(x), e_0(x) + e_3(x) + e_5(x), e_0(x) + e_2(x) + e_5(x) + e_1(x),
\]
\[ e_i(x) + e_2(x) + e_4(x), e_2(x) + e_3(x) + e_5(x) \] or \[ e_1(x) + e_3(x) + e_4(x), e_2(x) + e_4(x) + e_5(x), e_0(x) + e_3(x) + e_4(x) + e_5(x), e_1(x) + e_2(x) + e_4(x) + e_5(x), e_0(x) + e_2(x) + e_3(x), \]
eq_5 (\{e_0(x), e_1(x), e_2(x), e_3(x), e_4(x), e_5(x)\}).

**Proof:** From \( p \equiv 1 \pmod{24} \) it follows that \((p-1)/6\) is even and therefore \((p-1)/6 = 0\) over \(F_3\). By Lemma 2.5 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 \( a_i, a_j \in F_3, 0 \leq i \leq 5 \). Then \( 0 = \overline{E}_0(1) = a + \sum_{i=0}^{5} a_i e_i(1) = a + \left( \frac{p-1}{6} \right) \sum_{i=0}^{5} a_i \equiv a \pmod{2} \) and therefore \( \overline{E}_0(x) = \sum_{i=0}^{5} a_i e_i(x) \). Let \( \alpha \) be a primitive \( p \)-th root of unity in \( F_2^* \) as before. It is clear that each \( e_i(x) \) is an idempotent since \( 2 \) is a sixth residue modulo \( p \). Thus we have that \( e_0(\alpha) = 0 \) or \( 1 \) and \( e_0(\alpha) + e_1(\alpha) + e_2(\alpha) + e_3(\alpha) + e_4(\alpha) + e_5(\alpha) = 1 \), and the number of \( 1 \) among \( e_0(\alpha), e_1(\alpha), e_2(\alpha), e_3(\alpha), e_4(\alpha), e_5(\alpha) \) is odd. We have to consider three cases in the following.

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

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

\[ \begin{align*}
1 \in R_0, 0 = \overline{E}_0(\alpha) = a, \quad \forall b = \rho^{6k+1} \in R_1, 1 = \overline{E}_0(\alpha^b) = a_{i+5(\mod 6)}, \quad \forall c = \rho^{6k+2} \in R_2, \\
1 = \overline{E}_0(\alpha^c) = a_{i+6(\mod 6)}, \quad \forall d = \rho^{6k+3} \in R_3, 1 = \overline{E}_0(\alpha^d) = a_{i+3(\mod 6)}, \quad \forall e = \rho^{6k+4} \in R_4, \\
1 = \overline{E}_0(\alpha^e) = a_{i+2(\mod 6)}, \quad \forall f = \rho^{6k+5} \in R_5, 1 = \overline{E}_0(\alpha^f) = a_{i+1(\mod 6)}. \end{align*} \]

Thus \( a_i = 0, a_{i+1(\mod 6)} = a_{i+2(\mod 6)} = a_{i+3(\mod 6)} = a_{i+4(\mod 6)} = a_{i+5(\mod 6)} = 1, 0 \leq i \leq 5 \).

\[ \overline{E}_0(x) = e_{i+1(\mod 6)}(x) + e_{i+2(\mod 6)}(x) + e_{i+3(\mod 6)}(x) + e_{i+4(\mod 6)}(x) + e_{i+5(\mod 6)}(x), 0 \leq i \leq 5. \]

By Lemma 2.7, the set consisting of generating idempotents of \( \overline{C}_0, \overline{C}_1, \overline{C}_2, \overline{C}_3, \overline{C}_4, \overline{C}_5 \) is

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

\[ \{ e_0(x), e_1(x), e_2(x), e_3(x), e_4(x), e_5(x) \} \]

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

1) Let \( e_i(\alpha) = 1 \), \( e_{i+1(\mod 6)}(\alpha) = e_{i+2(\mod 6)}(\alpha) = 1, e_{i+3(\mod 6)}(\alpha) = e_{i+4(\mod 6)}(\alpha) = e_{i+5(\mod 6)}(\alpha) = 0 \), where \( 0 \leq i \leq 5 \). Then

\[ 0 = \overline{E}_0(\alpha) = a_i + a_{i+1(\mod 6)} + a_{i+2(\mod 6)} \quad (1) \]

\[ \forall b = \rho^{6k+1} \in R_1, 1 = \overline{E}_0(\alpha^b) = a_i + a_{i+1(\mod 6)} + a_{i+5(\mod 6)} \quad (2) \]

\[ \forall c = \rho^{6k+2} \in R_2, 1 = \overline{E}_0(\alpha^c) = a_i + a_{i+4(\mod 6)} + a_{i+5(\mod 6)} \quad (3) \]

\[ \forall d = \rho^{6k+3} \in R_3, 1 = \overline{E}_0(\alpha^d) = a_{i+3(\mod 6)} + a_{i+4(\mod 6)} + a_{i+5(\mod 6)} \quad (4) \]

\[ \forall e = \rho^{6k+4} \in R_4, 1 = \overline{E}_0(\alpha^e) = a_{i+2(\mod 6)} + a_{i+3(\mod 6)} + a_{i+4(\mod 6)} \quad (5) \]

\[ \forall f = \rho^{6k+5} \in R_5, 1 = \overline{E}_0(\alpha^f) = a_{i+1(\mod 6)} + a_{i+2(\mod 6)} + a_{i+3(\mod 6)} \quad (6) \]

235
From (1) + (6) it follows that \( a_i + a_{i+3(\text{mod} 6)} = 1 \). from (3)+(4) it follows that \( a_i + a_{i+3(\text{mod} 6)} = 0 \), a contradiction.

2) Let \( e_i(\alpha) = e_{i+1(\text{mod} 6)}(\alpha) = e_{i+3(\text{mod} 6)}(\alpha) = 1, e_{i+2(\text{mod} 6)}(\alpha) = e_{i+4(\text{mod} 6)}(\alpha) = e_{i+5(\text{mod} 6)}(\alpha) = 0 \), where \( 0 \leq i \leq 5 \). Then \( 0 = E_0(\alpha) = a_i + a_{i+1(\text{mod} 6)} + a_{i+3(\text{mod} 6)} \).

\[
\forall b = \rho^{6 i+1} \in R_1 \ 1 = E_0(\alpha^b) = a_i + a_{i+2(\text{mod} 6)} + a_{i+5(\text{mod} 6)}
\]

\[
\forall c = \rho^{6 i+2} \in R_2 \ 1 = E_0(\alpha^c) = a_i + a_{i+3(\text{mod} 6)} + a_{i+4(\text{mod} 6)}
\]

\[
\forall d = \rho^{6 i+3} \in R_3 \ 1 = E_0(\alpha^d) = a_i + a_{i+4(\text{mod} 6)} + a_{i+5(\text{mod} 6)}
\]

\[
\forall e = \rho^{6 i+4} \in R_4 \ 1 = E_0(\alpha^e) = a_i + a_{i+3(\text{mod} 6)} + a_{i+4(\text{mod} 6)}
\]

\[
\forall f = \rho^{6 i+5} \in R_5 \ 1 = E_0(\alpha^f) = a_i + a_{i+2(\text{mod} 6)} + a_{i+4(\text{mod} 6)}
\]

By solving system of linear equations in 6 unknowns \( a_i(\text{mod} 5), a_{i+1(\text{mod} 5)}, a_{i+2(\text{mod} 5)}, a_{i+3(\text{mod} 5)}, a_{i+4(\text{mod} 5)}, a_{i+5(\text{mod} 6)} \) we get \( a_i = 1, a_{i+1(\text{mod} 6)} = 0, a_{i+2(\text{mod} 6)} = 0, a_{i+3(\text{mod} 6)} = 1, a_{i+4(\text{mod} 6)} = 1, a_{i+5(\text{mod} 6)} = 0, 0 \leq i \leq 5 \), and therefore \( E_0(\alpha) = e_i(\alpha) + e_{i+3(\text{mod} 6)}(\alpha) + e_{i+4(\text{mod} 6)}(\alpha) \). By lemma 2.7, the set consisting of generating idempotents of \( \overline{C}_0, \overline{C}_1, \overline{C}_2, \overline{C}_3, \overline{C}_4, \overline{C}_5 \) is

\[
\{ e_0(\alpha) + e_3(\alpha), e_1(\alpha) + e_4(\alpha), e_5(\alpha), e_0(\alpha) + e_2(\alpha) + e_5(\alpha), e_0(\alpha) + e_1(\alpha) + e_4(\alpha), e_2(\alpha) + e_3(\alpha) \}
\]

3) Let

\[
e_i(\alpha) = e_{i+1(\text{mod} 6)}(\alpha) = e_{i+4(\text{mod} 6)}(\alpha) = 1, e_{i+2(\text{mod} 6)}(\alpha) = e_{i+3(\text{mod} 6)}(\alpha) = e_{i+5(\text{mod} 6)}(\alpha) = 0 \), \( 0 \leq i \leq 5 \).Then

\[
0 = E_0(\alpha) = a_i + a_{i+1(\text{mod} 6)} + a_{i+4(\text{mod} 6)}
\]

\[
\forall b = \rho^{6 i+1} \in R_1 \ 1 = E_0(\alpha^b) = a_i + a_{i+3(\text{mod} 6)} + a_{i+5(\text{mod} 6)}
\]

\[
\forall c = \rho^{6 i+2} \in R_2 \ 1 = E_0(\alpha^c) = a_i + a_{i+4(\text{mod} 6)} + a_{i+5(\text{mod} 6)}
\]

\[
\forall d = \rho^{6 i+3} \in R_3 \ 1 = E_0(\alpha^d) = a_i + a_{i+1(\text{mod} 6)} + a_{i+4(\text{mod} 6)}
\]

\[
\forall e = \rho^{6 i+4} \in R_4 \ 1 = E_0(\alpha^e) = a_i + a_{i+3(\text{mod} 6)} + a_{i+4(\text{mod} 6)}
\]

\[
\forall f = \rho^{6 i+5} \in R_5 \ 1 = E_0(\alpha^f) = a_i + a_{i+2(\text{mod} 6)} + a_{i+4(\text{mod} 6)}
\]

By solving system of linear equations in 6 unknowns \( a_i(\text{mod} 5), a_{i+1(\text{mod} 5)}, a_{i+2(\text{mod} 5)}, a_{i+3(\text{mod} 5)}, a_{i+4(\text{mod} 5)}, a_{i+5(\text{mod} 6)} \) we get that

\[
a_i = 0, a_{i+1(\text{mod} 6)} = 1, a_{i+2(\text{mod} 6)} = 0, a_{i+3(\text{mod} 6)} = 1, a_{i+4(\text{mod} 6)} = 1, a_{i+5(\text{mod} 6)} = 0, 0 \leq i \leq 5 \).

Thus, we have \( E_0(\alpha) = e_{i+1(\text{mod} 6)}(\alpha) + e_{i+3(\text{mod} 6)}(\alpha) + e_{i+4(\text{mod} 6)}(\alpha) \). By lemma 2.7, the set consisting of generating idempotents of \( \overline{C}_0, \overline{C}_1, \overline{C}_2, \overline{C}_3, \overline{C}_4, \overline{C}_5 \) is

\[
\{ e_0(\alpha) + e_3(\alpha), e_1(\alpha) + e_4(\alpha) + e_5(\alpha), e_0(\alpha) + e_2(\alpha) + e_5(\alpha), e_0(\alpha) + e_1(\alpha) + e_4(\alpha), e_2(\alpha) + e_3(\alpha) \}
\]

4) Let \( e_i(\alpha) = e_{i+2(\text{mod} 6)}(\alpha) = e_{i+4(\text{mod} 6)}(\alpha) = 1, e_{i+1(\text{mod} 6)}(\alpha) = e_{i+3(\text{mod} 6)}(\alpha) = e_{i+5(\text{mod} 6)}(\alpha) = 0 \), \( 0 \leq i \leq 5 \).

\[
0 = E_0(\alpha) = a_i + a_{i+2(\text{mod} 6)} + a_{i+4(\text{mod} 6)}
\]

\[
\forall b = \rho^{6 i+1} \in R_1 \ 1 = E_0(\alpha^b) = a_i + a_{i+3(\text{mod} 6)} + a_{i+5(\text{mod} 6)}
\]

\[
\forall c = \rho^{6 i+2} \in R_2 \ 1 = E_0(\alpha^c) = a_i + a_{i+2(\text{mod} 6)} + a_{i+4(\text{mod} 6)}
\]

(7) and (9) 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 \( e_i(\alpha) = 0, e_{i+2(\mod 6)}(\alpha) = e_{i+1(\mod 6)}(\alpha) = e_{i+3(\mod 6)}(\alpha) = e_{i+4(\mod 6)}(\alpha) = e_{i+5(\mod 6)}(\alpha) = 1, \quad 0 \leq i \leq 5 \).

Then \( 0 = \overline{E}_0(\alpha) = a_i + a_{i+1(\mod 6)} + a_{i+2(\mod 6)} + a_{i+3(\mod 6)} + a_{i+4(\mod 6)} + a_{i+5(\mod 6)} \)

\( \forall b = p^{6i+1} \in R_1 \; 1 = \overline{E}_0(\alpha^b) = a_i + a_{i+1(\mod 6)} + a_{i+2(\mod 6)} + a_{i+3(\mod 6)} + a_{i+4(\mod 6)} + a_{i+5(\mod 6)} \)

\( \forall c = p^{6i+2} \in R_2 \; 1 = \overline{E}_0(\alpha^c) = a_i + a_{i+1(\mod 6)} + a_{i+2(\mod 6)} + a_{i+3(\mod 6)} + a_{i+4(\mod 6)} + a_{i+5(\mod 6)} \)

\( \forall d = p^{6i+3} \in R_3 \; 1 = \overline{E}_0(\alpha^d) = a_i + a_{i+1(\mod 6)} + a_{i+2(\mod 6)} + a_{i+3(\mod 6)} + a_{i+4(\mod 6)} + a_{i+5(\mod 6)} \)

\( \forall e = p^{6i+4} \in R_4 \; 1 = \overline{E}_0(\alpha^e) = a_i + a_{i+1(\mod 6)} + a_{i+2(\mod 6)} + a_{i+3(\mod 6)} + a_{i+4(\mod 6)} + a_{i+5(\mod 6)} \)

\( \forall f = p^{6i+5} \in R_5 \; 1 = \overline{E}_0(\alpha^f) = a_i + a_{i+1(\mod 6)} + a_{i+2(\mod 6)} + a_{i+3(\mod 6)} + a_{i+4(\mod 6)} + a_{i+5(\mod 6)} \)

By solving system of linear equations in 6 unknowns \( a_i, a_{i+1(\mod 6)}, a_{i+2(\mod 6)}, a_{i+3(\mod 6)}, a_{i+4(\mod 6)}, a_{i+5(\mod 6)} \) we get that \( a_i = 1, a_{i+1(\mod 6)} = a_{i+2(\mod 6)} = a_{i+3(\mod 6)} = a_{i+4(\mod 6)} = a_{i+5(\mod 6)} = 0, \)

\( 0 \leq i \leq 5, \overline{E}_0(\alpha) = e_i(x) \). By lemma 2.7, the set consisting of generating idempotents of \( \overline{C}_0, \overline{C}_1, \overline{C}_2, \overline{C}_3, \overline{C}_4, \overline{C}_5 \) is \( \{ e_0(x), e_1(x), e_2(x), e_3(x), e_4(x), e_5(x) \} \).

Summary

Using coding theory, we have given precise expressions of generating idempotents of some sixth residue codes of length \( p \) over the binary field, where \( p \) is a prime such that \( p \equiv 1(\mod 24) \). Thus, the generating polynomials can be found by computing GCD of these generating idempotents and \( x^p - 1 \) without factoring \( x^p - 1 \). When \( p \) is a prime, where \( p \equiv 7(\mod 24) \), precise expressions of generating idempotents of some sixth residue codes of length \( p \) over the binary field will be discussed in the other paper.

Acknowledgement

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

References


