Good reversible quasi-cyclic codes via unfolding cyclic codes

Ramy Taki ElDin\(^{1(a)}\) and Hajime Matsui\(^{1}\)

\(^{1}\) Toyota Technological Institute, 2-12-1 Hisakata, Tempaku, Nagoya, Aichi 468-8511, Japan
\(^{a}\) ramy@toyota-ti.ac.jp

Abstract: In this paper, we consider the reversibility problem in the class of quasi-cyclic (QC) codes \(\mathcal{Q}\) over \(\mathbb{F}_q\) of length \(n\ell\) and index \(\ell\) generated by unfolding cyclic codes \(\mathcal{C}\) over \(\mathbb{F}_{q^\ell}\) of length \(n\). We prove a necessary and sufficient condition on \(\mathcal{C}\) that ensures the reversibility of \(\mathcal{Q}\). Using computer search, we offer some good reversible QC codes that are generated by unfolding cyclic codes.

Keywords: Reciprocal polynomial, binary code, computer search, best known parameters, minimum distance.

Classification: Fundamental theories for communications.

References

[1] R. Taki ElDin, H. Matsui, “Run-length constraint of cyclic reverse-complement and constant GC-content DNA codes,” IEICE Trans. on Fundamental of Electronics, Communications and Computer Sciences, vol.E103–A, no.1, pp.325–333, Jan. 2020.
[2] R. Taki ElDin, H. Matsui, “Quasi-cyclic codes via unfolded cyclic codes and their reversibility,” IEEE Access, vol.7, pp.184500–184508, Dec. 2019.
[3] M. Grassl, “Bounds on the minimum distance of linear codes and quantum codes,” 2020. [Online] Available: http://www.codetables.de/
[4] J.L. Massey, “Reversible codes,” Information and Control, vol.7, no.3, pp.369–380, Sep. 1964.

1 Introduction

Let \(\mathbb{F}_q\) denote a finite field of \(q\) elements. A cyclic code over \(\mathbb{F}_q\) of length \(n\) is a linear subspace of \(\mathbb{F}_q^n\) invariant under the cyclic shifts of its codewords. A quasi-cyclic (QC) code over \(\mathbb{F}_q\) of length \(n\ell\) and index \(\ell\) is a linear subspace of \(\mathbb{F}_q^{n\ell}\) invariant under cyclic shifts of its codewords by \(\ell\) coordinates. Let \(\Gamma\) denote the class of QC codes over \(\mathbb{F}_q\) of length \(n\ell\) and index \(\ell\) generated by unfolding cyclic codes over \(\mathbb{F}_{q^\ell}\) of length \(n\). By unfolding we mean a one-to-one map \(\phi_\theta\) that represents elements of \(\mathbb{F}_{q^\ell}\) by vectors in \(\mathbb{F}_q^\ell\) using the basis \(\{1, \theta, \ldots, \theta^{\ell-1}\}\), where \(\theta\) is a root of an irreducible polynomial \(p(x) \in \mathbb{F}_q[x]\) of degree \(\ell\), i.e., \(\mathbb{F}_{q^\ell} = \mathbb{F}_q(\theta)\). A code is called reversible if it is invariant under reversing the coordinates of codewords. Reversible codes are important in some applications, e.g., DNA codes [1].

In this paper, we extend our work [2] by presenting some good reversible...
QC codes in \( \Gamma \). Here, by a good code, we mean an optimal or suboptimal code, where we say a code is optimal (resp. suboptimal) if its minimum distance is the optimal value (resp. the optimal value minus one or two) provided by [3]. In Theorem 1, we prove a necessary and sufficient condition for the reversibility of QC codes generated by unfolding cyclic codes over \( \mathbb{F}_{q^\ell} \). Theorem 1 in this paper is more useful than Theorem 3 in [2] because it does not assume a predetermined \( \theta \), does not require to build the defining set of the cyclic code, and shows that the self-reciprocity of the minimal polynomial of \( \theta \) is a sufficient condition for the reversibility but not necessary. As an application of Theorem 1, we present in Table I some good reversible QC codes in \( \Gamma \) of even \( \ell \) obtained by computer search.

The rest of this paper is organized as follows. Preliminaries are summarized in Section 2. We show the main contribution in Section 3. Our work is concluded in Section 4.

2 Preliminaries

We denote by \( \mathcal{C} \) a cyclic code over \( \mathbb{F}_{q^\ell} \) of length \( n \) and dimension \( k \), where \( n \) is coprime to \( q \). That is, \( \mathcal{C} \) is an ideal in \( \mathbb{F}_{q^\ell}[x]/\langle x^n - 1 \rangle \) generated by a generator polynomial \( g(x) \) that divides \( x^n - 1 \). Massey [4] showed that a cyclic code is reversible if and only if \( g(x) \) is self-reciprocal, i.e., \( g^*(x)|g(x) \), where \( g^*(x) = x^{\deg(g(x))}g(1/x) \) is the reciprocal polynomial of \( g(x) \). Let \( \theta \in \mathbb{F}_{q^\ell} \) be a zero to an irreducible polynomial \( p(x) \in \mathbb{F}_q[x] \) of degree \( \ell \). Any element \( \alpha \in \mathbb{F}_{q^\ell} \) is written as \( \alpha = \sum_{j=0}^{\ell-1} a_j \theta^j \) for uniquely determined \( a_j \in \mathbb{F}_q(0 \leq j \leq \ell - 1) \). Hence, the codeword \( c = (a_0, a_1, \ldots, a_{n-1}) \in \mathcal{C} \), where \( a_i \in \mathbb{F}_{q^\ell}(0 \leq i \leq n - 1) \), is represented by the polynomial

\[
c(x) = \sum_{i=0}^{n-1} a_i x^i = \sum_{i=0}^{n-1} x^i \left( \sum_{j=0}^{\ell-1} a_{i,j} \theta^j \right), \tag{1}
\]

where \( a_{i,j} \in \mathbb{F}_q \) and \( a_i = \sum_{j=0}^{\ell-1} a_{i,j} \theta^j \) for \( 0 \leq i \leq n - 1 \) and \( 0 \leq j \leq \ell - 1 \).

**Definition 1.** Define the map \( \varphi_\theta : \mathbb{F}_{q^\ell} \rightarrow \mathbb{F}_q^\ell \) such that

\[
\varphi_\theta : \alpha = \sum_{j=0}^{\ell-1} a_j \theta^j \mapsto (a_0, a_1, \ldots, a_{\ell-1}).
\]

We refer to \( \varphi_\theta \) as the unfolding map, while \( \varphi_\theta^{-1} : (a_0, a_1, \ldots, a_{\ell-1}) \mapsto \alpha \) is the folding map. The unfolding map \( \varphi_\theta \) can be applied to codewords of \( \mathcal{C} \) as follows

\[
c = (a_0, a_1, \ldots, a_{n-1}) \in \mathcal{C} \xrightarrow{\varphi_\theta} (a_0, a_0, \ldots, a_{\ell-1}, \ldots, a_{n-1,0}, \ldots, a_{n-1,\ell-1}). \tag{2}
\]

From (2), the reverse of \( \varphi_\theta(c) \) is the unfolding of the word \( r \in \mathbb{F}_q^n \), which is given in the polynomial form by

\[
r(x) = x^{n-1} \theta^{\ell-1} \sum_{i=0}^{n-1} x^{-i} \left( \sum_{j=0}^{\ell-1} a_{i,j} \theta^{-j} \right). \tag{3}
\]
Unfolding a cyclic code $C$ over $\mathbb{F}_{q^r}$ of length $n$ and dimension $k$ generates a QC code, which we refer to as $Q = \varphi_\theta(C)$, over $\mathbb{F}_q$ of length $n\ell$, index $\ell$, and dimension $k\ell$. In fact, $Q$ is an $\mathbb{F}_q$-linear code invariant under cyclic shifts by $\ell$ coordinates. That is,

$$
(a_0,0,\ldots,a_0,\ell-1,a_1,0,\ldots,a_1,\ell-1,\ldots,a_{n-1},0,\ldots,a_{n-1},\ell-1) \in Q
$$

$$
\implies (a_{n-1},0,\ldots,a_{n-1},\ell-1,a_0,0,\ldots,a_0,\ell-1,\ldots,a_{n-2},0,\ldots,a_{n-2},\ell-1) \in Q.
$$

Let $\Gamma$ be the class of QC codes over $\mathbb{F}_q$ of length $n\ell$ and index $\ell$ generated by unfolding cyclic codes over $\mathbb{F}_{q^r}$ of length $n$.

## 3 Good Reversible QC Codes in $\Gamma$

Hereinafter, $C$ denotes a cyclic code over $\mathbb{F}_{q^r} = \mathbb{F}_q(\theta)$ of length $n$ and dimension $k$, and generator polynomial $g(x)$. Moreover, $Q = \varphi_\theta(C)$ refers to a QC code in the class $\Gamma$ over $\mathbb{F}_q$ of length $n\ell$ and dimension $k\ell$. The following theorem gives a necessary and sufficient condition for reversibility of QC codes in $\Gamma$. Contrary to [2, Theorem 3], Theorem 1 does not require constructing the defining set of the cyclic code $C$.

**Theorem 1.** Let $C$ be a cyclic code over $\mathbb{F}_{q^r} = \mathbb{F}_q(\theta)$ of length $n$ and dimension $k$. Let $g(x) = \sum_{i=0}^{n-k} \alpha_i x^i \in \mathbb{F}_{q^r}[x]$ be the monic generator polynomial of $C$, where $\alpha_i = \sum_{j=0}^{\ell-1} a_{ij} \theta^j$ for some $a_{ij} \in \mathbb{F}_q$. The QC code $Q = \varphi_\theta(C)$ over $\mathbb{F}_q$ of index $\ell$, length $n\ell$, and dimension $k\ell$ is reversible if and only if any of the following conditions is true:

A) $g(x)$ is a self-reciprocal polynomial over $\mathbb{F}_q$.

B) $p(x)$ is a self-reciprocal polynomial and $g(x)|\tilde{g}^*(x)$, where

$$
\tilde{g}(x) = \sum_{i=0}^{n-k} \left( \sum_{j=0}^{\ell-1} a_{ij} \theta^{-j} \right) x^i.
$$

**Proof.** Let $\sigma$ be the $\mathbb{F}_q$-linear transformation on $\mathbb{F}_{q^r}[x]/(x^n - 1)$ such that $\sigma(\theta^j x^i) = \theta^{-j} x^{-i}$ for $0 \leq j \leq \ell - 1$ and $0 \leq i \leq n - 1$. Informally, $\sigma$ corresponds to the reverse of the codewords in $Q$, and in particular

$$
\sigma(g(x)) = \sigma\left( \sum_{i=0}^{n-k} \alpha_i x^i \right) = \sigma\left( \sum_{i=0}^{n-k} \sum_{j=0}^{\ell-1} a_{ij} \theta^j x^i \right) = \sum_{i=0}^{n-k} \sum_{j=0}^{\ell-1} \sigma(a_{ij} \theta^j x^i)
$$

$$
= \sum_{i=0}^{n-k} \sum_{j=0}^{\ell-1} a_{ij} \sigma(\theta^j x^i) = \sum_{i=0}^{n-k} \sum_{j=0}^{\ell-1} a_{ij} \theta^{-j} x^{-i}.
$$

Thus $\tilde{g}^*(x) = x^{n-k} \sigma(g(x))$. Similarly, $\sigma(ax^i) = \sigma(\alpha) x^{-i}$ for any $\alpha \in \mathbb{F}_{q^r}$ and $0 \leq i \leq n - 1$. For any $c(x) \in C$, there exists $b(x) = \sum_{i=0}^{k-1} \beta_i x^i$ such that $c(x) = g(x)b(x)$, where $\beta_i \in \mathbb{F}_{q^r}$ for $0 \leq i \leq k - 1$. In addition, (1) and (3) show that $r(x) = x^{n-1} \theta^{\ell-1} \sigma(c(x))$. Hence

$$
r(x) = x^{n-1} \theta^{\ell-1} \sigma(g(x)b(x)) = x^{n-1} \theta^{\ell-1} \sigma\left( \sum_{i=0}^{n-k} \alpha_i x^i \sum_{i=0}^{k-1} \beta_i x^i \right)
$$

$$
= x^{n-1} \theta^{\ell-1} \sum_{i=0}^{n-k} \sum_{i=0}^{k-1} \sigma(\alpha_i \beta_i x^{i+i}) = x^{n-1} \theta^{\ell-1} \sum_{i=0}^{n-k} x^{-i} \sum_{i=0}^{k-1} \sigma(\alpha_i \beta_i) x^{-i}.
$$

© IEICE 2020
Firstly, we show that condition A implies the reversibility of $Q$. Let $g(x)$ be self-reciprocal with coefficients $a_i \in \mathbb{F}_q$ for $0 \leq i \leq n - k$. Since $\sigma$ is linear, $\sigma(\alpha \beta) = \alpha \sigma(\beta)$ and $r(x) = x^{n-1}\theta^{k-1}\sum_{i=0}^{n-k} a_i x^{-i} \sum_{i=0}^{k-1} \sigma(\beta_i)x^{-i} = x^{n-1}\theta^{k-1}g(x^{-1}) \sum_{i=0}^{k-1} \sigma(\beta_i)x^{-i}$. Consequently, $g^*(x)|r(x)$. But $g(x)$ is self-reciprocal, then $g(x)|r(x)$, $r(x) \in C$, and $Q$ is reversible.

Secondly, we show that condition B implies the reversibility of $Q$. If $p(x)$ is self-reciprocal, then $\ell$ is even and $\theta^{-1}$ is a root of $p(x)$. The restriction of $\sigma$ to $\mathbb{F}_q$ is the field automorphism $\theta \mapsto \theta^{-1}$ that fixes $\mathbb{F}_q$. Thus $\sigma(\alpha \beta) = \sigma(\alpha)\sigma(\beta)$. Using $\sigma(\alpha)x^{-i} = \sigma(ax^i)$ and $x^{n-k}\sigma(g(x)) = \hat{g}^*(x)$, we get

$$r(x) = x^{n-1}\theta^{k-1} \sum_{i=0}^{n-k} a_i x^{-i} \sum_{i=0}^{k-1} \sigma(\beta_i)x^{-i} = x^{n-1}\theta^{k-1} \sum_{i=0}^{n-k} a_i x^{-i} \sum_{i=0}^{k-1} \sigma(\beta_i)x^{-i}$$

$$= x^{n-1}\theta^{k-1}\sigma(g(x)) \sum_{i=0}^{k-1} \sigma(\beta_i)x^{-i} = x^{k-1}\theta^{k-1}\hat{g}^*(x) \sum_{i=0}^{k-1} \sigma(\beta_i)x^{-i}.$$ 

Since $g(x)|\hat{g}^*(x)$, we have $g(x)|r(x)$, $r(x) \in C$, and $Q$ is reversible.

Finally, we show that the reversibility of $Q$ implies A or B. Since $Q$ is reversible, then $g(x)|r(x)$ for every choice of $b(x)$. By choosing $b(x) = 1$, we get $r(x) = x^{n-1}\theta^{k-1} \sum_{i=0}^{n-k} a_i x^{-i} = x^{n-1}\theta^{k-1} \sum_{i=0}^{n-k} \sigma(\alpha_i x^i) = x^{n-1}\theta^{k-1}\sigma \left( \sum_{i=0}^{n-k} a_i x^i \right) = x^{n-1}\theta^{k-1}x^{n-k}\sigma \left( g(x) \right) = x^{k-1}\theta^{k-1}\hat{g}^*(x)$. This proves that $g(x)|\hat{g}^*(x)$. In addition, we distinguish the following two cases:

a) If $a_i \in \mathbb{F}_q$ for all $0 \leq i \leq n - k$, then $\hat{g}(x) = g(x)$. The self-reciprocity of $g(x)$ is a consequence of $g(x)|\hat{g}^*(x)$. Condition A follows.

b) If $a_h \not\in \mathbb{F}_q$ for some $0 \leq h \leq n - k$, there exists $a_{ht} \neq 0$ with $0 < t \leq \ell - 1$ such that $a_h = \sum_{j=0}^{t} a_{ht} \theta^j$. By choosing $b(x) = \theta^{t-\ell}$, we have $r(x) = x^{k-1}\theta^{k-1}x^{n-k}\sigma \left( \theta^{t-\ell}g(x) \right)$ is a codeword of $C$. Thus, $g(x)|x^{n-k}\sigma \left( \theta^{t-\ell}g(x) \right)$. In fact, deg $(\hat{g}^*(x)) = \deg \left( x^{n-k}\sigma(\theta^{t-\ell}g(x)) \right) = n - k$ which is the least polynomial degree in $C$. Moreover, the constant terms of $\hat{g}^*(x)$ and $x^{n-k}\sigma(\theta^{t-\ell}g(x))$ are 1 and $\sigma(\theta^{t-\ell})$, respectively. Therefore, $x^{n-k}\sigma(\theta^{t-\ell}g(x)) = \sigma(\theta^{t-\ell})\hat{g}^*(x)$. In particular, equating the coefficients of $x^{n-k-h}$ yields $\sigma(\theta^{t-\ell}a_h) = \sigma(\theta^{t-\ell})\sigma(a_h)$. Consequently,

$$\sum_{j=0}^{t-1} a_{ht}\theta^{-j} \sum_{j=0}^{t-1} a_{ht} \theta^{-j} = a_{ht} \theta^{t} \sum_{j=0}^{t-1} a_{ht} \theta^{-j} + a_{ht} \theta^{-t}.$$ 

From the outermost sides of the last equation, we conclude $\sigma(\theta^{t}) = \theta^{-t}$. Let $p(x) = x^\ell + \sum_{i=0}^{\ell-1} a_i x^i$ be the monic minimal polynomial of $\theta$ over $\mathbb{F}_q$. Then, $0 = \sigma(0) = \sigma(\theta^{t} + \sum_{i=0}^{\ell-1} a_i \theta^i) = \sigma(\theta^{t}) + \sum_{i=0}^{\ell-1} a_i \theta^{-i} = \theta^{-t} + \sum_{i=0}^{\ell-1} a_i \theta^{-i} = p(\theta^{-t})$. Thus, $\theta^{-t}$ is a root of $p(x)$, $p(x)$ is self-reciprocal, and condition B follows.

© IEICE 2020
Example 1. Let $\mathcal{C}$ be the cyclic code over $\mathbb{F}_4$ of length $n = 43$, dimension $k = 35$, and generator polynomial $g(x) = 1 + \theta x^2 + (1 + \theta)x^3 + \theta x^5 + (1 + \theta)x^6 + x^8 \in \mathbb{F}_4[x]$, where $\theta \in \mathbb{F}_4$ is a zero to $p(x) = 1 + x + x^2 \in \mathbb{F}_2[x]$. The map $\varphi_\theta : \mathbb{F}_4 \to \mathbb{F}_2^2$ unfolds $\mathcal{C}$ to a binary QC code $\mathcal{Q}$ in $\Gamma$ of index $\ell = 2$, length $n\ell = 86$, and dimension $k\ell = 70$. The minimum distance of $\mathcal{Q}$ is $d_Q = 6$. According to [3], a linear binary code of length 86, dimension 70, and minimum distance 6 is optimal. Moreover, $\mathcal{Q}$ is reversible as it meets condition B of Theorem 1. Hence, $\mathcal{Q}$ is an optimal reversible code in $\Gamma$.

Other examples of good binary reversible QC codes in $\Gamma$ of even index are shown in Table I, where all suboptimal codes have their minimum distances which are equal to the optimal values minus two provided by [3]. In this table, $p(x) \in \mathbb{F}_2[x]$ is the monic minimal polynomial of $\theta \in \mathbb{F}_2^\ell$ that defines $\varphi_\theta$. Using condition B of Theorem 1, one can verify the reversibility of the QC codes listed in Table I.

Remark 1. It is derived from Theorem 1 that, for odd index, $\mathcal{Q} = \varphi_\theta(\mathcal{C})$ is reversible code if and only if $g(x)$ is a self-reciprocal polynomial over $\mathbb{F}_q$.

Remark 2. As far as we have searched, all good codes satisfy condition B and only one of them also satisfies condition A in Theorem 1. It seems that good reversible QC codes generated by unfolding are likely to satisfy condition B instead of condition A. One reason for this observation is that, under condition A, $d_Q \leq \text{wt}(g(x))$ holds, where $d_Q$ denotes the minimum distance of $\mathcal{Q}$ and $\text{wt}(g(x))$ denotes the number of nonzero coefficients of $g(x)$. On the other hand, under condition B, this upper bound for $d_Q$ does not hold, e.g., the first code in Table I satisfies condition B but $d_Q = 8 > \text{wt}(g(x)) = 6$. On a lower bound for $d_Q$, in general we have $d_Q \geq d_C$, which suggests that larger $d_C$ tends to increase $d_Q$.

4 Conclusion

Theorem 1 proposed an equivalent condition for the reversibility of QC codes generated by unfolding cyclic codes over an extension field. Applying this theorem to computer search, we found various good reversible QC codes in $\Gamma$ as shown in Table I.

Acknowledgments

Ramy Taki ElDin is on leave of absence from Faculty of Engineering, Ain Shams University, Cairo, Egypt.

This work was supported in part by the JSPS KAKENHI under Grant JP19K22850.
| $\ell$ | $n$ | $k$ | $p(x)$ | $g(x)$ | $Q$ Parameters | Opt./Subopt. |
|---|---|---|---|---|---|---|
| 2 | 11 | 5 | $1 + x + x^2$ | $1 + (1 + \theta)x + (1 + \theta)x^2 + \theta x^4 + \theta x^5 + x^6$ | [22, 10, 8] | Optimal |
| 2 | 33 | 22 | $1 + x + x^2$ | $1 + x^3 + x^4 + x^5 + x^7 + x^8 + x^{10} + x^{11}$ | [66, 44, 6] | Suboptimal |
| 2 | 43 | 35 | $1 + x + x^2$ | $1 + \theta x^2 + (1 + \theta)x^3 + \theta x^5 + (1 + \theta)x^6 + x^8$ | [86, 70, 6] | Optimal |
| 4 | 5 | 3 | $\sum_{i=0}^{4} x^i$ | $\theta^3 + (1 + \theta^3)x + x^2$ | [20, 12, 4] | Optimal |
| 4 | 13 | 6 | $\sum_{i=0}^{4} x^i$ | $1 + (\theta^2 + \theta^3)x + (1 + \theta^2 + \theta^3)x^2 + (\theta^2 + \theta^3)x^3 + (\theta^2 + \theta^3)x^4 + (1 + \theta^2 + \theta^3)x^5 + (\theta^2 + \theta^3)x^6 + x^7$ | [52, 24, 10] | Suboptimal |
| 4 | 13 | 9 | $\sum_{i=0}^{4} x^i$ | $1 + (1 + \theta + \theta^2 + \theta^3)x + (1 + \theta^2 + \theta^3)x^2 + \theta x^3 + x^4$ | [52, 36, 6] | Optimal |
| 6 | 7 | 4 | $1 + x^3 + x^6$ | $1 + (\theta^4 + \theta^5)x + (\theta^4 + \theta^5)x^2 + x^3$ | [42, 24, 6] | Suboptimal |
| 6 | 9 | 6 | $1 + x^3 + x^6$ | $(1 + \theta^3) + (1 + \theta + \theta^3 + \theta^5)x + (1 + \theta + \theta^5)x^2 + x^3$ | [54, 36, 6] | Suboptimal |
| 6 | 19 | 15 | $1 + x^3 + x^6$ | $1 + (1 + \theta^2 + \theta^3)x + (1 + \theta + \theta^2 + \theta^3)x^2 + (\theta + \theta^3 + \theta^4)x^3 + x^4$ | [114, 90, 6] | Suboptimal |
| 8 | 5 | 3 | $1 + x + x^2 + x^4 + x^6 + x^7 + x^8$ | $1 + (1 + \theta^2 + \theta^4 + \theta^5)x + x^2$ | [40, 24, 5] | Suboptimal |
| 8 | 17 | 12 | $1 + x + x^2 + x^4 + x^6 + x^7 + x^8$ | $(\theta + \theta^3 + \theta^5 + \theta^6 + \theta^7) + (\theta^2 + \theta^3 + \theta^4 + \theta^7)x + (\theta + \theta^2 + \theta^4 + \theta^5 + \theta^7)x^2 + (\theta + \theta^2 + \theta^3 + \theta^4)x^3 + (1 + \theta + \theta^2 + \theta^3 + \theta^4)x^4 + x^5$ | [136, 96, 10] | Suboptimal |
| 10 | 11 | 7 | $\sum_{i=0}^{10} x^i$ | $\theta^6 + (\theta^3 + \theta^4 + \theta^5 + \theta^6)x + (\theta + \theta^2 + \theta^4 + \theta^5)x^2 + (1 + \theta + \theta^2 + \theta^3)x^3 + x^4$ | [110, 70, 10] | Suboptimal |