Jurnal Matematika Thales (JMT)
Vol. 07, No. 01 (2025), pp. 22–34.

Secret Sharing Schemes from Two Families of Cyclic Codes Using Massey's Construction

Syahrul Zada[1]*, Karyati[2]

[1,2]Universitas Negeri Yogyakarta, Indonesia

[1]syahrulzada.2020@student.uny.ac.id, [2]karyati@uny.ac.id

Abstract. The objectives of this study include proving that $\widetilde{C}_{(q,m,\delta_2)}$ and $\widetilde{C}_{(q,m,\delta_3)}$, which are Primitive BCH codes, with $m \geq 5$ are minimal codes, and presenting specific examples of secret-sharing schemes based on dual of these codes. To prove that $\widetilde{C}_{(q,m,\delta_2)}$ and $\widetilde{C}_{(q,m,\delta_3)}$ with $m \geq 5$ are minimal codes, the criterion $\frac{W_{min}}{W_{max}} > \frac{q-1}{q}$ used, where W_{min} and W_{max} are the minimum weight and maximum weight, respectively. Data on the minimum weight and maximum weight of $\widetilde{C}_{(q,m,\delta_2)}$ and $\widetilde{C}_{(q,m,\delta_3)}$ are obtained from previous research. To give an example of secret-sharing scheme construction based on these codes, the construction method to be used is Massey construction. This research successfully proves that $\widetilde{C}_{(q,m,\delta_2)}$ and $\widetilde{C}_{(q,m,\delta_3)}$ with $m \geq 5$ are minimal codes. In addition, this research also successfully presents an example of secret-sharing scheme construction based on these codes using Massey's construction.

Keywords: dual codes, Massey's contruction, minimal codes, primitive BCH codes, secret-sharing.

1. INTRODUCTION

The *secret sharing* scheme is one of the protocols in cryptography that aims to share secret data with several parties, where the parties receiving the secret sharing must work together to access the secret data. The idea of secret sharing was first pioneered by Shamir [1]. The scheme he introduced is called the (k, n) threshold scheme

The (k, n) threshold scheme uses polynomial interpolation in the sharing and recovery of *secret.* Besides using polynomial interpolation, secret sharing schemes

[*] Corresponding author

2020 Mathematics Subject Classification: 55S30

Received: 01-07-2025, accepted: 21-08-2025.

can be built using other mathematical objects. The idea of replacing polynomial interpolation with other algorithms was first proposed by McEliece & Sarwate [2]. They replaced polynomial interpolation on the (k, n) threshold scheme with a Reed-Solomon code encoding and decoding algorithm.

Apart from using Reed-Solomon codes, the *secret-sharing* scheme can be constructed using linear codes in general. In the existing literature, there are two approaches to construct textitsecret sharing schemes based on linear codes. The first approach was developed in 1989 by Brickell [3]. While the second approach was developed by Massey [4].

In the second construction or commonly called Massey construction, the minimal *codeword* is needed to determine the minimal access set (the smallest set of participants that can select the secret). Therefore, the minimal *codeword* in a linear code needs to be found. Finding all minimal codewords of a linear code is quite a difficult problem as it requires testing q^k codewords of a linear code. The problem is one form of the *covering problem.*

One way to simplify the *covering problem* on linear codes is to use the Ashikhmin-Barg [5] criterion. If a linear code satisfies this criterion, it is called a minimal linear code. A minimal linear code is a type of linear code that can produce a *secret sharing* scheme with an interesting access structure [6].

An example of a minimal linear code has been produced by Ding, Fan, and Zhou [7], namely the $\widetilde{C}_{(q,m,\delta_2)}$ code and the $\widetilde{C}_{(q,m,\delta_3)}$ code with $m \geq 5$ which are Primitive BCH codes with designed distances δ_2 and δ_3. Let $m > 1$ be a positive integer, and let $n = q^m - 1$. Suppose α is the generator of $\mathbb{F}_{q^m}^*$, which is the multiplicative group of $\mathbb{F}_{q^m}$. For every i with $0 \leq i \leq q^m - 2$, let $m_i(x)$ denote the minimal polynomial of α^i over $\mathbb{F}_{q^m}$. For every $2 \leq \delta < n$, define

$$g_{q,m,\delta}(x) = KPK(m_1(x), m_2(x), \cdots, m_{\delta-1}(x)),$$

where KPK denotes the least common multiple. In addition, also define

$$\tilde{g}_{q,m,\delta}(x) = (x-1)g_{q,m,\delta}(x).$$

Let $C_{(q,m,\delta)}$ and $\tilde{C}_{(q,m,\delta)}$ denote cyclic codes of length n with generator polynomials $g_{(q,m,\delta)}(x)$ and $\tilde{g}_{(q,m,\delta)}(x)$, respectively. The set $C_{(q,m,\delta)}$ is a primitive BCH code with designed distance δ, and $\tilde{C}_{(q,m,\delta)}$ is a primitive BCH code with designed distance δ.

Actually, Ding et al. discuss the dimensions and weights of two families of BCH codes. However, in the last part of their article, Ding et al. the code $\widetilde{C}_{(q,m,\delta_2)}$ and the code $\widetilde{C}_{(q,m,\delta_3)}$ satisfy the Ashikhmin-Barg criterion when $m \geq 5$ so they are minimal codes. Unfortunately, the statement has not been accompanied by a proof. Thus, in this paper, the proof that these 2 codes are minimal codes will be presented.

2. **Weight Distribution and Parameter of Code**

Before presenting the characterization results of primitive BCH codes with δ_2 and δ_3 designed distances, the following two theorems are first presented. These two theorems have been proved in [7]. The following theorem provides information about the weight distribution of the code $\widetilde{C}_{(q,m,\delta_2)}$.

Theorem 2.1. [7] *The code* $\widetilde{C}_{(q,m,\delta_2)}$ *has parameters* $[n,\tilde{k},\tilde{d}]$, *where* $\tilde{d} \geq \delta_2 + 1$ *and*

$$\tilde{k} = \begin{cases} 2m & \textit{for odd } m, \\ \frac{3m}{2} & \textit{for even } m. \end{cases}$$

When q is an odd prime, $\tilde{d} = \delta_2 + 1$ *and* $\widetilde{C}_{q,m,\delta_2}$ *is three-weight code with the weight distribution of Table 1 for odd m and Table 2 for even m.*

Table 1. Weight distribution of $\widetilde{C}_{(q,m,\delta_2)}$ for odd m

Weight w	**Number of codeword** A_w
0	1
$(q-1)q^{m-1} - q^{(m-1)/2}$	$(q-1)(q^{m-1})(q^{m-1} + q^{(m-1)/2})/2$
$(q-1)q^{m-1}$	$(q^m - 1)(q^{m-1} + 1)$
$(q-1)q^{m-1} + q^{(m-2)/2}$	$(q-1)(q^{m-1})(q^{m-1} - q^{(m-1)/2})/2$

Table 2. Weight distribution of $\widetilde{C}_{(q,m,\delta_2)}$ for even m

Weight w	**Number of codeword** A_w
0	1
$(q-1)\,q^{m-1} - q^{(m-1)/2}$	$(q-1)(q^{(3m-2)/2} - q^{(m-2)/2})$
$(q-1)\,q^{m-1}$	$q^m - 1$
$(q-1)\,(q^{m-1} + q^{(m-2)/2})$	$q^{(m-2)/2}(q^m - q^{(m+2)/2} + q - 1)$

The following theorem informs about the weight distribution of the code $\widetilde{C}_{(q,m,\delta_3)}$.

Theorem 2.2. [7] *Let* $m \geq 4$. *The code* $\tilde{C}_{q,m,\delta_3}$ *has parameters* $[n,\tilde{k},\tilde{d}]$, *where* $\tilde{d} \geq \delta_3 + 1 = (q-1)q^m - 1 - q^{\lfloor (m+1)/2 \rfloor}$ *and*

$$\tilde{k} = \begin{cases} 2m & \textit{for odd } m, \\ \frac{5m}{2} & \textit{for even } m. \end{cases}$$

When q is an odd prime and $m \geq 4$ *is even, the code* $\tilde{C}_{(}(q,m,\delta_3)$ *has minimum distance* $\tilde{d} = \delta_3 + 1$ *and its weight distribution is given in Table 3. When q is an odd prime and* $m \geq 5$ *is odd, the code* $\tilde{C}_{(q,m,\delta_3)}$ *has minimum distance* $\tilde{d} = \delta_3 + 1$ *and its weight distribution is given in Table 4*

Table 3. The weight distribution of $\tilde{C}_{(q,m,\delta_3)}$ for even m and odd q

Weight w	**Number of codeword** A_w
0	1
$(q-1)q^{m-1}-q^{m/2}$	$(q^m-1)\left(\left(q^2-1\right)\left(q^{(3m-6)/2}+q^{m-2}\right)+2\left(q^{(m-2)/2}-1\right)\left(q^{m-3}+q^{(m-4)/2}\right)\right)/2(q+1)$
$(q-1)\left(q^{m-1}-q^{(m-2)/2}\right)$	$q\left(q^{m/2}+1\right)(q^m-1)\left(q^{m-1}+(q-1)q^{(m-2)/2}\right)/2(q+1)$
$(q-1)q^{m-1}-q^{(m-2)/2}$	$\left(q^{m+1}-2q^m+q\right)\left(q^{m/2}-1\right)\left(q^{m-1}+q^{(m-2)/2}\right)/2$
$(q-1)q^{m-1}$	$(q^m-1)\left(1+q^{(3m-2)/2}-q^{(3m-4)/2}+2q^{(3m-6)/2}-q^{m-2}\right)$
$(q-1)q^{m-1}+q^{(m-2)/2}$	$q\left(q^{m/2}+1\right)(q^m-1)(q-1)\left(q^{m-1}-q^{(m-2)/2}\right)/2(q+1)$
$(q-1)\left(q^{m-1}+q^{(m-2)/2}\right)$	$\left(q^{m+1}-2q^m+q\right)\left(q^{m/2}-1\right)\left(q^{m-1}-(q-1)q^{(m-2)/2}\right)/2(q-1)$
$(q-1)q^{m-1}+q^{m/2}$	$q^{(m-2)/2}(q^m-1)(q-1)\left(q^{m-2}-q^{(m-2)/2}\right)/2$
$(q-1)\left(q^{m-1}+q^{m/2}\right)$	$\left(q^{(m-2)/2}-1\right)(q^m-1)\left(q^{m-3}-(q-1)q^{(m-4)/2}\right)/\left(q^2-1\right)$

Table 4. The weight distribution of $\tilde{C}_{(q,m,\delta_3)}$ for odd m and odd q

Weight w	**Number of codeword** A_w
0	1
$(q-1)q^{m-1}-q^{(m+1)/2}$	$(q^m-1)\left(q^{m-3}+q^{(m-3)/2}\right)\left(q^{m-1}-1\right)/2(q+1)$
$(q-1)\left(q^{m-1}-q^{(m-1)/2}\right)$	$(q^m-1)\left(q^{m-1}+q^{(m-1)/2}\right)\left(q^{m-2}+(q-1)q^{(m-3)/2}\right)/2$
$(q-1)q^{m-1}-q^{(m-1)/2}$	$(q^m-1)\left(q^{m-2}+q^{(m-3)/2}\right)\left(q^{m+3}-q^{m+2}-q^{m-1}-q^{(m+3)/2}+q^{(m-1)/2}+q^3\right)/2(q+1)$
$(q-1)q^{m-1}$	$(q^m-1)\left(1+\left(q^2-q+1\right)q^{m-3}+(q-1)q^{2m-4}+(q-2)q^{2m-2}+q^{2m-1}\right)$
$(q-1)q^{m-1}+q^{(m-1)/2}$	$(q^m-1)\left(q^{m-2}-q^{(m-3)/2}\right)\left(q^{m+3}-q^{m+2}-q^{m-1}+q^{(m+3)/2}-q^{(m-1)/2}+q^3\right)/2(q+1)$
$(q-1)\left(q^{m-1}+q^{(m-1)/2}\right)$	$(q^m-1)\left(q^{m-1}-q^{(m-1)/2}\right)\left(q^{m-2}-(q-1)q^{(m-3)/2}\right)/2$
$(q-1)q^{m-1}+q^{(m+1)/2}$	$(q^m-1)\left(q^{m-3}-q^{(m-3)/2}\right)\left(q^{m-1}-1\right)/2(q+1)$

3. **Minimal Codeword**

The following concepts of *support* and *covering* are the origin of minimal linear codes. The definition of *support* is explained as follows.

Definition 3.1. [6] *The **support** of* $\mathbf{c}\in\mathbb{F}_q^n$ *is defined by*

$$supp(c)=\{0\leq i\leq n-1|c_i\neq 0\}.$$

Definition 3.2. [6] *A vector* $u\in\mathbb{F}_q^n$ *covers a vector* $v\in\mathbb{F}_q^n$ *if* $supp(v)$ *is subset of* $supp(u)$*.*

Minimal code is defined as follows.

Definition 3.3. [6] *A nonzero codeword* $\mathbf{u}$ *in a linear code* C *is minimal if* $\mathbf{u}$ *covers only scalar multiples of* $\mathbf{u}$*, but no other nonzero codewords in* C*. A linear code* C *is minimal if every nonzero codeword in* C *is minimal.*

The following lemma is often used in Linear Code Characterization. This lemma will also be used in this paper

Lemma 3.4 (Ashikhmin-Barg)**.** [6] *A* $[n,k,d]_q$ *linear code* C *is minimal if*

$$\frac{W_{min}}{W_{max}}>\frac{q-1}{q}. \tag{1}$$

where W_{min} *and* W_{max} *denote the minimum and maximum nonzero Hamming weights of* C *respectively.*

Using Lemma 3.4, many families of minimal linear codes with $\frac{W_{min}}{W_{max}} > \frac{q-1}{q}$ have been found, such as those by Carlet, Ding and Yuan [8]. However, most of these codes have a limited number of weights. For example, [9] introduced a type of cyclic code that has three weights, where each *codeword* has one of the three different weights. The code satisfies this lemma.

4. **Massey's Construction**

Consider the linear code $C[n,k,d]_q$. Suppose $G = [\mathbf{g_0}, \mathbf{g_1}, \dots, \mathbf{g_{n-1}}]$ the generator matrix of C. The secret S is a member of $\mathbb{F}_q$. *Share* can be determined by the following procedure. Randomly select the vector $\mathbf{u} = (u_0, u_1, \dots, u_{k-1}) \in \mathbb{F}_q^k$ such that $S = \mathbf{u}\mathbf{g}_0$. Then, the vector $\mathbf{s}$ can be calculated by

$$\mathbf{s} = (S, s_1, \dots, s_{n-1}) = uG.$$

share for each participant P_i is s_i for all $1 \le i \le n-1$.

Assume m people collect their respective *share*$\{s_{i_1}, s_{i_2}, \dots, s_{i_m}\}$ with $1 \le m \le n-1$. Then, the secret $S = s_0 + \mathbf{u}\mathbf{g}_0$ can be determined if and only if g_0 is a linear combination of $g_0, g_1, \dots, g_{n-1}$. Thus, resulting in the following proposition.

Proposition 4.1. *Let G be a generator matrix of an $[n,k,d]_q$ linear code C. In the secret-sharing based on C with respect to the second construction, a set of share $\{s_{i_1}, s_{i_2},$*
$\dots, s_{i_m}\}$ with $1 \le i_1 < i_2 < \dots < i_m \le n-1$ and $1 \le m \le n-1$, determines the secret if and only if there is a codeword

$$\mathbf{c} = (1, 0, \dots, 0, c_{i_1}, 0, \dots, 0, c_{i_m}, 0, \dots, 0)$$

in the dual code $C^{\perp}$, where $c_{i_j} \ne 0$ for at least one j.

5. **The proof of $\widetilde{C}_{(q,m,\delta_2)}$ with $m \ge 5$ is a minimal code**

In this section, we will present the results of proving that Primitive BCH codes with designed distances δ_2 and δ_3 with $m \ge 5$ satisfy Lemma 3.4, so they are minimal codes.

The first result of this research is presented in the following theorem along with its proof. The following theorem states that the Primitive BCH code with Designed Distance δ_2 satisfies Lemma 3.4.

Theorem 5.1. *Let $\delta_2 = (q-1)q^{m-1} - 1 - q^{(m-1)/2}$,*

(1) If $m \ge 5$ and m is odd, $\widetilde{C}_{(q,m,\delta_2)}$ is minimal code.

(2) If $m \ge 6$ and m is even, $\widetilde{C}_{(q,m,\delta_2)}$ is minimal code.

Proof. (a) From the Table 1, we know that $\widetilde{C}_{(q,m,\delta_2)}$ with odd m has nonzero minimum weight $W_{min} = (q-1)q^{m-1} - q^{(m-1)/2}$ and maximum weight $W_{max} = (q-1)q^{m-1} + q^{(m-2)/2}$.

Using Lemma 3.4, we will proof that

$$\frac{(q-1)\,q^{m-1}-q^{(m-1)/2}}{(q-1)\,q^{m-1}+q^{(m-1)/2}}>\frac{q-1}{q}.$$

Suppose $A=(q-1)q^{m-1}$ and $B=q^{(m-1)/2}$. So that the inequality becomes

$$\begin{aligned}\frac{A-B}{A+B}&>\frac{q-1}{q}\\(A-B)q&>(A+B)(q-1)\\Aq-Bq&>Aq-A+Bq-B\\A&>2Bq-B)\\A&>B(2q-1)\end{aligned}$$

Substitute $A=(q-1)q^{m-1}$ and $B=q^{(m-1)/2}$ back into the inequality above.

$$\begin{aligned}(q-1)q^{m-1}&>q^{(m-1)/2}(2q-1).\\(q-1)q^{(m-1)/2}&>2q-1.\end{aligned}$$

Since q is an odd prime number and $m>5$ is odd, $q^{(m-1)/2}$ is a large positive number, making the left side larger than the right side. Thus, it is proved that for q odd primes and $m>5$ odd,

$$\frac{(q-1)\,q^{m-1}-q^{(m-1)/2}}{(q-1)\,q^{m-1}+q^{(m-1)/2}}>\frac{q-1}{q}.$$

(b) From Table 2, it can be seen that $\widetilde{C}_{(q,m,\delta_2)}$ with even m have a nonzero minimum weight ($W_{min}=(q-1)\,q^{m-1}-q^{(m-1)/2}$ and maximum weight ($W_{max}=(q-1)\,(q^{m-1}+q^{(m-2)/2})$.

Using Lemma 3.4, we will proof that

$$\frac{(q-1)q^{m-1}-q^{(m-2)/2}}{(q-1)(q^{m-1}+q^{(m-2)/2})}>\frac{q-1}{q}.$$

with algebraic manipulation the above inequality becomes

$$\frac{(q-1)q^{m-1}-q^{(m-2)/2}}{q^{m-1}+q^{(m-2)/2}}>\frac{(q-1)^2}{q}.$$

Suppose $A = q^{m-1}$ and $B = q^{(m-2)/2}$. So that the above inequality becomes

$$\begin{aligned}
\frac{(q-1)A - B}{A+B} &> \frac{(q-1)^2}{q} \\
q\{(q-1)A - B\} &> (q-1)^2(A+B) \\
A(q^2-q) - Bq &> (q^2-2q+1)(A+B) \\
Aq^2 - Aq - Bq &> Aq^2 - 2Aq + A + Bq^2 - 2Bq + B \\
Aq + Bq &> A + Bq^2 + B \\
Aq - A &> Bq^2 + B - Bq \\
(q-1)A &> (q^2-q+1)B
\end{aligned}$$

subtitute $A = q^{m-1}$ and $B = q^{(m-2)/2}$ back into the inequality above.

$$\begin{aligned}
(q-1)q^{m-1} &> (q^2-q+1)q^{(m-2)/2} \\
(q-1)q^{m/2} &> (q^2-q+1) \\
(q-1)q^{m/2} - 1 &> q^2 - q \\
(q-1)q^{m/2} - (q-1)\frac{1}{q-1} &> (q-1)q \\
q^{m/2} - \frac{1}{q-1} &> q
\end{aligned}$$

since q is an odd prime number then $0 < \frac{1}{q-1} \leq 1$, and since $m \geq 5$ then $q^{m/2} > q$, so the left side will always be greater than the right side. So it is proven that

$$\frac{(q-1)q^{m-1} - q^{(m-2)/2}}{(q-1)(q^{m-1} + q^{(m-2)/2})} > \frac{q-1}{q}.$$

□

The next result of this research is presented in the following theorem and its proof.

6. Proof of $\widetilde{C}_{(q,m,\delta_3)}$ with $m \geq 5$ is a minimal code

The following theorem states that the Primitive BCH code with Designed Distance δ_3 satisfies Lemma 3.4.

Theorem 6.1. *Let* $\delta_2 = (q-1)q^{m-1} - 1 - q^{(m+1)/2}$,

(1) If $m \geq 6$ *and* m *is even, then* $\widetilde{C}_{(q,m,\delta_3)}$ *is minimal code.*
(2) If $m \geq 5$ *and* m *is odd, then* $\widetilde{C}_{(q,m,\delta_3)}$ *is minimal code.*

Proof. (a) From the table 3, can be seen that for even m the code $\widetilde{C}_{(q,m,\delta_3)}$ have nonzero minimal weight $(q-1)q^{m-1} - q^{m/2}$ and maximum weight $(q-1)\left(q^{m-1} + q^{m/2}\right)$.

Using Lemma 3.4, we will show that

$$\frac{(q-1)q^{m-1} - q^{m/2}}{(q-1)(q^{m-1} + q^{m/2})} > \frac{q-1}{q}$$

multiply both side by $(q-1)$ so that

$$\frac{(q-1)q^{m-1} - q^{m/2}}{(q-1)(q^{m-1} + q^{m/2})} \cdot (q-1) > \frac{q-1}{q} \cdot (q-1)$$
$$\frac{(q-1)q^{m-1} - q^{m/2}}{(q^{m-1} + q^{m/2})} > \frac{(q-1)^2}{q}$$

suppose $A = q^{m-1}$ and $B = q^{m/2}$. So that the inequality becomes

$$\begin{aligned}
\frac{(q-1)A - B}{A+B} &> \frac{(q-1)^2}{q} \\
q\{(q-1)A - B)\} &> (q-1)^2(A+B) \\
A(q^2 - q) - Bq &> (q^2 - 2q + 1)(A+B) \\
Aq^2 - Aq - Bq &> Aq^2 - 2Aq + A + Bq^2 - 2Bq + B \\
Aq + Bq &> A + Bq^2 + B \\
Aq - A &> Bq^2 - Bq + B \\
(q-1)A &> (q^2 - q + 1)B
\end{aligned}$$

sustitude $A = q^{m-1}$ and $B = q^{m/2}$ back into the inequality above

$$\begin{aligned}
(q-1)q^{m-1} &> (q^2 - q + 1)q^{m/2} \\
(q-1)q^{(m-2)/2} &> (q^2 - q + 1) \\
(q-1)q^{(m-2)/2} - 1 &> q^2 - q \\
(q-1)q^{(m-2)/2} - (q-1)\frac{1}{q-1} &> (q-1)q \\
q^{(m-2)/2} - \frac{1}{q-1} &> q \\
q^{(m-2)/2} &> q + \frac{1}{q-1}
\end{aligned}$$

Since q is an odd prime number and $m > 5$ so the left side will always greater than right side. So it is proven that for q odd prime number and even $m > 5$

$$\frac{(q-1)q^{m-1} - q^{m/2}}{(q-1)(q^{m-1} + q^{m/2})} > \frac{q-1}{q}$$

(b) From the table 4, we know that for odd m, $\widetilde{C}_{(q,m,\delta_3)}$ have nonzero minimal weight $(q-1)q^{m-1} - q^{(m+1)/2}$ and maximum weight $(q-1)q^{m-1} + q^{(m-1)/2}$.

Using Lemma 3.4, we will prove that

$$\frac{(q-1)q^{m-1} - q^{(m+1)/2}}{(q-1)q^{m-1} + q^{(m+1)/2}} > \frac{q-1}{q}$$

let $A = (q-1)q^{m-1}$ and $B = q^{(m+1)/2}$, then

$$\begin{aligned}
\frac{A-B}{A+B} &> \frac{q-1}{q} \\
(A-B)q &> (A+B)(q-1) \\
Aq - Bq &> Aq - A + Bq - B \\
A &> 2Bq - B \\
A &> B(2q-1)
\end{aligned}$$

Substitute $A = (q-1)q^{m-1}$ and $B = q^{(m+1)/2}$ back to the inequality above

$$\begin{aligned}
(q-1)q^{m-1} &> q^{(m+1)/2}(2q-1) \\
(q-1)q^{(m^2-1)/2} &> 2q-1
\end{aligned}$$

Because (q) is odd prime number and $(m \geq 5)$, $(q^{(m^2-1)/2})$ is a large positive number, making the left side larger than the right side. Thus, it is proved that for q odd primes, $m \geq 5$ and odd m,

$$\frac{(q-1)q^{m-1} - q^{(m+1)/2}}{(q-1)q^{m-1} + q^{(m+1)/2}} > \frac{q-1}{q}$$

□

7. Example of Secret Sharing Schemes Based On Dual Code of $\widetilde{C}_{(q,m,\delta_2)}$ with $m \geq 5$ using Massey's Construction

The next goal of this paper is to provide an example of a secret sharing scheme based on the dual code of $\widetilde{C}_{(q,m,\delta_2)}$ with $m \geq 5$ using Massey's Construction.

Example 7.1. *Let $q = 2$, $m = 5$, then $n = q^m - 1 = 31$ and designed distance $\delta_2 = (q-1)q^{m-1} - 1 - q^{(m+1)/2} = 11$. With the commonly known technique to construct the generator matrix of cyclic codes, the generator matrix of $\widetilde{C}_{(2,5,11)}$ is obtained, that is*

$$\widetilde{G} = \left[\begin{array}{ccccccccccccccccccccccccccccccc}
1&1&1&1&1&1&1&0&1&1&0&1&0&1&1&0&0&1&0&1&1&1&0&0&0&0&0&0&0&0&0 \\
0&1&1&1&1&1&1&1&0&1&1&0&1&0&1&1&0&0&1&0&1&1&1&0&0&0&0&0&0&0&0 \\
0&0&1&1&1&1&1&1&1&0&1&1&0&1&0&1&1&0&0&1&0&1&1&1&0&0&0&0&0&0&0 \\
0&0&0&1&1&1&1&1&1&1&0&1&1&0&1&0&1&1&0&0&1&0&1&1&1&0&0&0&0&0&0 \\
0&0&0&0&1&1&1&1&1&1&1&0&1&1&0&1&0&1&1&0&0&1&0&1&1&1&0&0&0&0&0 \\
0&0&0&0&0&1&1&1&1&1&1&1&0&1&1&0&1&0&1&1&0&0&1&0&1&1&1&0&0&0&0 \\
0&0&0&0&0&0&1&1&1&1&1&1&1&0&1&1&0&1&0&1&1&0&0&1&0&1&1&1&0&0&0 \\
0&0&0&0&0&0&0&1&1&1&1&1&1&1&0&1&1&0&1&0&1&1&0&0&1&0&1&1&1&0&0 \\
0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&0&1&1&0&1&0&1&1&0&0&1&0&1&1&1&0 \\
0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&0&1&1&0&1&0&1&1&0&0&1&0&1&1&1
\end{array}\right]$$

Based on matrix $\widetilde{G}$ and Proposition 4.1, there is no dictator participant in the example textitsecret-sharing scheme based on the code dual of code $\widetilde{C}_{(q,m,\delta_2)}$. The participant P_i with $1 \leq i \leq n-1$ is in $(q-1)q^{k-2} = (2-1)2^{10-2} = 2^8 = 256$ of $q^{k-1} = 2^{10-1} = 512$ minimal access set.

By using the common method, the parity check matrix of $\widetilde{C}_{(2,5,11)}$ *is obtained, that is*

$$\widetilde{H}=\begin{bmatrix}
1&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&0&0&0&0&1&1
\end{bmatrix}$$

Suppose the secret is 0. *The Massey's construction will be applied to the dual code of* $\widetilde{C}_{(q,m,\delta_2)}$ *to construct the secret sharing scheme. A vector* $\mathbf{u}\in\mathbb{F}_2^{21}$ *needs to be chosen such that* $S=\mathbf{u}\widetilde{\mathbf{h}}_0$, *where* $\widetilde{h}_0$ *is the first column of the matrix* $\widetilde{H}$ *Misalkan* $\mathbf{u}=(0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0)$. *Then the following share can be obtained:*

$$\begin{aligned}\mathbf{s}&=\mathbf{u}\widetilde{H}\\&=(S,1,1,1,0,1,0,1,0,1,1,0,1,0,1,0,1,0,1,0,1,1,0,1,1,1,1,1,1,1,0).\end{aligned}$$

Suppose there are 30 *participants* $P_1,P_2,\ldots,P_{30}$. *Each participant* P_i *gets* s_i *as its share. Now, find the set of participants who can reconstruct the secret. That is, the set of participants such that* $\widetilde{\mathbf{h}}_0$ *is a linear combination of the column of* $\widetilde{H}$ *corresponding to the participants in the set. Here are* 3 *of* $q^{k-1}=2^{10-1}=512$ *sets of participants that can produce secrets:* $\{P_1,P_2,P_3,P_4,P_5,P_6,P_8,P_9,P_{11},P_{13},P_{14},P_{17},P_{19},P_{20},P_{21}\}$, $\{P_1,P_2,P_3,P_4,P_5,P_6,P_8,P_{10},P_{12},P_{10},P_{15},P_{18},P_{19},P_{21},P_{22},P_{23},P_{26},P_{28},P_{29},P_{30}\}$, *and* $\{P_1,P_2,P_3,P_4,P_7,P_{10},P_{16},P_{17},P_{18},P_{20},P_{21},P_{22},P_{24},P_{25},P_{26}\}$

Based on Proposition 4.1, these participant sets can produce secret. Other minimal access sets can be computed using proggramming.

Suppose the group of participants recovering share is $\{P_1,P_2,P_3,P_4,P_5,P_6,P_8,P_9,P_{11},P_{13},P_{14},P_{17},P_{19},P_{20},P_{21}\}$, *can be seen that* $\widetilde{\mathbf{h}}_0=\{1\cdot\widetilde{\mathbf{h}}_1+1\cdot\widetilde{\mathbf{h}}_2+1\cdot\widetilde{\mathbf{h}}_3+1\cdot\widetilde{\mathbf{h}}_4+1\cdot\widetilde{\mathbf{h}}_5+1\cdot\widetilde{\mathbf{h}}_6+1\cdot\widetilde{\mathbf{h}}_8+1\cdot\widetilde{\mathbf{h}}_9+1\cdot\widetilde{\mathbf{h}}_{11}+1\cdot\widetilde{\mathbf{h}}_{13}+1\cdot\widetilde{\mathbf{h}}_{14}+1\cdot\widetilde{\mathbf{h}}_{17}+1\cdot\widetilde{\mathbf{h}}_{19}+1\cdot\widetilde{\mathbf{h}}_{20}+1\cdot\widetilde{\mathbf{h}}_{21}\}$

So that we get share $S = \mathbf{u}\widetilde{\mathbf{h}}_0 = 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 0 + 1 \cdot 1 + 1 \cdot 0 + 1 \cdot 0 + 1 \cdot 1 + 1 \cdot 0 + 1 \cdot 0 + 1 \cdot 1 + 1 \cdot 0 + 1 \cdot 0 + 1 \cdot 1 + 1 \cdot 1 = 0.$

8. Example of Secret Sharing Schemes Based On Dual Code of $\widetilde{C}_{(q,m,\delta_3)}$ with $m \geq 5$ using Massey's Construction

The next goal of this paper is to give an example of a secret sharing scheme based on the dual code of $\widetilde{C}_{(q,m,\delta_3)}$ with $m \geq 5$ with Massey construction.

Example 8.1. *Let* $q = 2$*,* $m = 5$*, then* $n = 2^m - 1 = 2^5 - 1 = 31$ *and designed distance* $\delta_3 = (q-1)q^{m-1} - 1 - q^{(m+1)/2} = 7$ *.*

By constructing the generator matrix of a commonly known cyclic code, the generator matrix of the code $\widetilde{C}_{(2,5,7)}$ *is obtained, that is*

$$\widetilde{G} = \begin{bmatrix}
1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&1&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&1&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&1&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&1&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&1&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&1&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&1&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&1&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&1&1
\end{bmatrix}$$

Based on matrix $\widetilde{G}$ *and Proposition 4.1, there is no dictator participant in this example. The participant* P_i *with* $1 \leq i \leq n-1$ *is in* $(q-1)q^{k-2} = (2-1)2^{15-2} = 2^{13} = 8192$ *of* $q^{k-1} = 2^{15-1} = 16384$ *minimal access set.*

In a common way, one can also obtain the parity check matrix of $\widetilde{C}_{(2,5,7)}$*, as follows*

$$\widetilde{H} = \begin{bmatrix}
1&1&1&1&0&1&0&1&1&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&1&1&0&1&0&1&1&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&1&1&0&1&0&1&1&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&1&1&1&0&1&0&1&1&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&1&0&1&0&1&1&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&1&1&1&0&1&0&1&1&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&1&1&1&0&1&0&1&1&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&1&1&1&0&1&0&1&1&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&1&1&0&1&0&1&1&1&1&1&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&1&1&1&0&1&0&1&1&1&1&1&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&1&0&1&1&1&1&1&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&1&0&1&1&1&1&1&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&1&0&1&1&1&1&1&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&1&0&1&1&1&1&1&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&1&0&1&1&1&1&1&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&1&0&1&1&1&1&1&0&0&0&1
\end{bmatrix}$$

In this step, the secret sharing scheme will be built. Since in constructing th secret sharing scheme the dual code of $\widetilde{C}(q, m, \delta_3)$ *will be used, the parity check matrix of the code will be used as the generator matrix. Suppose the secret is* 1*. The Massey's construction will be applied to this code to build the secret sharing scheme. The vector* $\mathbf{u} \in \mathbb{F}_2^{16}$ *needs to be chosen such that* $S = \mathbf{u}\widetilde{\mathbf{h}}_0$*, where* $\widetilde{\mathbf{h}}_\mathbf{0}$ *is the first column of the matrix* $\widetilde{H}$*. Let* $\mathbf{u} = (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$*. Then the following share can be obtained:*

$$\begin{aligned}\mathbf{s} &= \mathbf{u}\widetilde{H} \\ &= (S, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0).\end{aligned}$$

Suppose there are 30 *participants* $P_1, P_2, \ldots, P_{30}$*. Each participant* P_i *gets* s_i *as its share. Now find the set of participants who can recontruct the secret. That is, the set of participants such that* $\widetilde{\mathbf{h}}_0$ *is a linear combination of the columns of* $\widetilde{H}$ *corresponding to the participants in the set. Here are* 3 *of* $q^{k-1} = 2^{15-1} = 16384$ *sets of participants that can produce secrets:* $\{P_4, P_5, P_6, P_7, P_{12}, P_{15}, P_{16}\}$*,* $\{P_4, P_5, P_6, P_7, P_{12}, P_{14}, P_{15}, P_{16}, P_{18}, P_{19}, P_{20}, P_{21}, P_{26}, P_{29}, P_{30}\}$*, and* $\{P_8, P_{16}, P_{18}, P_{22}, P_{23}, P_{25}, P_{26}\}$

Example of the set of participants that can produce the secret are obtained from the codeword on $\widetilde{C}_{(2,5,7)}$ *whose first component is* 1*. While the search for the codeword can be done with programming.*

Suppose the group of participants recovering share is $\{P_4, P_5, P_6, P_7, P_{12}, P_{15}, P_{16}\}$*, can be seen that* $\widetilde{\mathbf{h}}_0 = 1 \cdot \widetilde{\mathbf{h}}_4 + 1 \cdot \widetilde{\mathbf{h}}_5 + 1 \cdot \widetilde{\mathbf{h}}_6 + 1 \cdot \widetilde{\mathbf{h}}_7 + 1 \cdot \widetilde{\mathbf{h}}_{12} + 1 \cdot \widetilde{\mathbf{h}}_{15} + 1 \cdot \widetilde{\mathbf{h}}_{16} + 1 \cdot$*. So, we get share* $S = \mathbf{u}\widetilde{\mathbf{h}}_0 = 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 0 + 1 \cdot 0 + 1 \cdot 0 + 1 \cdot 1 + 1 \cdot 0 + 1 \cdot 0 = 1$.

9. **CLOSING**

From this study it is proved that $\widetilde{C}_{(q,m,\delta_2)}$ and $\widetilde{C}_{(q,m,\delta_3)}$ with $m \geq 5$ are minimal codes. In addition, this research also succefully present an example of the construction of a secret sharing scheme based on the dual code of the code using Massey's construction. Nevertheless, there are still open problem related to linear code based on secret sharing schemes. One of them is to prove the minimality of the codes $\widetilde{C}_{(q,m,\delta_2)}$ and $\widetilde{C}_{(q,m,\delta_3)}$ when $m \leq 5$. Besides using the Ashikhmin-Barg criterion, other criteria can also be used as in [10] and [11].

REFERENCES

[1] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979. .

[2] R. J. McEliece and D. V. Sarwate, "On sharing secrets and reed-solomon codes," *Commun. ACM*, vol. 24, pp. 583–584, 1981. .

[3] E. Brickell, *Some Ideal Secret Sharing Schemes in : J. Quisquater Jean-Jacques and Vandewalle (Ed.).* Springer Berlin Heidelberg, 1990. .

[4] J. L. Massey, "Minimal codewords and secret sharing," in *Proceedings of the 6th joint Swedish-Russian international workshop on information theory*, pp. 276–279, 1993. .

[5] A. Ashikhmin and A. Barg, "Minimal vectors in linear codes," *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 2010–2017, 1998. .

[6] W. C. Huffman, J.-L. Kim, and P. Solé, *Concise Encyclopedia of Coding Theory*. Chapman and Hall/CRC, 2021. .

[7] C. Ding, C. Fan, and Z. Zhou, "The dimension and minimum distance of two classes of primitive bch codes," *Finite Fields Their Appl*, vol. 45, pp. 237–263, 2016. .

[8] C. Carlet, C. Ding, and J. Yuan, "Linear codes from perfect nonlinear mappings and their secret sharing schemes," *IEEE Transactions on Information Theory*, vol. 51, pp. 2089–2102, 2005. .

[9] Z. Zhou and C. Ding, "A class of three-weight cyclic codes," *Finite Fields and Their Applications*, vol. 25, pp. 79–93, 2014. .

[10] S. Chang and J. Hyun, "Linear codes from simplicial complexes," *Des. Codes Cryptogr*, vol. 86, pp. 2167–2181, 2018. .

[11] C. Ding, Z. Heng, and Z. Zhou, "Minimal binary linear codes," *IEEE Transactions on Information Theory*, vol. 64, pp. 6536–6545, 2018. .