Korean J. Math. **30** (2022), No. 4, pp. 653–663
http://dx.doi.org/10.11568/kjm.2022.30.4.653

ON THE IDEMPOTENTS OF CYCLIC CODES OVER $\mathbb{F}_{2^t}$

Sunghyu Han

Abstract. We study cyclic codes of length n over $\mathbb{F}_{2^t}$. Cyclic codes can be viewed as ideals in $\mathcal{R}_n = \mathbb{F}_{2^t}[x]/(x^n - 1)$. It is known that there is a unique generating idempotent for each ideal. Let $e(x) \in \mathcal{R}_n$. If $t = 1$ or $t = 2$, then there is a necessary and sufficient condition that $e(x)$ is an idempotent. But there is no known similar result for $t \geq 3$. In this paper we give an answer for this problem.

1. Introduction

There are many interesting classes of codes in coding theory. Among them, cyclic codes are very important. Cyclic codes contain Hamming codes, Golay codes, and Reed-Solomon codes. E. Prange started the study of cyclic codes with two 1957 and 1959 AFCRL reports. In 1961, W. W. Peterson published a comprehensive book about cyclic codes [2]. This book was expanded by Peterson and E. J. Weldon [3].

Cyclic codes have a very nice algebraic structure, i.e., cyclic codes over finite fields are equivalent to ideals in an appropriate ring. Therefore the study of cyclic codes is the study of ideals. There are two important generators for cyclic codes. One is the generator polynomial and the other is the generating idempotent.

This paper is about the generating idempotent. The generating idempotent for cyclic codes over $\mathbb{F}_2$ are completely determined. For cyclic codes over $\mathbb{F}_4$, a similar result is found [1]. But further results are not known. In this paper, we study the generating idempotents for cyclic codes over $\mathbb{F}_{2^t}$ $(t \geq 1)$ and completely determine the generating idempotents for finite fields $\mathbb{F}_{2^t}$ for all $t \geq 1$.

This paper is organized as follows. In Section 2, we provide basic facts for cyclic codes and known results about the generating idempotents of cyclic codes over $\mathbb{F}_2$ and $\mathbb{F}_4$. In Section 3, we describe our main results which are about the generating idempotents of cyclic codes over $\mathbb{F}_{2^t}$ $(t \geq 1)$. In Section 4, we summarize this paper and give some future works.

Received May 30, 2022. Revised October 4, 2022. Accepted December 1, 2022.
2010 Mathematics Subject Classification: 94B15.
Key words and phrases: cyclic codes, finite fields, idempotents.
This work was supported by Education and Research promotion program of KOREATECH in 2022.

2. Preliminaries

In this section, we give well-known facts about cyclic codes over finite fields [1]. Let $\mathbb{F}_q$ be a finite field with q elements. A linear $[n,k]$ code $\mathcal{C}$ is defined by a k-dimensional subspace of n-dimensional vector space $(\mathbb{F}_q)^n$. We call n the code length of $\mathcal{C}$ and k the dimension of $\mathcal{C}$, and an element of $\mathcal{C}$ is called a codeword. Let $c = (c_0, c_1, c_2, \ldots, c_{n-1})$ be a codeword of $\mathcal{C}$. We consider cyclic shift of c, $c' = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$. We call $\mathcal{C}$ a cyclic code if $c' \in \mathcal{C}$ for all $c \in \mathcal{C}$.

Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{F}_q$. We assume that n and q are relatively prime. Let $\mathcal{R}_n = \mathbb{F}_q[x]/(x^n - 1)$. Then we can identify a codeword $c = (c_0, c_1, c_2, \ldots, c_{n-1})$ of $\mathcal{C}$ with an element $c(x) + (x^n - 1) \in \mathcal{R}_n$, where $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$. It is known that the set of all such $c(x) + (x^n - 1)$ is an ideal of $\mathcal{R}_n$. In other words, the set

$$A = \{c(x) + (x^n - 1) \mid c \in \mathcal{C}\}$$

is an ideal of $\mathcal{R}_n$. Conversely if A is an ideal of $\mathcal{R}_n$, then we can construct a cyclic code $\mathcal{C}$,

$$\mathcal{C} = \{c \mid c(x) + (x^n - 1) \in A\}.$$

From now on, we identify $c = (c_0, c_1, c_2, \ldots, c_{n-1})$ with $c(x) + (x^n - 1)$, where $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$. For notation simplicity, we write $c(x)$ for $c(x) + (x^n - 1)$ if there is no confusion. Therefore we can say that $\mathcal{C}$ is a cyclic code of length n over $\mathbb{F}_q$ if and only if $\mathcal{C}$ is an ideal in $\mathcal{R}_n = \mathbb{F}_q[x]/(x^n - 1)$.

It is known that $\mathcal{R}_n$ is a principal ring. In other words, every ideal of $\mathcal{R}_n$ is principal. Let $\mathcal{C}$ be an ideal in $\mathcal{R}_n$. Then there is $f(x) \in \mathcal{R}_n$ such that $\mathcal{C} = \langle f(x) \rangle$, i.e., $\mathcal{C}$ is generated by $f(x)$. Let $\mathcal{C}$ be a nonzero cyclic code in $\mathcal{R}_n$. Then it is known that there is a unique monic polynomial of minimum degree in $\mathcal{C}$. Let $g(x)$ be the polynomial. Then it is also known that $\mathcal{C} = \langle g(x) \rangle$, $g(x) \mid (x^n - 1)$, the dimension of $\mathcal{C}$ is $n - \deg(g(x))$, and $\{g(x), xg(x), \ldots, x^{n-\deg(g(x))-1} g(x)\}$ is a basis for $\mathcal{C}$. Conversely, let $g(x)$ be a monic polynomial such that $g(x) \mid (x^n - 1)$ and $\mathcal{C} = \langle g(x) \rangle$. Then $g(x)$ is the monic polynomial of minimum degree in $\mathcal{C}$. We call the polynomial $g(x)$ *the generator polynomial* of the cyclic code $\mathcal{C}$. We define the generator polynomial of the zero cyclic code $\{\mathbf{0}\}$ to be $x^n - 1$. From the discussion above, we know that there is one-to-one correspondence between all the cyclic codes in $\mathcal{R}_n$ and all the monic divisors of $x^n - 1$. By this correspondence, we have the following. Let m be the number of irreducible factors of $x^n - 1$ in $\mathbb{F}_q[x]$. Then the number of cyclic codes in $\mathcal{R}_n$ is 2^m.

Therefore it is important to find irreducible factors of $x^n - 1$ in $\mathbb{F}_q[x]$. We define $ord_n(q)$ by the order q modulo n, i.e., the smallest positive integer a such that $q^a \equiv 1 \pmod{n}$. Let $t = ord_n(q)$. Then $\mathbb{F}_{q^t}$ is the splitting field of $x^n - 1$ over $\mathbb{F}_q$. Let γ be a primitive element in $\mathbb{F}_{q^t}$ and let $\alpha = \gamma^{(q^t-1)/n}$. Then α is a primitive nth root of unity in $\mathbb{F}_{q^t}$ and

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \alpha^i).$$

We define q-cyclotomic coset of s modulo n by

$$C_s^q = \{s, sq, sq^2, \ldots, sq^{r-1}\} \pmod{n},$$

where $0 \leq s < n$ and r is the smallest positive integer such that $s \equiv sq^r \pmod{n}$. We use C_s instead of C_s^q if q is clear from the context. It follows that C_s^q is the orbit of the permutation $i \to iq \pmod{n}$ that contains s. The distinct q-cyclotomic cosets modulo n partition the set of integers $\{0, 1, 2, \ldots, n-1\}$. We define $S(q)$ as a set of representatives of q-cyclotomic cosets modulo n. Let s be an integer with $0 \leq s < n$. Then the minimal polynomial of α^s over $\mathbb{F}_q$ is

$$M_{\alpha^s}(x) = \prod_{i \in C_s} (x - \alpha^i)$$

and

$$x^n - 1 = \prod_{s \in S(q)} M_{\alpha^s}(x)$$

is the factorization of $x^n - 1$ into irreducible factors over $\mathbb{F}_q$.

Let $e(x)$ be an element of $\mathcal{R}_n$. If $e(x)^2 = e(x)$, then $e(x)$ is called an idempotent. Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{F}_q$. Then there is a unique idempotent in $\mathcal{R}_n$ which generate $\mathcal{C}$. We call the idempotent $e(x)$ *the generating idempotent* of $\mathcal{C}$. Let $\mathcal{C}$ be an $[n, k]$ cyclic code with the generating idempotent $e(x)$. Then $\{e(x), xe(x), \ldots, x^{k-1}e(x)\}$ is a basis for $\mathcal{C}$. For a cyclic code $\mathcal{C}$, the generator polynomial $g(x)$ and the generating idempotent are closely related. We can calculate the other if one of two is known. Suppose that we know the generator polynomial $g(x)$ for a cyclic code $\mathcal{C}$. Let $h(x) = (x^n - 1)/g(x)$. By the Euclidean Algorithm, we have $a(x)$ and $b(x)$ such that $1 = a(x)g(x) + b(x)h(x)$ in $\mathbb{F}_q[x]$. Then $a(x)g(x)$ in $\mathcal{R}_n$ is the generating idempotent $e(x)$ of $\mathcal{C}$. Conversely, suppose that we know the generating idempotent $e(x)$ of $\mathcal{C}$. Then $\gcd(e(x), x^n - 1)$ in $\mathbb{F}_q[x]$ is the generator polynomial $g(x)$ of $\mathcal{C}$.

The generating idempotent of a cyclic code and the q-cyclotomic cosets are closely related. Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{F}_q$ with the generating idempotent $e(x)$. Then

$$e(x) = \sum_{j \in S(q)} a_j \sum_{i \in C_j} x^i,$$

where $a_j \in \mathbb{F}_q$. If $q = 2$, then every element of $\mathcal{R}_n$ of the form

$$e(x) = \sum_{j \in S(2)} a_j \sum_{i \in C_j} x^i, \ (a_j \in \mathbb{F}_2) \tag{1}$$

is an idempotent of $\mathcal{R}_n$. Therefore, for $q = 2$ case, the generating idempotents of all the cyclic codes in $\mathcal{R}_n$ are completely determined by the 2-cyclotomic cosets modulo n.

Example 2.1. Let $q = 2$ and $n = 7$. Then the 2-cyclotomic cosets modulo 7 are $C_0 = \{0\}$, $C_1 = \{1, 2, 4\}$, and $C_3 = \{3, 6, 5\}$. Therefore $S(2) = \{0, 1, 3\}$. Let $\mathcal{C}$ be a cyclic code of length 7 over $\mathbb{F}_2$ with the generating idempotent $e(x)$. Then

$$e(x) = \sum_{j \in S(2)} a_j \sum_{i \in C_j} x^i, \tag{2}$$

where $a_j \in \mathbb{F}_2$. By equation (2), there are eight cyclic codes of length 7 over $\mathbb{F}_2$. In Table 1, we give the eight idempotents. In the table, dim, $g_i(x)$, and $e_i(x)$ means that the dimension, the generator polynomial, and the generating idempotent for a cyclic code of length 7 over $\mathbb{F}_2$, respectively.

TABLE 1. Idempotents of cyclic codes of length 7 over $\mathbb{F}_2$

i	dim	$g_i(x)$	$e_i(x)$
0	0	$1+x^7$	0
1	1	$1+x+x^2+\cdots+x^6$	$1+x+x^2+\cdots+x^6$
2	3	$1+x^2+x^3+x^4$	$1+x^3+x^5+x^6$
3	3	$1+x+x^2+x^4$	$1+x+x^2+x^4$
4	4	$1+x+x^3$	$x+x^2+x^4$
5	4	$1+x^2+x^3$	$x^3+x^5+x^6$
6	6	$1+x$	$x+x^2+\cdots+x^6$
7	7	1	1

TABLE 2. Idempotents of cyclic codes of length 11 over $\mathbb{F}_3$

i	dim	$g_i(x)$	$e_i(x)$
0	0	$-1+x^{11}$	0
1	1	$1+x+x^2+\cdots+x^{10}$	$-1-x-x^2-\cdots-x^{10}$
2	3	$1-x-x^2-x^3+x^4+x^6$	$1+x+x^3+x^4+x^5+x^9$
3	3	$1+x^2-x^3-x^4-x^5+x^6$	$1+x^2+x^6+x^7+x^8+x^{10}$
4	4	$-1+x^2-x^3+x^4+x^5$	$-x^2-x^6-x^7-x^8-x^{10}$
5	4	$-1-x+x^2-x^3+x^5$	$-x-x^3-x^4-x^5-x^9$
6	6	$-1+x$	$-1+x+x^2+\cdots+x^{10}$
7	7	1	1

For other cases, i.e., $q \neq 2$ cases, we know that the idempotents are the following form:

$$e(x) = \sum_{j \in S(q)} a_j \sum_{i \in C_j} x^i, \tag{3}$$

where $a_j \in \mathbb{F}_q$. But the converse is not always true. In other words, the expression $e(x)$ in equation (3) is not always an idempotent.

EXAMPLE 2.2. Let $q = 3$ and $n = 11$. Then the 3-cyclotomic cosets modulo 11 are $C_0 = \{0\}$, $C_1 = \{1, 3, 4, 5, 9\}$, and $C_2 = \{2, 6, 7, 8, 10\}$. Therefore $S(3) = \{0, 1, 2\}$. Let $\mathcal{C}$ be a cyclic code of length 11 over $\mathbb{F}_3$ with generating idempotent $e(x)$. Then

$$e(x) = \sum_{j \in S(3)} a_j \sum_{i \in C_j} x^i, \tag{4}$$

where $a_j \in \mathbb{F}_3$. By equation (4), there are 27 possibilities for $e(x)$. In fact, there are exactly eight cyclic codes of length 11 over $\mathbb{F}_3$. Therefore all the expressions of equation (4) are not idempotents. In Table 2, we give the eight idempotents.

For $q = 4$ case, there is a similar result as $q = 2$ case in [1, Section 4.3]. Let

$$S(4) = K \cup L_1 \cup L_2, \tag{5}$$

where K, L_1, and L_2 are pairwise disjoint. K consists of distinct representatives k, where $C_k = C_{2k}$. L_1 and L_2 are chosen so that if $k \in L_1 \cup L_2$, $C_k \neq C_{2k}$; furthermore $L_2 = \{2k \mid k \in L_1\}$. Then $e(x)$ is an idempotent in R_n if and only if

$$e(x) = \sum_{j \in K} a_j \sum_{i \in C_j} x^i + \sum_{j \in L_1} (b_j \sum_{i \in C_j} x^i + b_j^2 \sum_{i \in C_j} x^{2i}), \tag{6}$$

where $a_j \in \mathbb{F}_2$ and $b_j \in \mathbb{F}_4$.

EXAMPLE 2.3. Let $q = 4$ and $n = 7$. Then the 4-cyclotomic cosets modulo 7 are $C_0 = \{0\}$, $C_1 = \{1, 4, 2\}$, and $C_3 = \{3, 5, 6\}$. Therefore $K = \{0, 1, 3\}$ and $L_1 = L_2 = \emptyset$. Let $\mathcal{C}$ be a cyclic code of length 7 over $\mathbb{F}_4$ with generating idempotent $e(x)$. Then

$$e(x) = \sum_{j \in K} a_j \sum_{i \in C_j} x^i,$$

where $a_j \in \mathbb{F}_2$. Therefore, there are exactly eight cyclic codes of length 7 over $\mathbb{F}_4$.

EXAMPLE 2.4. Let $q = 4$ and $n = 21$. Then the 4-cyclotomic cosets modulo 21 are $C_0 = \{0\}$, $C_1 = \{1, 4, 16\}$, $C_2 = \{2, 8, 11\}$, $C_3 = \{3, 12, 6\}$, $C_5 = \{5, 20, 17\}$, $C_7 = \{7\}$, $C_9 = \{9, 15, 18\}$, $C_{10} = \{10, 19, 13\}$, $C_{14} = \{14\}$. Therefore, $K = \{0, 3, 9\}$, $L_1 = \{1, 5, 7\}$, $L_2 = \{2, 10, 14\}$. Let $\mathcal{C}$ be a cyclic code of length 7 over $\mathbb{F}_4$ with generating idempotent $e(x)$. Then

$$e(x) = \sum_{j \in K} a_j \sum_{i \in C_j} x^i + \sum_{j \in L_1} (b_j \sum_{i \in C_j} x^i + b_j^2 \sum_{i \in C_j} x^{2i}),$$

where $a_j \in \mathbb{F}_2$ and $b_j \in \mathbb{F}_4$. Therefore, there are exactly $2^9 (= 2^3 \times 4^3)$ cyclic codes of length 21 over $\mathbb{F}_4$.

3. Main results

In this section, we continue the study of the generating idempotents of cyclic codes over $\mathbb{F}_{2^t}$, $(t \geq 1)$. We start with the following theorem.

THEOREM 3.1. *Let n be an odd positive integer and $t \geq 1$. If $|C_s^2| = r$, then*

$$C_s^2 = C_s^{2^t} \cup C_{2s}^{2^t} \cup C_{2^2 s}^{2^t} \cup \cdots \cup C_{2^{d-1} s}^{2^t}, \tag{7}$$

where $d = \gcd(t, r)$. Furthermore, we have

$$|C_s^{2^t}| = |C_{2s}^{2^t}| = |C_{2^2 s}^{2^t}| = \cdots = |C_{2^{d-1} s}^{2^t}| = \frac{r}{d},$$

$$C_{2^i s}^{2^t} \cap C_{2^j s}^{2^t} = \emptyset, (0 \leq i < j \leq d-1),$$

and

$$C_{2^d s}^{2^t} = C_s^{2^t}. \tag{8}$$

Proof. Let $t = dt_1$ and $r = dr_1$. Note that $\gcd(t_1, r_1) = 1$. First we prove that $|C_s^{2^t}| = \frac{r}{d} = r_1$. Let $|C_s^{2^t}| = m$. Then we have

$$s \equiv s \cdot (2^t)^m = s \cdot 2^{tm} \pmod{n}.$$

Since $|C_s^2| = r$, we have $r \mid tm$. Therefore $dr_1 \mid dt_1 m$ and $r_1 \mid m$. Since $|C_s^2| = r$, we have the following equation.

$$s \cdot (2^t)^{r_1} = s \cdot 2^{dt_1 r_1} = s \cdot (2^r)^{t_1} \equiv s \pmod{n}.$$

Since $|C_s^{2^t}| = m$, we have $m \mid r_1$. Therefore $m = r_1$ and $|C_s^{2^t}| = \frac{r}{d}$.

Second we prove that $|C_{2^i s}^{2^t}| = \frac{r}{d}$ for all $i = 0, 1, 2, \ldots, d-1$. Let $|C_{2^i s}^{2^t}| = m'$. Then we have the following equivalent statements.

$$2^i s \equiv 2^i s \cdot (2^t)^{m'} \pmod{n} \Leftrightarrow s \equiv s \cdot (2^t)^{m'} \pmod{n}.$$

Therefore $|C^{2^t}_{2^i s}| = \frac{r}{d}$ and we have

$$|C^{2^t}_s| = |C^{2^t}_{2s}| = |C^{2^t}_{2^2 s}| = \cdots = |C^{2^t}_{2^{d-1} s}| = \frac{r}{d}. \tag{9}$$

Third we prove that

$$C^2_s \subseteq \big(C^{2^t}_s \cup C^{2^t}_{2s} \cup C^{2^t}_{2^2 s} \cup \cdots \cup C^{2^t}_{2^{d-1} s}\big).$$

Choose an element $s \cdot 2^i$ in C^2_s for some i, $(0 \le i < r)$. By division algorithm, there are a and b such that $i = ad + b$, $(0 \le b < d)$. Since $d = \gcd(t, r)$, there are e and f such that

$$d = et + fr. \tag{10}$$

Therefore

$$\begin{aligned} s \cdot 2^i &= s \cdot 2^{ad+b} \\ &= s \cdot 2^{a(et+fr)+b} \\ &= s \cdot (2^r)^{af} \cdot 2^b \cdot (2^t)^{ae} \\ &\equiv s \cdot 2^b \cdot (2^t)^{ae} \pmod{n}. \end{aligned}$$

So, $s \cdot 2^i \in C^{2^t}_{2^b s}$. This leads to

$$C^2_s \subseteq \big(C^{2^t}_s \cup C^{2^t}_{2s} \cup C^{2^t}_{2^2 s} \cup \cdots \cup C^{2^t}_{2^{d-1} s}\big). \tag{11}$$

Since $|C^2_s| = r$, by Eqn. (9) and Eqn. (11), we have

$$C^{2^t}_{2^i s} \cap C^{2^t}_{2^j s} = \emptyset, (0 \le i < j \le d-1).$$

and

$$C^2_s = C^{2^t}_s \cup C^{2^t}_{2s} \cup C^{2^t}_{2^2 s} \cup \cdots \cup C^{2^t}_{2^{d-1} s}.$$

Finally, we prove that $C^{2^t}_{2^d s} = C^{2^t}_s$. Using Eqn. (10) and $|C^2_s| = r$ we have

$$\begin{aligned} s \cdot 2^d &= s \cdot 2^{et+fr} \\ &= s \cdot (2^r)^f (2^t)^e \\ &\equiv s \cdot (2^t)^e \pmod{n}. \end{aligned}$$

Therefore $s \cdot 2^d \in C^{2^t}_s$. This leads to $C^{2^t}_{2^d s} = C^{2^t}_s$ and completes the proof. □

Example 3.2. We give an example for Theorem 3.1. Let $n = 21$, $t = 9$, and $s = 1$. Then $C^2_1 = \{1, 2, 4, 8, 16, 11\}$. Therefore $r = 6$, $d = \gcd(9, 6) = 3$, $C^{2^9}_1 = \{1, 8\}$, $C^{2^9}_2 = \{2, 16\}$, $C^{2^9}_4 = \{4, 11\}$, and

$$C^2_1 = C^{2^9}_1 \cup C^{2^9}_2 \cup C^{2^9}_4.$$

Theorem 3.3. *Let $S(2)$ be a fixed set of representatives of 2-cyclotomic cosets modulo n. Then we can describe $S(2^t)$, a set of representatives of 2^t-cyclotomic cosets modulo n, by the following.*

$$S(2^t) = \bigcup_{d|t} \Big(\bigcup_{k=0}^{d-1} M^d_k \Big),$$

where

$$M^d_k = \{2^k \cdot s \mid s \in S(2), d = \gcd(t, |C^2_s|)\}, (k = 0, 1, 2, \ldots, d-1). \tag{12}$$

Proof. By Eqn. (7) we have

$$S(2^t) = \{s, 2s, 2^2 s, \ldots, 2^{d-1}s \mid s \in S(2), d = \gcd(t, |C_s^2|)\}.$$

From this, the result follows. □

Note that if $t = 1$ in Theorem 3.3, then

$$S(2^t) = M_0^1 = S(2). \tag{13}$$

If if $t = 2$ in Theorem 3.3, then

$$S(2^t) = S(4) = M_0^1 \cup (M_0^2 \cup M_1^2).$$

By Eqn. (8), we have $C_{2s}^4 = C_s^4$ for $s \in M_0^1$. By Eqn. (12), we have

$$M_0^2 = \{s \mid s \in S(2),\ 2 = \gcd(2, |C_s^2|)\},\ M_1^2 = \{2s \mid s \in S(2),\ 2 = \gcd(2, |C_s^2|)\}.$$

Therefore for $t = 2$ case, M_0^1, M_0^2, and M_1^2 correspond to K, L_1, and L_2 in Eqn. (5) respectively. In other words, we have

$$M_0^1 = K,\ M_0^2 = L_1,\ M_1^2 = L_2. \tag{14}$$

Now we give our main result.

THEOREM 3.4. *Let $q = 2^t$ $(t \geq 1)$, C_j be the q-cyclotomic coset of j modulo n, and $\mathcal{R}_n = \mathbb{F}_{2^t}[x]/(x^n - 1)$. Then $e(x)$ is an idempotent in $\mathcal{R}_n$ if and only if*

(15)

$$e(x) = \sum_{d|t} \sum_{j \in M_0^d} \Big(m_j^d \sum_{i \in C_j} x^i + (m_j^d)^2 \sum_{i \in C_j} x^{2i} + (m_j^d)^{2^2} \sum_{i \in C_j} x^{2^2 i} + \cdots + (m_j^d)^{2^{d-1}} \sum_{i \in C_j} x^{2^{d-1} i} \Big),$$

where $m_j^d \in \mathbb{F}_{2^d}$.

Proof. Let

$$e(x) = \sum_{d|t} \sum_{j \in M_0^d} \Big(m_j^d \sum_{i \in C_j} x^i + (m_j^d)^2 \sum_{i \in C_j} x^{2i} + (m_j^d)^{2^2} \sum_{i \in C_j} x^{2^2 i} + \cdots + (m_j^d)^{2^{d-1}} \sum_{i \in C_j} x^{2^{d-1} i} \Big),$$

where $m_j^d \in \mathbb{F}_{2^d}$. Then,

$$e(x)^2 = \sum_{d|t} \sum_{j \in M_0^d} \Big((m_j^d)^2 \sum_{i \in C_j} x^{2i} + (m_j^d)^{2^2} \sum_{i \in C_j} x^{2^2 i} + \cdots + (m_j^d)^{2^{d-1}} \sum_{i \in C_j} x^{2^{d-1} i} + (m_j^d)^{2^d} \sum_{i \in C_j} x^{2^d i} \Big).$$

Since $m_j^d \in \mathbb{F}_{2^d}$, we have $(m_j^d)^{2^d} = m_j^d$. By Eqn. (8), we know $C_{2^d j} = C_j$. Therefore we have $\sum_{i \in C_j} x^{2^d i} = \sum_{i \in C_{2^d j}} x^i = \sum_{i \in C_j} x^i$ and $(m_j^d)^{2^d} \sum_{i \in C_j} x^{2^d i} = m_j^d \sum_{i \in C_j} x^i$. This leads to $e(x)^2 = e(x)$ and proves that $e(x)$ is an idempotent in $\mathcal{R}_n$.

For the converse statement, let m be the number of 2^t-cyclotomic cosets modulo n. Since

$$S(2^t) = \bigcup_{d|t} \Big(\bigcup_{k=0}^{d-1} M_k^d \Big),$$

we have

$$m = \sum_{d|t} \sum_{k=0}^{d-1} |M_k^d|$$

Since

$$|M_0^d| = |M_1^d| = \cdots = |M_{d-1}^d|,$$

we have

$$m = \sum_{d|t} d \cdot |M_0^d|.$$

We know that the number of cyclic codes in $\mathcal{R}_n$ is 2^m. Therefore the number of idempotents in $\mathcal{R}_n$ is 2^m. On the other hand, the number of all possible different expressions in Eqn.(15) is

$$\prod_{d|t} (2^d)^{|M_0^d|} = 2^{\sum_{d|t} d \cdot |M_0^d|} = 2^m.$$

This completes the proof. □

Note that if $t = 1$ in Theorem 3.4, then Eqn. (15) becomes

$$e(x) = \sum_{j \in M_0^1} \Big(m_j^1 \sum_{i \in C_j} x^i \Big), (m_j^1 \in \mathbb{F}_2).$$

By Eqn.(13), we have $M_0^1 = S(2)$. Therefore

$$e(x) = \sum_{j \in S(2)} \Big(m_j^1 \sum_{i \in C_j} x^i \Big), (m_j^1 \in \mathbb{F}_2).$$

This equals to Eqn. (1). Therefore Theorem 3.4 agrees with the known result for $t = 1$ case. If $t = 2$ in Theorem 3.4, then Eqn. (15) becomes

$$e(x) = \sum_{j \in M_0^1} \Big(m_j^1 \sum_{i \in C_j} x^i \Big) + \sum_{j \in M_0^2} \Big(m_j^2 \sum_{i \in C_j} x^i + (m_j^2)^2 \sum_{i \in C_j} x^{2i} \Big),$$

where $m_j^1 \in \mathbb{F}_2$ and $m_j^2 \in \mathbb{F}_4$. By Eqn. (14) we have $M_0^1 = K,\ M_0^2 = L_1,\ M_1^2 = L_2$. Therefore

$$e(x) = \sum_{j \in K} \Big(m_j^1 \sum_{i \in C_j} x^i \Big) + \sum_{j \in L_1} \Big(m_j^2 \sum_{i \in C_j} x^i + (m_j^2)^2 \sum_{i \in C_j} x^{2i} \Big).$$

This equals to Eqn. (6). Therefore Theorem 3.4 agrees with the known result for $t = 2$ case.

In the following, we give examples of Theorem 3.3 and Theorem 3.4 for $t \geq 3$.

Example 3.5. Let $t = 3$ and $n = 15$. Then $q = 8$ and we have the following:

1. $C_0 = \{0\}$, $C_1 = \{1, 8, 4, 2\}$, $C_3 = \{3, 9, 12, 6\}$, $C_5 = \{5, 10\}$, $C_7 = \{7, 11, 13, 14\}$.
2. $S(8) = M_0^1 \cup (M_0^3 \cup M_1^3 \cup M_2^3)$, where $M_0^1 = \{0, 1, 3, 5, 7\}$, $M_0^3 = M_1^3 = M_2^3 = \emptyset$.

Then $e(x)$ is an idempotent in $\mathcal{R}_n = \mathbb{F}_8[x]/(x^{15} - 1)$ if and only if

$$e(x) = \sum_{j \in M_0^1} a_j \sum_{i \in C_j} x^i,$$

where $a_j \in \mathbb{F}_2$. Therefore, there are exactly 2^5 cyclic codes of length 15 over $\mathbb{F}_8$.

Example 3.6. Let $t = 3$ and $n = 21$. Then $q = 8$ and we have the following:

1. $C_0 = \{0\}$, $C_3 = \{3\}$, $C_6 = \{6\}$, $C_9 = \{9\}$, $C_{12} = \{12\}$, $C_{15} = \{15\}$, $C_{18} = \{18\}$, $C_1 = \{1, 8\}$, $C_2 = \{2, 16\}$, $C_4 = \{4, 11\}$, $C_5 = \{5, 19\}$, $C_7 = \{7, 14\}$, $C_{10} = \{10, 17\}$, $C_{13} = \{13, 20\}$.
2. $S(8) = M_0^1 \cup (M_0^3 \cup M_1^3 \cup M_2^3)$, where $M_0^1 = \{0, 3, 6, 9, 12, 15, 18, 7\}$, $M_0^3 = \{1, 5\}$, $M_1^3 = \{2, 10\}$, $M_2^3 = \{4, 20\}$.

Then $e(x)$ is an idempotent in $\mathcal{R}_n = \mathbb{F}_8[x]/(x^{21}-1)$ if and only if

$$e(x) = \sum_{j\in M_0^1} a_j \sum_{i\in C_j} x^i + \sum_{j\in M_0^3} (b_j \sum_{i\in C_j} x^i + b_j^2 \sum_{i\in C_j} x^{2i} + b_j^4 \sum_{i\in C_j} x^{4i}),$$

where $a_j \in \mathbb{F}_2$, $b_j \in \mathbb{F}_8$. Therefore, there are exactly $2^{14}(= (2)^8 \times (2^3)^2)$ cyclic codes of length 21 over $\mathbb{F}_8$.

Example 3.7. Let $t = 4$ and $n = 7$. Then $q = 16$ and we have the following:

1. $C_0 = \{0\}$, $C_1 = \{1, 2, 4\}$, $C_3 = \{3, 6, 5\}$.
2. $S(16) = M_0^1 \cup (M_0^2 \cup M_1^2) \cup (M_0^4 \cup M_1^4 \cup M_2^4 \cup M_3^4)$, where $M_0^1 = \{0, 1, 3\}$, $M_0^2 = M_1^2 = M_0^4 = M_1^4 = M_2^4 = M_3^4 = \emptyset$.

Then $e(x)$ is an idempotent in $\mathcal{R}_n = \mathbb{F}_{16}[x]/(x^7-1)$ if and only if

$$e(x) = \sum_{j\in M_0^1} a_j \sum_{i\in C_j} x^i,$$

where $a_j \in \mathbb{F}_2$. Therefore, there are exactly 2^3 cyclic codes of length 7 over $\mathbb{F}_{16}$.

Example 3.8. Let $t = 4$ and $n = 21$. Then $q = 16$ and we have the following:

1. $C_0 = \{0\}$, $C_1 = \{1, 16, 4\}$, $C_2 = \{2, 11, 8\}$, $C_3 = \{3, 6, 12\}$, $C_5 = \{5, 17, 20\}$, $C_7 = \{7\}$, $C_9 = \{9, 18, 15\}$, $C_{10} = \{10, 13, 19\}$, $C_{14} = \{14\}$.
2. $S(16) = M_0^1 \cup (M_0^2 \cup M_1^2) \cup (M_0^4 \cup M_1^4 \cup M_2^4 \cup M_3^4)$, where $M_0^1 = \{0, 3, 9\}$, $M_0^2 = \{1, 5, 7\}$, $M_1^2 = \{2, 10, 14\}$, $M_0^4 = M_1^4 = M_2^4 = M_3^4 = \emptyset$.

Then $e(x)$ is an idempotent in $\mathcal{R}_n = \mathbb{F}_{16}[x]/(x^{21}-1)$ if and only if

$$e(x) = \sum_{j\in M_0^1} a_j \sum_{i\in C_j} x^i + \sum_{j\in M_0^2} (b_j \sum_{i\in C_j} x^i + b_j^2 \sum_{i\in C_j} x^{2i}),$$

where $a_j \in \mathbb{F}_2$ and $b_j \in \mathbb{F}_4$. Therefore, there are exactly $2^9(= (2)^3 \times (2^2)^3)$ cyclic codes of length 21 over $\mathbb{F}_{16}$.

Example 3.9. Let $t = 4$ and $n = 15$. Then $q = 16$ and we have the following:

1. $C_i = \{i\}$, $(i = 0, 1, 2, \ldots, 14)$,
2. $S(16) = M_0^1 \cup (M_0^2 \cup M_1^2) \cup (M_0^4 \cup M_1^4 \cup M_2^4 \cup M_3^4)$, $M_0^1 = \{0\}$, $M_0^2 = \{5\}$, $M_1^2 = \{10\}$, $M_0^4 = \{1, 3, 7\}$, $M_1^4 = \{2, 6, 14\}$, $M_2^4 = \{4, 12, 13\}$, $M_3^4 = \{8, 9, 11\}$.

Then $e(x)$ is an idempotent in $\mathcal{R}_n = \mathbb{F}_{16}[x]/(x^{15}-1)$ if and only if

$$\begin{aligned} e(x) &= \sum_{j\in M_0^1} a_j \sum_{i\in C_j} x^i \\ &+ \sum_{j\in M_0^2} (b_j \sum_{i\in C_j} x^i + b_j^2 \sum_{i\in C_j} x^{2i}) \\ &+ \sum_{j\in M_0^4} (f_j \sum_{i\in C_j} x^i + f_j^2 \sum_{i\in C_j} x^{2i} + f_j^4 \sum_{i\in C_j} x^{4i} + f_j^8 \sum_{i\in C_j} x^{8i}), \end{aligned}$$

where $a_j \in \mathbb{F}_2$, $b_j \in \mathbb{F}_4$, and $f_j \in \mathbb{F}_{16}$. Therefore, there are exactly $2^{15}(= (2) \times (2^2) \times (2^4)^3)$ cyclic codes of length 15 over $\mathbb{F}_{16}$.

Example 3.10. Let $t = 5$ and $n = 21$. Then $q = 32$ and we have the following:

1. $C_0 = \{0\}$, $C_1 = \{1, 2, 4, 8, 16, 11\}$, $C_3 = \{3, 6, 12\}$, $C_5 = \{5, 10, 20, 19, 17, 13\}$, $C_7 = \{7, 14\}$, $C_9 = \{9, 18, 15\}$.

2. $S(32) = M_0^1 \cup (M_0^5 \cup M_1^5 \cup M_2^5 \cup M_3^5 \cup M_4^5)$, where $M_0^1 = \{0, 1, 3, 5, 7, 9\}$, $M_0^5 = M_1^5 = M_2^5 = M_3^5 = M_4^5 = \emptyset$.

Then $e(x)$ is an idempotent in $\mathcal{R}_n = \mathbb{F}_{32}[x]/(x^{21} - 1)$ if and only if

$$e(x) = \sum_{j \in M_0^1} a_j \sum_{i \in C_j} x^i$$

where $a_j \in \mathbb{F}_2$. Therefore, there are exactly 2^6 cyclic codes of length 21 over $\mathbb{F}_{32}$.

EXAMPLE 3.11. Let $t = 6$ and $n = 21$. Then $q = 64$ and we have the following:

1. $C_i = \{i\}$, $(i = 0, 1, 2, \ldots, 20)$,
2. $S(64) = M_0^1 \cup (M_0^2 \cup M_1^2) \cup (M_0^3 \cup M_1^3 \cup M_2^3) \cup (M_0^6 \cup M_1^6 \cup M_2^6 \cup M_3^6 \cup M_4^6 \cup M_5^6)$, where $M_0^1 = \{0\}$, $M_0^2 = \{7\}$, $M_1^2 = \{14\}$, $M_0^3 = \{3, 9\}$, $M_1^3 = \{6, 18\}$, $M_2^3 = \{12, 15\}$, $M_0^6 = \{1, 5\}$, $M_1^6 = \{2, 10\}$, $M_2^6 = \{4, 20\}$, $M_3^6 = \{8, 19\}$, $M_4^6 = \{16, 17\}$, $M_5^6 = \{11, 13\}$.

Then $e(x)$ is an idempotent in $\mathcal{R}_n = \mathbb{F}_{64}[x]/(x^{21} - 1)$ if and only if

$$\begin{aligned} e(x) &= \sum_{j \in M_0^1} a_j \sum_{i \in C_j} x^i \\ &+ \sum_{j \in N_1} (b_j \sum_{i \in C_j} x^i + b_j^2 \sum_{i \in C_j} x^{2i}) \\ &+ \sum_{j \in M_1} (f_j \sum_{i \in C_j} x^i + f_j^2 \sum_{i \in C_j} x^{2i} + f_j^4 \sum_{i \in C_j} x^{4i}) \\ &+ \sum_{j \in M_0^2} (g_j \sum_{i \in C_j} x^i + g_j^2 \sum_{i \in C_j} x^{2i} + g_j^4 \sum_{i \in C_j} x^{4i} + g_j^8 \sum_{i \in C_j} x^{8i} + g_j^{16} \sum_{i \in C_j} x^{16i} + g_j^{32} \sum_{i \in C_j} x^{32i}), \end{aligned}$$

where $a_j \in \mathbb{F}_2$, $b_j \in \mathbb{F}_4$, $f_j \in \mathbb{F}_8$, $g_j \in \mathbb{F}_{64}$. Therefore, there are exactly $2^{21} (= 2 \times 2^2 \times (2^3)^2 \times (2^6)^2)$ cyclic codes of length 21 over $\mathbb{F}_{64}$.

4. Summary

In this paper, we study the generating idempotents of cyclic codes over finite fields. For an element $e(x) \in \mathcal{R}_n$, $(\mathcal{R}_n = \mathbb{F}_{2^t}[x]/(x^n - 1))$, there is an equivalent condition that $e(x)$ is an idempotent if $t = 1$ or $t = 2$. We extended this result for the case $t \geq 3$ and presented an equivalent condition that $e(x)$ is an idempotent for all $t \geq 1$. For a future work, it is worth to study the same subject for other finite fields or rings. For example, $\mathbb{F}_{3^t}$ and $\mathbb{Z}_4$ can be possible candidates.

Acknowledgments. The author would like to thank the referees for their valuable comments which improved the clarity of this paper.

References

[1] W. C. Huffman, V. S. Pless, *Fundamentals of Error-correcting Codes*, Cambridge: Cambridge University Press, 2003.
[2] W. W. Peterson, *Error-Correcting Codes*, Cambridge, MA: MIT Press, 1961.
[3] W. W. Peterson, E. J. Weldon, Jr., *Error-Correcting Codes*, 2nd ed. Cambridge, MA.: MIT Press, 1972.

Sunghyu Han
School of Liberal Arts, KoreaTech,
Cheonan 31253, Republic of Korea.
E-mail: sunghyu@koreatech.ac.kr