Another Generalization of the Reed-Muller Codes

Cunsheng Ding, Chunlei Li, and Yongbo Xia

Abstract

The punctured binary Reed-Muller code is cyclic and was generalized into the punctured generalized Reed-Muller code over GF$(q)$ in the literature. The major objective of this paper is to present another generalization of the punctured binary Reed-Muller code. Another objective is to construct a family of reversible cyclic codes that are related to the newly generalized Reed-Muller codes.

Index Terms

BCH codes, cyclic codes, linear codes, punctured Reed-Muller codes, punctured generalized Reed-Muller codes, Reed-Muller codes.

I. INTRODUCTION

Throughout this paper, let $p$ be a prime and let $q = p^s$ be a power of $p$, where $s$ is a positive integer. An $[n,k,d]$ code $C$ over GF$(q)$ is a $k$-dimensional subspace of GF$(q)^n$ with minimum (Hamming) distance $d$. An $[n,k]$ code $C$ over GF$(q)$ is called cyclic if $(c_0,c_1,\cdots,c_{n-1}) \in C$ implies $(c_{n-1},c_0,c_1,\cdots,c_{n-2}) \in C$. By identifying any vector $(c_0,c_1,\cdots,c_{n-1}) \in$ GF$(q)^n$ with $c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} \in$ GF$(q)[x]/(x^n - 1)$, any code $C$ of length $n$ over GF$(q)$ corresponds to a subset of the quotient ring GF$(q)[x]/(x^n - 1)$. A linear code $C$ is cyclic if and only if the corresponding subset in GF$(q)[x]/(x^n - 1)$ is an ideal of the ring GF$(q)[x]/(x^n - 1)$.

Note that every ideal of GF$(q)[x]/(x^n - 1)$ is principal. Let $C = \langle g(x) \rangle$ be a cyclic code, where $g(x)$ is monic and has the smallest degree among all the generators of $C$. Then $g(x)$ is unique and called the generator polynomial, and $h(x) = (x^n - 1)/g(x)$ is referred to as the check polynomial of $C$.

The original Reed-Muller codes were discovered by Reed and Muller independently in 1964 [12], [13]. These codes are standard materials in textbooks and research monographs on coding theory, and were employed in space communication in the Mariner 9 Spacecraft. These facts show the importance of the Reed-Muller codes.

Recently, Reed-Muller codes have become a hot topic in coding theory due to the fact that they belong to the classes of locally testable codes and locally decodable codes, which makes them useful in the design of probabilistically checkable proofs in computational complexity theory [15].

The original Reed-Muller codes are binary and linear, but not cyclic. However, the punctured Reed-Muller codes are cyclic. The punctured binary Reed-Muller code was generalized into the punctured generalized Reed-Muller code over GF$(q)$ in the literature [11], [2], [6], [5], [7]. In this paper, we present another generalization of the punctured binary Reed-Muller code, and study properties of the generalized codes. We also construct a family of reversible cyclic codes from the newly generalized Reed-Muller codes and analyse their parameters.

C. Ding’s research was supported by the Hong Kong Research Grants Council, under Grant No. 16301114.

C. Ding is with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China (Email: cding@ust.hk).

C. Li is with the Department of Electrical Engineering and Computer Science, University of Stavanger, Stavanger, 4036, Norway (Email: chunlei.li@uis.no).

Y. Xia is with the Department of Mathematics and Statistics, South-Central University for Nationalities, Wuhan 430074, China (Email: xia@mail.scuec.edu.cn).
II. $q$-CYCLOTOMIC COSETS MODULO $n$ AND AUXILIARIES

To deal with cyclic codes of length $n$ over $\text{GF}(q)$, we have to study the canonical factorization of $x^n - 1$ over $\text{GF}(q)$. To this end, we need to introduce $q$-cycloctic cosets modulo $n$. Note that $x^n - 1$ has no repeated factors over $\text{GF}(q)$ if and only if $\gcd(n, q) = 1$. Throughout this paper, we assume that $\gcd(n, q) = 1$.

Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, denoting the ring of integers modulo $n$. For any $s \in \mathbb{Z}_n$, the $q$-cycloctic coset of $s$ modulo $n$ is defined by

$$C_s = \{sq^i \text{ mod } n : 0 \leq i \leq \ell_s - 1\} \subseteq \mathbb{Z}_n,$$

where $\ell_s$ is the smallest positive integer such that $s \equiv sq^\ell_s \pmod{n}$, and is the size of the $q$-cycloctic coset. The smallest integer in $C_s$ is called the coset leader of $C_s$. Let $\Gamma_{n,q}$ be the set of all the coset leaders. We have then $C_s \cap C_t = \emptyset$ for any two distinct elements $s$ and $t$ in $\Gamma_{n,q}$, and

$$\bigcup_{s \in \Gamma_{n,q}} C_s = \mathbb{Z}_n. \tag{1}$$

Hence, the distinct $q$-cycloctic cosets modulo $n$ partition $\mathbb{Z}_n$.

Let $m = \text{ord}_n(q)$, and let $\alpha$ be a generator of $\text{GF}(q^m)^*$. Put $\beta = \alpha^{(q^m-1)/n}$. Then $\beta$ is a primitive $n$-th root of unity in $\text{GF}(q^m)$. The minimal polynomial $m_s(x)$ of $\beta^s$ over $\text{GF}(q)$ is a monic polynomial of the smallest degree over $\text{GF}(q)$ with $\beta^s$ as a zero. It is now straightforward to see that this polynomial is given by

$$m_s(x) = \prod_{i \in C_s} (x - \beta^i) \in \text{GF}(q)[x], \tag{2}$$

which is irreducible over $\text{GF}(q)$. It then follows from (1) that

$$x^n - 1 = \prod_{s \in \Gamma_{n,q}} m_s(x) \tag{3}$$

which is the factorization of $x^n - 1$ into irreducible factors over $\text{GF}(q)$. This canonical factorization of $x^n - 1$ over $\text{GF}(q)$ is fundamental for the study of cyclic codes.

III. THE PUNCTURED GENERALIZED REED-MULLER CODES OVER $\text{GF}(q)$

Let $m$ be a positive integer and let $n = q^m - 1$ from now on, where $q = p^s$, $p$ is a prime and $s$ is a positive integer. For any integer $a$ with $0 \leq a \leq n - 1$, we have the following $q$-adic expansion

$$a = \sum_{j=0}^{m-1} a_j q^j,$$

where $0 \leq a_j \leq q - 1$. The $q$-weight of $a$, denoted by $\omega(a)$, is defined by

$$\omega(a) = \sum_{j=0}^{m-1} a_j.$$

Let $\alpha$ be a generator of $\text{GF}(q^m)^*$. Let $\ell = \ell_1(q-1) + \ell_0 < q(m-1)$, where $0 \leq \ell_0 \leq q - 1$. The $\ell$-th order punctured generalized Reed-Muller code $\text{PGRM}_{q}(\ell, m)$ over $\text{GF}(q)$ is the cyclic code of length $n = q^m - 1$ with generator polynomial

$$g_R(x) := \prod_{1 \leq a < n-1 \atop \omega(a) < (q-1)m-\ell} (x - \alpha^a). \tag{4}$$

Since $\omega_q(a)$ is a constant function on each $q$-cycloctic coset modulo $n$, $g_R(x)$ is a polynomial over $\text{GF}(q)$. By definition, $g_R(x)$ is a divisor of $x^n - 1$. 
The parameters of the punctured generalized Reed-Muller code are known and given in the following theorem [1, Theorem 5.4.1].

**Theorem 1.** The code \( \text{PGRM}_q(\ell, m) \) has length \( n = q^m - 1 \), dimension

\[
k = \sum_{i=0}^{\ell} \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{i-jq+m-1}{i-jq},
\]

and minimum distance

\[
d = (q - \ell_0)q^{m-\ell_1-1} - 1.
\]

Let \( \mathbf{1} = (1, 1, \cdots, 1) \in \text{GF}(q)^n \) and

\[
\text{GF}(q)\mathbf{1} = \{a \mathbf{1} : a \in \text{GF}(q)\}.
\]

Then \( \text{GF}(q)\mathbf{1} \) is a subspace of \( \text{GF}(q)^n \) with dimension 1. A proof of the following property can be found in [2].

**Theorem 2.** The dual codes \( \text{PGRM}_q(\ell, m)^\perp \) and the original ones \( \text{PGRM}_q(\ell', m) \) are related as follows:

\[
\text{PGRM}_q(\ell, m)^\perp = (\text{GF}(q)\mathbf{1})^\perp \cap \text{PGRM}_q(m(q-1)-\ell, m).
\]

When \( q = 2 \), \( \text{PGRM}_q(\ell, m) \) becomes the punctured binary Reed-Muller code. Hence, \( \text{PGRM}_q(\ell, m) \) is indeed a generalization of the original punctured binary Reed-Muller code. Other properties of the code \( \text{PGRM}_q(\ell, m) \) can be found in [1] and the book chapter [2].

The only purpose of introducing the codes \( \text{PGRM}_q(\ell, m) \) in this section is to show the difference between the punctured generalized Reed-Muller codes \( \text{PGRM}_q(\ell, m) \) and the new family of generalized Reed-Muller codes to be introduced in the next section.

**IV. ANOTHER GENERALIZATION OF THE PUNCTURED BINARY REED-MULLER CODES**

**A. The newly generalized codes \( \mathbb{U}(q, m, \ell) \)**

Let \( m \) be a positive integer and let \( n = q^m - 1 \), where \( q = p^s \), \( p \) is a prime and \( s \) is a positive integer. For any integer \( a \) with \( 0 \leq a \leq n - 1 \), we have the following \( q \)-adic expansion

\[
a = \sum_{j=0}^{m-1} a_j q^j,
\]

where \( 0 \leq a_j \leq q - 1 \). The Hamming weight of \( a \), denoted by \( \text{wt}(a) \), is the the Hamming weight of the vector \((a_0, a_1, \cdots, a_{m-1})\).

Let \( \alpha \) be a generator of \( \text{GF}(q^m)^* \). For any \( 1 \leq \ell \leq m \), we define a polynomial

\[
g_{(q,m,\ell)}(x) = \prod_{1 \leq a \leq n-1, 1 \leq \text{wt}(a) \leq \ell} (x - \alpha^a).
\]  

Since \( \text{wt}(a) \) is a constant function on each \( q \)-cyclotomic coset modulo \( n \), \( g_{(q,m,\ell)}(x) \) is a polynomial over \( \text{GF}(q) \). By definition, \( g_{(q,m,\ell)}(x) \) is a divisor of \( x^n - 1 \).

Let \( \mathbb{U}(q, m, \ell) \) denote the cyclic code over \( \text{GF}(q) \) with length \( n \) and generator polynomial \( g_{(m,q,\ell)}(x) \).

To analyse this code, we set

\[
I(q, m, \ell) = \{1 \leq a \leq n - 1 : 1 \leq \text{wt}(a) \leq \ell\}.
\]

The dimension of the code \( \mathbb{U}(q, m, \ell) \) is equal to \( n - |I(q, m, \ell)| \).
Theorem 3. Let $m \geq 2$ and $1 \leq \ell \leq m - 1$. Then $\mathcal{U}(q,m,\ell)$ has parameters $[n,k,d \geq (q^{\ell+1} - 1)/(q-1)]$, where

$$k = q^m - \sum_{i=0}^{\ell} \binom{m}{i} (q-1)^i.$$ 

Proof: As shown earlier, $I(q,m,\ell)$ is the union of some $q$-cyclotomic cosets modulo $n$. The total number of elements in $\mathbb{Z}_n$ with Hamming weight $i$ is equal to $\binom{m}{i} (q-1)^i$. It then follows that

$$|I(q,m,\ell)| = \sum_{i=1}^{\ell} \binom{m}{i} (q-1)^i.$$ 

Hence, the dimension $k$ of the code is given by

$$k = q^m - \sum_{i=1}^{\ell} \binom{m}{i} (q-1)^i.$$ 

Note that every integer $a$ with $1 \leq a \leq (q^{\ell+1} - 1)/(q-1) - 1$ has Hamming weight $\text{wt}(a) \leq \ell$. By definition,

$$\{1,2,3,\ldots,(q^{\ell+1} - 1)/(q-1) - 1\} \subset I(q,m,\ell).$$ 

It then follows from the BCH bound that $d \geq (q^{\ell+1} - 1)/(q-1)$.

When $q = 2$, the code $\mathcal{U}(q,m,\ell)$ clearly becomes the classical punctured binary Reed-Muller code. Hence, $\mathcal{U}(q,m,\ell)$ is indeed a generalization of the original punctured binary Reed-Muller code.

Open Problem 1. Is it true that the minimum distance of the code $\mathcal{U}(q,m,\ell)$ is equal to $(q^{\ell+1} - 1)/(q-1)$?

Example 1. The following is a list of examples of the code $\mathcal{U}(q,m,\ell)$.

- When $(q,m,\ell) = (3,3,1)$, $\mathcal{U}(q,m,\ell)$ has parameters $[26,20,4]$.
- When $(q,m,\ell) = (3,4,1)$, $\mathcal{U}(q,m,\ell)$ has parameters $[80,72,4]$.
- When $(q,m,\ell) = (3,4,2)$, $\mathcal{U}(q,m,\ell)$ has parameters $[80,48,13]$.
- When $(q,m,\ell) = (3,4,3)$, $\mathcal{U}(q,m,\ell)$ has parameters $[80,16,40]$.
- When $(q,m,\ell) = (4,3,1)$, $\mathcal{U}(q,m,\ell)$ has parameters $[63,54,5]$.

B. The dual codes $\mathcal{U}(q,m,\ell)^\perp$

When $q = 2$, the parameters of the dual code $\mathcal{U}(q,m,\ell)^\perp$ are given by Theorems [1] and [2]. Therefore, we need to study the dual code $\mathcal{U}(q,m,\ell)^\perp$ for the case $q > 2$ only.

We will need the following theorem ([8], see also [11, p. 153]).

Theorem 4 (Hartmann-Tzeng Bound). Let $C$ be a cyclic code of length $n$ over $\text{GF}(q)$ with defining set $T$. Let $A$ be a set of $\delta - 1$ consecutive elements of $T$ and $B = \{jb \mod n : 0 \leq j \leq s\}$, where $\gcd(b,n) < \delta$. If $A + B \subset T$, then the minimum distance $d$ of $C$ satisfies $d \geq \delta + s$.

The following theorem gives information on the parameters of the dual code $\mathcal{U}(q,m,\ell)^\perp$.

Theorem 5. Let $m \geq 2$ and $1 \leq \ell \leq m - 1$. The dual code $\mathcal{U}(q,m,\ell)^\perp$ has parameters $[n,k^\perp,d^\perp]$, where

$$k^\perp = \sum_{i=1}^{\ell} \binom{m}{i} (q-1)^i.$$ 

The minimum distance $d^\perp$ of $\mathcal{U}(q,m,\ell)^\perp$ is lower bounded by

$$d^\perp \geq q^{m-\ell} + q - 2.$$
Proof: The desired conclusion on the dimension of $\mathcal{U}(q,m,\ell)^\perp$ follows from the dimension of $\mathcal{U}(q,m,\ell)$. What remains to be proved is the lower bound on the minimum distance $d^\perp$. Let $\mathcal{U}(q,m,\ell)^c$ denote the complement of $\mathcal{U}(q,m,\ell)$, which is generated by the check polynomial of $\mathcal{U}(q,m,\ell)$. It is well known that $\mathcal{U}(q,m,\ell)^c$ and $\mathcal{U}(q,m,\ell)^\perp$ have the same length, dimension and minimum distance.

By definition, the defining set of $\mathcal{U}(q,m,\ell)^c$ is

$$I(q,m,\ell)^c := \{0\} \cup \{1 \leq b \leq n-1 : \text{wt}(b) \geq \ell+1\}.$$ 

Let $b = q^{m-\ell} + q^{m-\ell+1} + \cdots + q^{m-1}$. Define

$$A = \{a+b : 1 \leq a \leq q^{m-\ell}-1\}$$

and

$$B = \{jb : 0 \leq j \leq q-2\}.$$ 

It is straightforward to verify that $A + B \subset I(q,m,\ell)^c$. Note that $n \in A + B$. In this case, we identify $n$ with 0.

Clearly, $A$ is a set of $q^{m-\ell}-1$ consecutive elements in the defining set $I(q,m,\ell)^c$. Note that

$$\gcd(b,n) = \gcd\left(\frac{q^\ell-1}{q-1},q^m-1\right) \leq \gcd(q^\ell-1,q^m-1) = q^{\gcd(\ell,m)}-1.$$ 

By assumption, $1 \leq \ell \leq m-1$. We then have $\gcd(\ell,m) \leq m-\ell$. Consequently,

$$\gcd(b,n) < q^{m-\ell}.$$ 

The desired conclusion on $d^\perp$ then follows from Theorem 4. \[ \square \]

When $q = 2$, the lower bound on the minimum distance $d^\perp$ of $\mathcal{U}(q,m,\ell)^\perp$ given in Theorem 5 is achieved. It is open if this lower bound can be improved for $q > 2$.

**Open Problem 2.** Determine the minimum distance $d^\perp$ of the code $\mathcal{U}(q,m,\ell)^\perp$.

To further study the dual code $\mathcal{U}(q,m,\ell)^\perp$, we need to establish relations between $\text{wt}(a)$ and $\text{wt}(n-a)$ for $a \in \mathbb{Z}_n$. Let $a \in \mathbb{Z}_n$ and let

$$a = \sum_{j=0}^{m-1} a_j q^j$$

be the $q$-adic expansion of $a$. We define

$$\gamma(a) = |\{0 \leq j \leq m-1 : 1 \leq a_j < q-1\}| = \text{wt}(a) - |\{0 \leq j \leq m-1 : a_j = q-1\}|.$$ 

Then we have the following lemma whose proof is straightforward and omitted.

**Lemma 6.** For $a \in \mathbb{Z}_n$, we have

$$\text{wt}(n-a) = m - \text{wt}(a) + \gamma(a) = m - |\{0 \leq j \leq m-1 : a_j = q-1\}|.$$ 

For $0 \leq i \leq m$, define

$$N(i) = \{a \in \mathbb{Z}_n : \text{wt}(a) = i\}$$

and

$$-N(i) = \{n-a : a \in N(i)\}.$$ 

Clearly, $|N(i)| = \binom{m}{i}(q-1)^i$.

The following lemma will be useful later.

**Lemma 7.** In the set $-N(i)$, there are exactly $\binom{m}{i}\binom{i}{h}(q-2)^h$ elements with Hamming weight $m-i+h$ for each $h$ with $0 \leq h \leq i$. 
Proof: Let \( a \in N(i) \). By definition, \( \text{wt}(a) = i \). It follows from Lemma \( 6 \) that
\[
\text{wt}(n - a) = m - i + \gamma(a).
\]
It is easily seen that
\[
|\{1 \leq a \leq n - 1 : \text{wt}(a) = i \text{ and } \gamma(a) = h\}| = \binom{m}{i} \binom{i}{h} (q - 2)^h.
\]
This completes the proof.

Theorem 8. \( \mathcal{U}(q, m, \ell)^\perp \) is a proper subcode of \( \mathcal{U}(q, m, m - 1 - \ell) \). When \( q = 2 \), \( \mathcal{U}(q, m, \ell)^\perp \) is the even-weight subcode of \( \mathcal{U}(q, m, m - 1 - \ell) \).

Proof: By definition, the defining set of \( \mathcal{U}(q, m, \ell)^\perp \) is \( -I(q, m, \ell)^c \). We now prove that
\[
I(q, m, m - 1 - \ell) \subseteq -I(q, m, \ell)^c.
\]
This is equivalent to proving that for every \( a \in I(q, m, m - 1 - \ell) \), \( n - a \in I(q, m, \ell)^c \). This is clearly true by Lemma \( 6 \). Consequently, \( \mathcal{U}(q, m, \ell)^\perp \) is a proper subcode of \( \mathcal{U}(q, m, m - 1 - \ell) \).

When \( q = 2 \), we have always the equality that \( \text{wt}(a) = m - \text{wt}(n - a) \) for all \( a \). Hence, in this case, we have
\[
\{0\} \cup I(q, m, m - 1 - \ell) = -I(q, m, \ell)^c.
\]
As a result, \( \mathcal{U}(q, m, \ell)^\perp \) is the even-weight subcode of \( \mathcal{U}(q, m, m - 1 - \ell) \) when \( q = 2 \).

Experimental data shows that one of \( I(q, m, m - \ell) \) and \( -I(q, m, \ell)^c \) is not a subset of the other. Consequently, one of \( \mathcal{U}(q, m, \ell)^\perp \) and \( \mathcal{U}(q, m, m - \ell) \) is not a subcode of the other.

Example 2. The following is a list of examples of the code \( \mathcal{U}(q, m, \ell)^\perp \).

- When \( (q, m, \ell) = (2, 4, 2) \), the code \( \mathcal{U}(q, m, \ell)^\perp \) has parameters [15, 10, 4]. In this case, the lower bound on the minimum distance is achieved.
- When \( (q, m, \ell) = (3, 3, 1) \), the code \( \mathcal{U}(q, m, \ell)^\perp \) has parameters [26, 6, 15]. In this case, the lower bound on the minimum distance is 10.
- When \( (q, m, \ell) = (3, 3, 2) \), the code \( \mathcal{U}(q, m, \ell)^\perp \) has parameters [26, 18, 6]. In this case, the lower bound on the minimum distance is 4.

C. The BCH cover of the cyclic code \( \mathcal{U}(q, m, \ell) \)

Recall that \( n = q^m - 1 \). For any \( i \) with \( 0 \leq i \leq n - 1 \), let \( m_i(x) \) denote the minimal polynomial of \( \alpha^i \) over \( GF(q) \). For any \( 2 \leq \delta \leq n \), define
\[
\bar{g}_{(q,n,\delta,b)}(x) = \text{lcm}(m_b(x), m_{b+1}(x), \ldots, m_{b+\delta-2}(x)),
\]
where \( b \) is an integer, \( \text{lcm} \) denotes the least common multiple of these minimal polynomials, and the addition in the subscript \( b + i \) of \( m_{b+i}(x) \) always means the integer addition modulo \( n \). Let \( \text{BCH}(q, n, \delta, b) \) denote the cyclic code of length \( n \) with generator polynomial \( \bar{g}_{(q,n,\delta,b)}(x) \).

When \( b = 1 \), the set \( \text{BCH}(q, n, \delta, b) \) is called a narrow-sense primitive BCH code with designed distance \( \delta \).

The BCH cover of a cyclic code is the BCH code with the smallest dimension containing the cyclic code as a subcode.

Theorem 9. \( \mathcal{U}(q, m, \ell) \) is a subcode of \( \text{BCH}(q, n, (q^{\ell+1} - 1)/(q - 1), 1) \).

Proof: In the proof of Theorem \( 3 \) we have shown that
\[
\{1, 2, 3, \ldots, (q^{\ell+1} - 1)/(q - 1) - 1\} \subseteq I(q, m, \ell).
\]
Hence, the generator polynomial of $\text{BCH}(q,n,(q^{\ell+1}-1)/(q-1),1)$ is a divisor of that of $\mathcal{U}(q,m,\ell)$. Hence, $\mathcal{U}(q,m,\ell)$ is a subcode of $\text{BCH}(q,n,(q^{\ell+1}-1)/(q-1),1)$.

When $\ell = 1$ or $\ell = m-1$, the two codes are identical. In other cases, the dimension of the code $\text{BCH}(q,n,(q^{\ell+1}-1)/(q-1),1)$ is larger than that of $\mathcal{U}(q,m,\ell)$.

The BCH cover of $\mathcal{U}(q,m,\ell)$ is $\text{BCH}(q,n,(q^{\ell+1}-1)/(q-1),1)$ if the minimum distance of $\mathcal{U}(q,m,\ell)$ is indeed equal to $(q^{\ell+1}-1)/(q-1)$.

**D. Comparisons of the two codes $\text{PGRM}_q(\ell,m)$ and $\mathcal{U}(q,m,\ell)$**

In this subsection, we compare the two codes $\text{PGRM}_q(\ell,m)$ and $\mathcal{U}(q,m,\ell)$ and make some comments.

First of all, the two codes $\text{PGRM}_q(\ell,m)$ and $\mathcal{U}(q,m,\ell)$ are clearly different, as their dimensions and minimum distances are different. Secondly, Theorem 8 tells us that $\mathcal{U}(q,m,\ell)$ is indeed a subcode of $\mathcal{U}(q,m,m-1-\ell)$. But the code $\mathcal{U}(q,m,\ell)$ does not have the property of Theorem 2.

**V. A FAMILY OF REVERSIBLE CYCLIC CODES FROM THE CODES $\mathcal{U}(q,m,\ell)$**

A code $C$ is called reversible if $(c_0,c_1,\ldots,c_{n-1}) \in C$ implies that $(c_{n-1},c_{n-2},\ldots,c_0) \in C$.

Let $f(x) = f_h x^h + f_{h-1} x^{h-1} + \cdots + f_1 x + f_0$ be a polynomial over $GF(q)$ with $f_h \neq 0$ and $f_0 \neq 0$. The reciprocal $f^*(x)$ of $f(x)$ is defined by

$$f^*(x) = f_0^{-1} x^h f(x^{-1}).$$

The conclusions of the following theorem are known in the literature, and are easy to prove. We will employ some of them later.

**Theorem 10.** Let $C$ be a cyclic code over $GF(q)$ with generator polynomial $g(x)$. Then the following statements are equivalent.

- $C$ is reversible.
- $g$ is self-reciprocal.
- $\beta^{-1}$ is a root of $g$ for every root $\beta$ of $g(x)$ over the splitting field of $g(x)$.

If $C$ is a reversible cyclic code of length $n$ over $GF(q)$, then $C + C^\perp = GF(q)^n$. Such a linear code is called a linear code with complement dual (LCD), as its dual code is equal to its complement.

LCD cyclic codes over finite fields are interesting in both theory and applications [9], [10], [14]. An important application of LCD codes in cryptography was recently documented in [4]. This is our major motivation of constructing LCD codes.

We now employ the codes $\mathcal{U}(q,m,\ell)$ to construct reversible cyclic codes. To this end, we need to make some preparations.

Recall that

$$I(q,m,t) = \{1 \leq i \leq n-1 : 1 \leq \text{wt}(i) \leq t\}$$

and

$$-I(q,m,t) = \{n-a : a \in I(q,m,t)\},$$

where $1 \leq t \leq m$.

**Lemma 11.** If $1 \leq t \leq \lceil m/2 \rceil - 1$, then $I(q,n,t) \cap (-I(q,n,t)) = \emptyset$.

**Proof:** Note that

$$n = q^m - 1 = (q-1)q^{m-1} + (q-1)q^{m-2} + \cdots + (q-1)q + (q-1)q^0.$$

By Lemma 6, $\text{wt}(n-i) \geq m - \text{wt}(i)$ for all $i \in \mathbb{Z}_m$.

If $i \in \mathbb{Z}_n$ and $\text{wt}(i) \leq \lceil m/2 \rceil - 1$, then $\text{wt}(n-i) \geq m - \text{wt}(i) > \lceil m/2 \rceil - 1$. The desired conclusion then follows. \[\blacksquare\]
Let $g_{(q,m,\ell)}(x)$ be the polynomial of [5], which is the generator polynomial of the cyclic code $\mathcal{U}(q,m,\ell)$. Let $g^*_{(q,m,\ell)}(x)$ denote the reciprocal of $g_{(q,m,\ell)}(x)$. Set

$$g(x) = (x - 1)\text{lcm}\left(g_{(q,m,\ell)}(x), g^*_{(q,m,\ell)}(x)\right).$$

Let $\mathcal{U}(q,m,\ell)$ denote the cyclic code of length $n$ over GF$(q)$ with generator polynomial $g(x)$. It follows from Theorem 10 that $\mathcal{U}(q,m,\ell)$ is reversible. Information on the parameters of the reversible cyclic code $\mathcal{U}(q,m,\ell)$ is given in the theorem below.

**Theorem 12.** If $1 \leq \ell \leq [m/2] - 1$, then the reversible cyclic code $\mathcal{U}(q,m,\ell)$ has minimum distance

$$d \geq 2\frac{q^{\ell+1} - 1}{q - 1},$$

and dimension

$$q^m - 2 \sum_{i=1}^{\ell} \binom{m}{i} (q - 1)^i. \quad (9)$$

**Proof:** When $1 \leq \ell \leq [m/2] - 1$, it follows from Lemma 11 that $g_{(q,m,\ell)}(x)$ and $g^*_{(q,m,\ell)}(x)$ are relatively prime. Consequently, $g(x) = (x - 1)g_{(q,m,\ell)}(x)g^*_{(q,m,\ell)}(x)$. Therefore,

$$\deg(g(x)) = 2\deg(g_{(q,m,\ell)}(x)) + 1.$$

By Theorem 3

$$\deg(g_{(q,m,\ell)}(x)) = \sum_{i=1}^{\ell} \binom{m}{i} (q - 1)^i.$$

The desired conclusion on the dimension then follows.

In this case, it follows from the proof of Theorem 3 that $g(x)$ has the roots $\alpha^i$ for all $i$ in the set

$$\left\{n - \left(\frac{q^{\ell+1} - 1}{q - 1} - 1\right), \ldots, n - 2, n - 1, 0, 1, 2, \ldots, \frac{q^{\ell+1} - 1}{q - 1} - 1\right\}.$$ 

The desired conclusion on the minimum distance then follows from the BCH bound.  

**Example 3.** The following is a list of examples of the reversible cyclic code $\mathcal{U}(q,m,\ell)$.

- When $(q,m,\ell) = (2,4,1)$, the code $\mathcal{U}(q,m,\ell)$ has parameters $[15,6,6]$.
- When $(q,m,\ell) = (2,6,2)$, the code $\mathcal{U}(q,m,\ell)$ has parameters $[63,20,14]$.
- When $(q,m,\ell) = (3,4,1)$, the code $\mathcal{U}(q,m,\ell)$ has parameters $[80,63,8]$.

**Open Problem 3.** Determine the minimum distance of the code $\mathcal{U}(q,m,\ell)$ of Theorem 12.

**Theorem 13.** Let $m \geq 2$ be even. Then the reversible cyclic code $\mathcal{U}(q,m,m/2)$ has minimum distance

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

and dimension

$$q^m - 2 \sum_{i=0}^{m/2} \binom{m}{i} (q - 1)^i + \binom{m}{m/2}. \quad (10)$$

**Proof:** The conclusion on the minimum distance comes from the BCH bound. We now prove the conclusion on the dimension of the code. It follows from Lemmas 11 and 7 that $a \in I(q,m,m/2) \cap (-I(q,m,m/2))$ if and only if $\text{wt}(a) = m/2$ and the $q$-adic expression of $a$ is of the form

$$(q - 1)(q^{i_1} + q^{i_2} + \cdots + q^{i_{m/2}}),$$
where $0 \leq i_1 < i_2 < \cdots < i_{m/2} \leq m - 1$. Consequently,

$$|I(q,m,m/2) \cap (-I(q,m,m/2))| = \left(\frac{m}{2}\right).$$

As before, let $g_{(q,m,m/2)}(x)$ be the generator polynomial of the code $\mathcal{O}(q,m,m/2)$. Then the generator polynomial of $\overline{\mathcal{O}}(q,m,m/2)$ is given by

$$g(x) = (x-1) \text{lcm}\left( g_{(q,m,m/2)}(x), g^*_{(q,m,m/2)}(x) \right)$$

$$= \frac{(x-1)g_{(q,m,m/2)}(x)g^*_{(q,m,m/2)}(x)}{\gcd(g_{(q,m,m/2)}(x), g^*_{(q,m,m/2)}(x))}.$$

Therefore,

$$\deg(g(x)) = 2\deg(g_{(q,m,m/2)}(x)) + 1 - \deg(\gcd(g_{(q,m,m/2)}(x), g^*_{(q,m,m/2)}(x)))$$

$$= 2\deg(g_{(q,m,m/2)}(x)) + 1 - |I(q,m,m/2) \cap (-I(q,m,m/2))|$$

$$= 1 + 2 \sum_{i=1}^{m/2} \left( \binom{m}{i} (q-1)^i - \left(\frac{m}{2}\right) \right).$$

The desired conclusion on the dimension then follows. □

We point out that the dimension of the code $\overline{\mathcal{O}}(q,m,m/2)$ is equal to zero when $q = 2$. Hence, the code is nontrivial only when $q > 2$.

**Example 4.** When $(q,m) = (5,2)$, the code $\overline{\mathcal{O}}(q,m,m/2)$ has parameters $[24,9,12]$. $\overline{\mathcal{O}}(q,m,m/2)$ has minimum distance $2. Hence, the code is nontrivial only when $q > 2$.

**Open Problem 4.** Determine the minimum distance of the code $\overline{\mathcal{O}}(q,m,m/2)$ of Theorem 13.

**Theorem 14.** Let $m \geq 3$ be odd. Then the reversible cyclic code $\overline{\mathcal{O}}(q,m,(m+1)/2)$ has minimum distance

$$d \geq 2 \frac{q^{(m+3)/2} - 1}{q-1}$$

and dimension

$$q^m - 2 \sum_{i=0}^{(m+1)/2} \left( \binom{m}{i} (q-1)^i + \frac{4 + (q-2)(m+1)}{2} \left( \frac{m}{2} \right) \right). \quad (11)$$

**Proof:** The conclusion on the minimum distance comes from the BCH bound. We now prove the desired conclusion on the dimension of the code. It follows from Lemmas 11, 6, and 7 that $a \in I(q,m,(m+1)/2) \cap (-I(q,m,(m+1)/2))$ if and only if one of the following three cases happens:

- **C1:** $\text{wt}(a) = \frac{m-1}{2}$, $\text{wt}(n-a) = \frac{m+1}{2}$, and the $q$-adic expression of $a$ is of the form

$$ (q-1)(q^{i_1} + q^{i_2} + \cdots + q^{i_{(m-1)/2}}),$$

where $0 \leq i_1 < i_2 < \cdots < i_{(m-1)/2} \leq m - 1$. The total number of such $a$’s is equal to $\left(\binom{m}{(m-1)/2}\right)$.

- **C2:** $\text{wt}(a) = \frac{m+1}{2}$, $\text{wt}(n-a) = \frac{m-1}{2}$, and the $q$-adic expression of $a$ is of the form

$$ (q-1)(q^{i_1} + q^{i_2} + \cdots + q^{i_{(m+1)/2}}),$$

where $0 \leq i_1 < i_2 < \cdots < i_{(m+1)/2} \leq m - 1$. The total number of such $a$’s is equal to $\left(\binom{m}{(m+1)/2}\right)$.

- **C3:** $\text{wt}(a) = \frac{m+1}{2}$, $\text{wt}(n-a) = \frac{m-1}{2}$, and the $q$-adic expression of $a$ is of the form

$$a_{i_1}q^{i_1} + a_{i_2}q^{i_2} + \cdots + a_{i_{(m+1)/2}}q^{i_{(m+1)/2}},$$

where $0 \leq i_1 < i_2 < \cdots < i_{(m+1)/2} \leq m - 1$. The total number of such $a$’s is equal to $\left(\binom{m}{(m+1)/2}\right)$.
where \( 0 \leq i_1 < i_2 < \cdots < i_{(m+1)/2} \leq m - 1, 1 \leq a_{ij} \leq q - 1 \), and all the entries of the vector \((a_{i_1}, a_{i_2}, \cdots, a_{i_{(m+1)/2}})\) are \( q - 1 \) except one that could be any element in \( \{1, 2, \cdots, q - 2\} \). The total number of such \( a \)'s is equal to

\[
\frac{(m+1)(q-2)}{2} \left( \frac{m}{2} \right).
\]

Summarizing the conclusions in the three cases above, we obtain that

\[
|I(q,m,(m+1)/2) \cap (-I(q,m,(m+1)/2))| = \frac{4 + (q-2)(m+1)}{2} \left( \frac{m}{m-1} \right).
\]

As before, let \( g_{q,m,(m+1)/2}(x) \) be the polynomial of the code \( \mathcal{U}(q,m,(m+1)/2) \). Then the generator polynomial of \( \overline{\mathcal{U}}(q,m,(m+1)/2) \) is given by

\[
g(x) = (x-1)\text{lcm}\left(g_{q,m,(m+1)/2}(x), g^*_{q,m,(m+1)/2}(x)\right)
= \frac{(x-1)g_{q,m,(m+1)/2}(x)g^*_{q,m,(m+1)/2}(x)}{\gcd(g_{q,m,(m+1)/2}(x), g^*_{q,m,(m+1)/2}(x))}.
\]

Therefore,

\[
\deg(g(x)) = 2\deg(g_{q,m,(m+1)/2}(x)) + 1 - \deg(\gcd(g_{q,m,(m+1)/2}(x), g^*_{q,m,(m+1)/2}(x))
= 2\deg(g_{q,m,(m+1)/2}(x)) + 1 - |I(q,m,(m+1)/2) \cap (-I(q,m,(m+1)/2))|
= 1 + 2 \sum_{i=1}^{(m+1)/2} \binom{m}{i} (q-1)^i - \frac{4 + (q-2)(m+1)}{2} \left( \frac{m}{m-1} \right).
\]

The desired conclusion on the dimension then follows.

We point out that the dimension of \( \overline{\mathcal{U}}(q,m,(m+1)/2) \) is equal to zero when \( q = 2 \). Hence, the code is nontrivial only when \( q > 2 \).

**Example 5.** When \( (q,m) = (4,3) \), \( \overline{\mathcal{U}}(q,m,(m+1)/2) \) has parameters \([63,8,42]\).

**Open Problem 5.** Determine the minimum distance of the code \( \overline{\mathcal{U}}(q,m,(m+1)/2) \) of Theorem \( \text{[14]} \).

### VI. Summary and Concluding Remarks

The first contribution of this paper is the new generalization of the classical punctured binary Reed-Muller codes. The newly generalized codes \( \mathcal{U}(q,m,\ell) \) are documented in Theorem \( \text{[5]} \). A lower bound on the minimum distance of \( \mathcal{U}(q,m,\ell) \) was developed and given in Theorem \( \text{[5]} \). Experimental data indicates that this lower bound is indeed the minimum distance. However, we were not able to prove this conjecture. It would be nice if this open problem can be settled. The dual code \( \mathcal{U}(q,m,\ell)^\perp \) was also studied. But the minimum distance \( d^\perp \) of \( \mathcal{U}(q,m,\ell)^\perp \) is also open, though a lower bound on \( d^\perp \) was given in Theorem \( \text{[5]} \). The locality of both \( \mathcal{U}(q,m,\ell) \) and \( \mathcal{U}(q,m,\ell)^\perp \) depends on \( d^\perp \) and \( d \) respectively. Hence, it is also valuable to settle Open Problem \( \text{[2]} \).

The second contribution of this paper is the construction of the reversible cyclic codes \( \overline{\mathcal{U}}(q,m,\ell) \), which are based on the cyclic codes \( \mathcal{U}(q,m,\ell) \). The dimension of \( \overline{\mathcal{U}}(q,m,\ell) \) was settled for all \( \ell \) with \( 1 \leq \ell \leq \lfloor m/2 \rfloor \). A lower bound on the reversible cyclic code \( \overline{\mathcal{U}}(q,m,\ell) \) was developed. But the minimum distance of \( \overline{\mathcal{U}}(q,m,\ell) \) is unknown. It would be nice if Open Problems \( \text{[3,4]} \) and \( \text{[5]} \) can be resolved.
REFERENCES

[1] E. F. Assmus and J. D. Key, Designs and Their Codes, Cambridge Tracts in Mathematics, Vol. 103, Cambridge University Press, Cambridge, 1992.
[2] E. F. Assmus, Jr and J. D. Key, “Polynomial codes and finite geometries”, In: V.S. Pless and W.C. Huffman (Eds.), Handbook of Coding Theory, Chapter 16, pp. 1269–1343, Elsevier, 1998.
[3] E. Betti and M. Sala, “A new bound for the minimum distance of a cyclic code from its defining set,” IEEE Trans. Inf. Theory, vol. 52, no. 8, pp. 3700–3706, 2006.
[4] C. Carlet and S. Guilley, “Complementary dual codes for counter-measures to side-channel attacks,” In: E. R. Pinto et al. (eds.), Coding Theory and Applications, CIM Series in Mathematical Sciences, vol. 3, pp. 97–105, Springer Verlag, 2014.
[5] P. Delsarte, J. M. Goethals, and F. J. MacWilliams, “On generalized Reed-Muller codes and their relatives, Information and Control, vol. 16, pp. 403–442, 1972.
[6] P. Ding and J. D. Key, “Minimum-weight codewords as generators of generalized Reed-Muller codes,” IEEE Trans. Inf. Theory, vol. 46, no. 6, pp. 2152–2158, Sept. 2000.
[7] G. van der Geer and M. van der Vlugt, “Generalized Reed-Muller codes and curves with many points, Journal of Number Theory, vol. 72, pp. 257268, 1998.
[8] C. R. P. Hartmann and K. K. Tzeng, “Generalizations of the BCH bound, Inform. and Control, vol. 20, pp. 489–498, 1972.
[9] J. L. Massey, “Reversible codes,” Information and Control, vol. 7, no. 3, pp. 369–380, 1964.
[10] J. L. Massey, “Linear codes with complementary duals,” Discrete Math., vol. 106/107, pp. 337–342, 1992.
[11] W. C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.
[12] D. E. Muller, “Application of boolean algebra to switching circuit design and to error detection, IEEE Trans. Computers, vol. 3, pp. 6–12, 1954.
[13] I. S. Reed, “A class of multiple-error-correcting codes and the decoding scheme, IRE Trans. Inf. Theory, vol. 4, pp. 38–49, 1954.
[14] N. Sendrier, “Linear codes with complementary duals meet the Gilbert-Varshamov bound,” Discrete Mathematics, vol. 285, pp. 345–347, 2004.
[15] S. Yekhanin, “Locally decodable codes: a brief survey,” In: Chee et al. (Eds.), Coding and Cryptography, Lecture Notes in Computer Science 6639, pp. 273–282, 2011, Springer Verlag.