Received June 11, 2020, accepted July 29, 2020, date of publication August 3, 2020, date of current version August 17, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3013958

On Reversibility and Self-Duality for Some Classes of Quasi-Cyclic Codes

RAMY TAKI ELDIN[1,2] **AND HAJIME MATSUI**[1]
[1]Toyota Technological Institute, Nagoya 468-8511, Japan
[2]*(On leave)* Faculty of Engineering, Ain Shams University, Cairo 11517, Egypt

Corresponding author: Ramy Taki ElDin (ramy@toyota-ti.ac.jp)

This work was supported by JSPS KAKENHI under Grant JP19K22850.

ABSTRACT In this work, we study two classes of quasi-cyclic (QC) codes and examine how several properties can be combined into the codes of these classes. We start with the class of QC codes generated by diagonal generator polynomial matrices; a QC code in this class is a direct sum of cyclic codes. Then we move on to the class of QC codes of index 2; various binary codes with good parameters are found in this class. In each class, we describe the generator polynomial matrices of reversible codes, self-orthogonal codes, and self-dual codes. Hence, we demonstrate how such properties can be merged in codes of these classes. Particularly for QC codes of index 2, we prove a necessary and sufficient condition for the self-orthogonality of reversible codes. Then we show that reversible QC codes of index 2 are self-dual under the same conditions in which self-dual codes are reversible. We clarify that self-orthogonal reversible QC codes of index 2 over $\mathbb{F}_q$ exist for even and odd q, however self-dual reversible codes exist only for even q. Theoretical results are reinforced by several numerical examples. Computer search is used to present some self-dual reversible QC codes of index 2 that have the best known parameters as linear codes. Finally, we highlight the class of 1-generator binary QC codes of index 2 by exploring many self-dual reversible codes that achieve the upper bound on the minimum distance for their parameters.

INDEX TERMS 1-generator quasi-cyclic code, best known parameters, generator polynomial matrix, self-orthogonal code.

I. INTRODUCTION

Cyclic codes over finite fields are easy to construct, encode and decode. Cyclic codes are naturally extended to the larger class of quasi-cyclic (QC) codes. A linear code is said to be QC of index ℓ if it is invariant under cyclic shifts of ℓ coordinates, where ℓ is a positive integer that meets this property. Linear codes achieving the best known parameters have been shown to be sometimes quasi-cyclic [1]–[3]. Various algebraic structures are used to represent QC codes. According to [4], QC codes are a subclass of generalized quasi-cyclic codes because their cyclic intervals are equal. Therefore, a QC code $\mathcal{Q}$ over $\mathbb{F}_q$ of index ℓ is identified by its unique reduced generator polynomial matrix G of size $\ell \times \ell$. In this structure, QC codes correspond to $\mathbb{F}_q[x]$-submodules of $\left(\mathbb{F}_q[x]\right)^\ell$. Several classes of QC codes over $\mathbb{F}_q$ of length $m\ell$ have been considered in literature. For example, the class of QC codes generated by unfolding cyclic codes of length m over $\mathbb{F}_{q^\ell}$ [5], [6], and the class of QC codes generated by diagonal generator polynomial matrices, denoted by

$$G = \mathrm{diag}[g_{1,1}, g_{2,2}, \ldots, g_{\ell,\ell}], \quad g_{i,i} \in \mathbb{F}_q[x] \text{ for } 1 \leq i \leq \ell.$$

In the latter case, the QC code is a direct sum of ℓ cyclic codes $\mathcal{C}_i$ over $\mathbb{F}_q$ of length m and generator polynomials $g_{i,i}$.

A code is said to be reversible if it is invariant under reversing the coordinates of its codewords. Recently, reversible codes have their applications in data storage systems, e.g., constructing locally repairable codes [7] and designing DNA codes [8]–[11]. Massey introduced reversible cyclic codes in [12], as he proved that the cyclic code generated by $g(x) \in \mathbb{F}_q[x]$ is reversible if and only if $g(x)$ is self-reciprocal, i.e., $g^*(x) = \alpha g(x)$ for some $\alpha \in \mathbb{F}_q - \{0\}$, where $f^*(x) = x^{\deg(f(x))} f\left(\frac{1}{x}\right)$ is the reciprocal polynomial of $f(x)$. On the other hand, a code is self-orthogonal (respectively, self-dual) if it is contained in (respectively, equal to) its dual code. Researchers were interested in achieving these properties in error correcting codes because some classical open problems relate to finding such codes with good parameters, e.g., [13], [14].

The associate editor coordinating the review of this manuscript and approving it for publication was Majed Haddad.

In this article, we investigate the QC codes in two specific classes in which multiple properties are merged. The first class is the class of QC codes generated by diagonal generator polynomial matrices. In this class, Proposition 1 provides an equivalent condition for reversibility and an equivalent condition for self-orthogonality. Hence, the corresponding condition for self-duality is deduced in Corollary 1. Some examples are also used to illustrate how self-duality and reversibility can be combined for QC codes with diagonal generator polynomial matrix G. Thereafter, we consider the class of QC codes of index $\ell = 2$. In this class, we prove conditions equivalent to reversibility, self-orthogonality, and self-duality, separately. Although [13, Theorem 1] offers a sufficient condition for reversibility of 1-generator QC codes, our conditions are necessary and sufficient, do not assume m coprime to q, and are not limited to 1-generator codes. Once reversible QC codes of index 2 are specified, we establish equivalent conditions for appending self-orthogonality and self-duality to these codes. For QC codes of index 2, Corollaries 3 and 4 show that self-dual codes are reversible under the same conditions in which reversible codes are self-dual. Specifically, these conditions are $g_{1,1}g_{2,2} = x^m + 1$ and q is even. In fact, this result generalizes that of [13, Corollary 4]. Although Examples 5 and 6 show that self-orthogonal reversible QC codes over $\mathbb{F}_q$ of index 2 exist for odd and even q, we demonstrate that self-dual reversible QC codes can only exist for even q. This result was partially confirmed in [13, Section 5.3] for 1-generator QC codes of index 2 and $\gcd(m, q) = 1$.

A linear code is called optimal if it meets the best known parameters. That is, a linear code that achieves the upper bound on the minimum distance provided by [15] is an optimal code. As an application, we use computer search to examine the ability to append optimality to self-dual reversible QC codes of index 2. We show that this is possible by introducing some examples of optimal self-dual reversible QC codes of various code lengths and dimensions. Finally, we consider the class of binary 1-generator QC codes of index 2. In literature, computer search is used to discover new good QC codes in different classes, e.g., [16]. By computer search, we present several binary optimal self-dual reversible QC codes in the class of index 2.

The rest of this article is organized as follows. Some preliminaries are presented in Section II. In Section III, we investigate the reversibility, self-orthogonality, and self-duality of QC codes with diagonal generator polynomial matrix G. These properties for the class of QC codes of index $\ell = 2$ are considered in Section IV. Section V considers combining different properties in this class and presents many numerical examples. We conclude our results in Section VI.

II. PRELIMINARIES

For a prime power q, the finite field of q elements is denoted by $\mathbb{F}_q$. We refer to QC codes, cyclic codes, and codewords by $\mathcal{Q}$, $\mathcal{C}$, and $\mathbf{c}$, respectively. The dimension of the QC code $\mathcal{Q}$ and its minimum Hamming distance are denoted by k and $d_{\min}$, respectively. A cyclic code over $\mathbb{F}_q$ of length n is a linear subspace of $\mathbb{F}_q^n$ that is invariant under cyclic shifts of codewords, whereas a QC code over $\mathbb{F}_q$ of length n and index ℓ is a linear subspace of $\mathbb{F}_q^n$ invariant under cyclic shifts of codewords by ℓ coordinates. The index ℓ of a QC code divides the code length, i.e., $n = m\ell$ for some positive integer m. A codeword $\mathbf{c} \in \mathcal{Q}$ given by

$$\mathbf{c} = \left(c_{1,0}, \ldots, c_{\ell,0}, c_{1,1}, \ldots, c_{\ell,1}, \ldots, c_{1,m-1}, \ldots, c_{\ell,m-1}\right), \tag{1}$$

where $c_{i,j} \in \mathbb{F}_q$ for $1 \le i \le \ell$ and $0 \le j \le m-1$, can be divided to ℓ subwords c_i each of length m. Namely, $\mathbf{c} = (c_1, c_2, \ldots, c_\ell)$, where $c_i = (c_{i,0}, c_{i,1}, \ldots, c_{i,m-1})$.

Similar to cyclic codes, codewords of QC codes can be represented by polynomials. The codeword given by (1) is represented by the polynomial vector

$$\mathbf{c} = (c_1(x), c_2(x), \ldots, c_\ell(x)) \in \left(\mathbb{F}_q[x]\right)^\ell,$$

where $c_i(x) = \sum_{j=0}^{m-1} c_{i,j}x^j \in \mathbb{F}_q[x]$ for $1 \le i \le \ell$. In this representation, the cyclic shift of a codeword by ℓ coordinates corresponds to multiplication by x followed by a reduction modulo $x^m - 1$. Consequently, the QC codes over $\mathbb{F}_q$ of index ℓ and length $m\ell$ are in one-to-one correspondence with the $\mathbb{F}_q[x]$-submodules of $\left(\mathbb{F}_q[x]\right)^\ell$ that contain $(x^m-1)\left(\mathbb{F}_q[x]\right)^\ell$. A generator polynomial matrix of $\mathcal{Q}$ is a polynomial matrix whose rows generate $\mathcal{Q}$ as an $\mathbb{F}_q[x]$-module. Therefore, if G is a generator polynomial matrix of some QC code, then there is an $\ell \times \ell$ polynomial matrix A such that

$$AG = \operatorname{diag}[x^m - 1, \ldots, x^m - 1], \tag{2}$$

where $\operatorname{diag}[x^m - 1, \ldots, x^m - 1]$ is the $\ell \times \ell$ diagonal matrix whose diagonal entries are $x^m - 1$. Elementary row operations over $\mathbb{F}_q[x]$ reduce a generator polynomial matrix to its unique reduced form [4], which we refer to as $G = [g_{i,j}]$. The reduced generator polynomial matrix G is the $\ell \times \ell$ upper triangular matrix

$$G = \begin{bmatrix} g_{1,1} & g_{1,2} & g_{1,3} & \cdots & g_{1,\ell} \\ 0 & g_{2,2} & g_{2,3} & \cdots & g_{2,\ell} \\ 0 & 0 & g_{3,3} & \cdots & g_{3,\ell} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & g_{\ell,\ell} \end{bmatrix} \tag{3}$$

such that:

1) For each $1 \le i \le \ell$, $g_{i,i}$ is a monic divisor of $x^m - 1$ and has a minimum degree among all codewords of the form $(0, \ldots, 0, c_i(x), \ldots, c_\ell(x))$ with $c_i(x) \ne 0$.
2) For $1 \le i \ne j \le \ell$, we have $\deg(g_{i,j}) < \deg(g_{j,j})$.

In [4], the dimension of $\mathcal{Q}$ is given by

$$k = \sum_{i=1}^{\ell} \left(m - \deg(g_{i,i})\right). \tag{4}$$

In addition, $\mathbf{c}$ is a codeword of $\mathcal{Q}$ if and only if there exist $a_i(x) \in \mathbb{F}_q[x]$ for $1 \le i \le \ell$ such that

$$\mathbf{c} = [a_1(x)\ a_2(x)\ \cdots\ a_\ell(x)]\, G. \tag{5}$$

From (5), one concludes that G is diagonal if and only if $\mathcal{Q}$ is a direct sum of ℓ cyclic codes $\mathcal{C}_i$ of lengths m. That is

$$G = \text{diag}[g_{1,1}, g_{2,2}, \ldots, g_{\ell,\ell}] \iff \mathcal{Q} = \bigoplus_{i=1}^{\ell} \mathcal{C}_i.$$

The QC code $\mathcal{Q}$ is also identified by its unique reduced parity check polynomial matrix H [4]. The relation between H and the polynomial matrix A that satisfies (2) is shown in [4, Theorem 1]. Hereinafter, $\mathcal{Q}$ refers to a QC code over $\mathbb{F}_q$ of index ℓ, length $n = m\ell$, dimension k, minimum distance $d_{\min}$, reduced generator polynomial matrix G, and reduced parity check polynomial matrix H. We denote the dual code of $\mathcal{Q}$ by $\mathcal{Q}^{\perp}$. In fact, $\mathcal{Q}^{\perp}$ is a QC code of length $m\ell$, dimension $m\ell - k$, and a generator polynomial matrix H. The code $\mathcal{Q}$ is self-orthogonal, i.e., $\mathcal{Q} \subseteq \mathcal{Q}^{\perp}$, if and only if $G = MH$ for some polynomial matrix M. Whereas $\mathcal{Q}$ is self-dual, i.e., $\mathcal{Q} = \mathcal{Q}^{\perp}$, if and only if $G = MH$ for an invertible polynomial matrix M. For a codeword $\mathbf{c} \in \mathcal{Q}$ as given by (1), we refer to its reverse by $\mathbf{r}$. That is,

$$\mathbf{r} = \left(c_{\ell,m-1}, \ldots, c_{1,m-1}, c_{\ell,m-2}, \ldots, c_{1,m-2}, \ldots, c_{\ell,0}, \ldots, c_{1,0}\right).$$

We call $\mathcal{Q}$ reversible if $\mathbf{r} \in \mathcal{Q}$ for every $\mathbf{c} \in \mathcal{Q}$. In polynomial representation $\mathbf{r} = (r_1(x), r_2(x), \ldots, r_{\ell-1}(x), r_\ell(x))$, where $r_i(x)$ for $1 \le i \le \ell$ is given by

$$r_i(x) = \sum_{j=0}^{m-1} c_{\ell-i+1,j} x^{m-1-j} = x^{m-1} c_{\ell-i+1}\left(\frac{1}{x}\right) \in \mathbb{F}_q[x].$$

Hence, $\mathcal{Q}$ is a reversible code if and only if

$$\mathbf{r} = \left(x^{m-1} c_\ell\left(\frac{1}{x}\right), x^{m-1} c_{\ell-1}\left(\frac{1}{x}\right), \ldots, x^{m-1} c_1\left(\frac{1}{x}\right)\right) \tag{6}$$

is in $\mathcal{Q}$ for every $\mathbf{c} = (c_1(x), \ldots, c_{\ell-1}(x), c_\ell(x)) \in \mathcal{Q}$.

III. REVERSIBILITY AND SELF-ORTHOGONALITY FOR QC CODES GENERATED BY DIAGONAL G

In this section, we consider the class of QC codes generated by diagonal generator polynomial matrices of the form

$$G = \text{diag}[g_{1,1}, g_{2,2}, \ldots, g_{\ell,\ell}]. \tag{7}$$

We present conditions on G that characterize the reversibility, self-orthogonality, and self-duality of $\mathcal{Q}$. Then we fulfill these conditions in some numerical examples.

Proposition 1: Let $\mathcal{Q}$ be a QC code over $\mathbb{F}_q$ of index ℓ, length $m\ell$, and generator polynomial matrix

$$G = \text{diag}[g_{1,1}, g_{2,2}, \ldots, g_{\ell,\ell}],$$

where $g_{i,i} \in \mathbb{F}_q[x]$ divides $x^m - 1$ for $1 \le i \le \ell$.

1) *The code $\mathcal{Q}$ is a reversible code if and only if there exist $\alpha_i \in \mathbb{F}_q - \{0\}$ such that*

$$g^*_{i,i} = \alpha_i g_{\ell-i+1,\ell-i+1} \quad \text{for every } 1 \le i \le \ell.$$

2) *The code $\mathcal{Q}$ is a self-orthogonal code if and only if*

$$g_{i,i} g^*_{i,i} \equiv 0 \pmod{x^m - 1} \quad \text{for every } 1 \le i \le \ell.$$

Proof: We start with the reversibility conditions. Assume $g^*_{i,i} = \alpha_i g_{\ell-i+1,\ell-i+1}$ for every $1 \le i \le \ell$. Then $\deg(g_{\ell-i+1,\ell-i+1}) = \deg(g^*_{i,i}) = \deg(g_{i,i})$, which we denote by d_i. For any $\mathbf{c} \in \mathcal{Q}$, (5) shows that there exist $a_1(x), \ldots, a_\ell(x) \in \mathbb{F}_q[x]$ such that

$$\mathbf{c} = \left(a_1(x) g_{1,1}, a_2(x) g_{2,2}, \ldots, a_\ell(x) g_{\ell,\ell}\right).$$

For $1 \le i \le \ell$, let

$$b_i(x) = \alpha_{\ell-i+1} x^{m-1-d_i} a_{\ell-i+1}\left(\frac{1}{x}\right).$$

Then $b_i(x) \in \mathbb{F}_q[x]$ because $\deg(a_{\ell-i+1}) \le m - 1 - d_i$. Consider the codeword $\mathbf{r} \in \mathcal{Q}$ given by

$$\begin{aligned}\mathbf{r} &= \left(b_1(x) g_{1,1}, b_2(x) g_{2,2}, \ldots, b_\ell(x) g_\ell\right) \\ &= \left(x^{m-1-d_\ell} a_\ell\left(\frac{1}{x}\right) g^*_{\ell,\ell}, \ldots, x^{m-1-d_1} a_1\left(\frac{1}{x}\right) g^*_{1,1}\right) \\ &= \left(x^{m-1} a_\ell\left(\frac{1}{x}\right) g_{\ell,\ell}\left(\frac{1}{x}\right), \ldots, x^{m-1} a_1\left(\frac{1}{x}\right) g_{1,1}\left(\frac{1}{x}\right)\right).\end{aligned}$$

From (6), $\mathbf{r}$ is the reverse of $\mathbf{c}$. Hence, $\mathcal{Q}$ is reversible.

Conversely, assume $\mathcal{Q}$ is reversible. For $1 \le i \le \ell$, let $\mathbf{c}_i \in \mathcal{Q}$ be the codeword corresponding to the i^{th} row of G, i.e., coordinates of $\mathbf{c}_i$ are all zero except the i^{th} coordinate is $g_{i,i}(x)$. From (6), the reverse $\mathbf{r}_i$ of $\mathbf{c}_i$ has all zero coordinates except the $(\ell - i + 1)^{\text{th}}$ coordinate is $x^{m-1} g_{i,i}\left(\frac{1}{x}\right) = x^{m-d_i-1} g^*_{i,i}(x)$. Since $\mathbf{r}_i \in \mathcal{Q}$, $g_{\ell-i+1,\ell-i+1}(x) | x^{m-d_i-1} g^*_{i,i}(x)$. That is,

$$g_{\ell-i+1,\ell-i+1}(x) | g^*_{i,i}(x).$$

Replacing i by $\ell - i + 1$, we get $g_{i,i}(x) | g^*_{\ell-i+1,\ell-i+1}(x)$. That is,

$$g^*_{i,i}(x) | g_{\ell-i+1,\ell-i+1}(x).$$

Hence $g^*_{i,i}(x) = \alpha_i g_{\ell-i+1,\ell-i+1}(x)$ for some $\alpha_i \in \mathbb{F}_q - \{0\}$.

Now we prove the self-orthogonality conditions. Since G is a diagonal matrix, $\mathcal{Q} = \bigoplus_{i=1}^{\ell} \mathcal{C}_i$ for some cyclic codes $\mathcal{C}_i$ of length m over $\mathbb{F}_q$. We denote the Euclidean inner product for the codewords $c_i, c'_i \in \mathcal{C}_i$ (respectively, $\mathbf{c}, \mathbf{c}' \in \mathcal{Q}$) by $\langle c_i, c'_i \rangle$ (respectively, $\langle \mathbf{c}, \mathbf{c}' \rangle$). If $\mathbf{c} = (c_1, \ldots, c_\ell)$ and $\mathbf{c}' = (c'_1, \ldots, c'_\ell)$, where $c_i, c'_i \in \mathcal{C}_i$, then

$$\langle \mathbf{c}, \mathbf{c}' \rangle = \sum_{i=1}^{\ell} \langle c_i, c'_i \rangle.$$

We show that $\mathcal{Q}$ is self-orthogonal if and only if $\mathcal{C}_i$ is self-orthogonal for every $1 \le i \le \ell$. Assume that $\mathcal{Q}$ is self-orthogonal. Since $\mathcal{Q} = \bigoplus_{i=1}^{\ell} \mathcal{C}_i$, the code $\mathcal{Q}$ contains an isomorphic copy of $\mathcal{C}_i$ for each $1 \le i \le \ell$. Then, for every codeword $c_i \in \mathcal{C}_i$, there exists a codeword in $\mathcal{Q}$ with all zero components except the i^{th} component is c_i. Therefore, the self-orthogonality of $\mathcal{Q}$ implies the self-orthogonality of $\mathcal{C}_i$. Conversely, assume that $\mathcal{C}_i$ is self-orthogonal for every $1 \le i \le \ell$. Then $\mathcal{Q}$ is self-orthogonal because

$$\langle \mathbf{c}, \mathbf{c}' \rangle = \sum_{i=1}^{\ell} \langle c_i, c'_i \rangle = \sum_{i=1}^{\ell} 0 = 0, \quad \forall \mathbf{c}, \mathbf{c}' \in \mathcal{Q}.$$

The result follows from the fact that the cyclic code $\mathcal{C}_i$ is self-orthogonal if and only if $g_{i,i}g_{i,i}^* \equiv 0 \pmod{x^m-1}$. ■

The reversibility condition in Proposition 1 generalizes the well-known result [12]. In fact, a cyclic code with a generator polynomial $g(x)$ is a QC code of index $\ell = 1$ and $G = [g(x)]$. If we consider Proposition 1 in the particular case of cyclic codes, it is required that $g(x) = \alpha g^*(x)$ for some $\alpha \in \mathbb{F}_q - \{0\}$ as a condition equivalent to reversibility.

Corollary 1: Let $\mathcal{Q}$ be a QC code over $\mathbb{F}_q$ of index ℓ, length $m\ell$, and generator polynomial matrix

$$G = \text{diag}[g_{1,1}, g_{2,2}, \ldots, g_{\ell,\ell}],$$

where $g_{i,i} \in \mathbb{F}_q[x]$ divides $x^m - 1$ for $1 \le i \le \ell$. The code $\mathcal{Q}$ is a self-dual code if and only if the following conditions are met:

1) *q and m are even.*
2) *There exist $\beta_i \in \mathbb{F}_q - \{0\}$ such that*

$$g_{i,i}g_{i,i}^* = \beta_i \left(x^m - 1\right), \quad \text{for every } 1 \le i \le \ell$$

Proof: Similar to the proof of Proposition 1, $\mathcal{Q}$ is self-dual if and only if $\mathcal{C}_i$ is self-dual for every $1 \le i \le \ell$. From [17, Proposition 1] and [17, Theorem 1], the proposed conditions are equivalent to the self-duality of each cyclic code $\mathcal{C}_i$. ■

Two conditions of reversibility and self-duality for QC codes with diagonal generator polynomial matrix G are generally independent. That is, we can construct a self-dual QC code which is not reversible, a reversible one which is not self-dual, and a reversible self-dual one. We illustrate these different cases with the following example.

Example 1: We consider QC codes over $\mathbb{F}_4$ of $n = 36, k = 18, \ell = 2$, and generated by diagonal generator polynomial matrices. The factorization of $x^{18}+1$ in $\mathbb{F}_4[x]$ into irreducible factors is

$$(x+1)^2(x+\omega)^2(x+\omega^2)^2(x^3+\omega)^2(x^3+\omega^2)^2,$$

where ω is a zero to $x^2+x+1 \in \mathbb{F}_2[x]$. Let

$$\begin{aligned} G_1 &= \text{diag}[(x+\omega)^2\, g, (x+\omega^2)^2\, g] \\ G_2 &= \text{diag}[(x+1)(x+\omega)g, (x+1)(x+\omega^2)g^*] \\ G_3 &= \text{diag}[(x+\omega)^2\, g, (x+\omega^2)^2\, g^*], \end{aligned}$$

where $g = (x+1)(x^3+\omega)^2$. By Proposition 1 and Corollary 1, G_1 generates a self-dual QC code which is not reversible, G_2 generates a reversible QC code which is not self-dual, and G_3 generates a reversible self-dual QC code.

IV. REVERSIBILITY AND SELF-ORTHOGONALITY FOR QC CODES OF INDEX 2

In this section, we focus on the class of QC codes over $\mathbb{F}_q$ of length $2m$ and index $\ell = 2$. We separately prove necessary and sufficient conditions for reversibility, self-orthogonality, and self-duality of QC codes in this class.

Theorem 1: Let $\mathcal{Q}$ be a QC code over $\mathbb{F}_q$ of length $2m$, index 2, and reduced generator polynomial matrix

$$G = \begin{bmatrix} g_{1,1} & g_{1,2} \\ 0 & g_{2,2} \end{bmatrix}, \tag{8}$$

where $g_{1,1}$ and $g_{2,2}$ divide $x^m - 1$. Let

$$\mu = \gcd(g_{1,2}, g_{2,2}), f_1 = \frac{g_{1,2}}{\mu}, f_2 = \frac{g_{2,2}}{\mu}, \text{ and } h = \frac{x^m-1}{g_{2,2}}.$$

Then,

1) *The code $\mathcal{Q}$ is reversible if and only if the following conditions are met*:
   a) *$g_{1,1} = \alpha\mu^*$ for some $\alpha \in \mathbb{F}_q - \{0\}$.*
   b) *f_2 is a self-reciprocal polynomial.*
   c) *f_2 divides $\left(x^{m-\deg(f_1)} f_1 f_1^* - \alpha^2\right)$.*
2) *The code $\mathcal{Q}$ is self-orthogonal if and only if the following conditions are met*:
   a) *$\mu = \beta h^*$ for some $\beta \in \mathbb{F}_q[x] - \{0\}$.*
   b) *$g_{1,1}g_{1,1}^* = \gamma\mu h$ for some $\gamma \in \mathbb{F}_q[x] - \{0\}$.*
   c) *f_2 divides $\left(\beta^* x^{m+d_{11}-d_{12}} f_1 f_1^* + \gamma\right)$, where $d_{ij} = \deg(g_{i,j})$ for $1 \le i, j \le 2$.*

Proof: By assumption, G can be written as

$$G = \begin{bmatrix} g_{1,1} & \mu f_1 \\ 0 & \mu f_2 \end{bmatrix},$$

where $g_{1,1}, \mu, f_2$ are factors of $x^m - 1$. From [4, Theorem 1], a parity check polynomial matrix for $\mathcal{Q}$ is

$$H = \begin{bmatrix} (x^m-1)/g_{1,1}^* & 0 \\ -x^{m+d_{11}-d_{12}} f_1^* \mu^* h^* / g_{1,1}^* & h^* \end{bmatrix}. \tag{9}$$

We start with the reversibility conditions. If $\mathcal{Q}$ is reversible, the reverses of the codewords

$$\mathbf{c}_1 = (g_{1,1}, g_{1,2}), \quad \mathbf{c}_2 = (0, g_{2,2}),$$

using (6), are the codewords

$$\begin{aligned} \mathbf{r}_1 &= x^{m-1}\left(g_{1,2}\left(\frac{1}{x}\right), g_{1,1}\left(\frac{1}{x}\right)\right) \\ &= \left(x^{m-d_{12}-1}\mu^* f_1^*, x^{m-d_{11}-1} g_{1,1}^*\right), \\ \mathbf{r}_2 &= \left(x^{m-1} g_{2,2}\left(\frac{1}{x}\right), 0\right) = \left(x^{m-d_{22}-1}\mu^* f_2^*, 0\right). \end{aligned}$$

Then, there exist $a_1(x), a_2(x), a_3(x), a_4(x) \in \mathbb{F}_q[x]$ such that

$$a_1(x)g_{1,1} = x^{m-d_{12}-1}\mu^* f_1^*, \tag{10}$$

$$a_1(x)\mu f_1 + a_2(x)\mu f_2 = x^{m-d_{11}-1} g_{1,1}^*, \tag{11}$$

$$a_3(x)g_{1,1} = x^{m-d_{22}-1}\mu^* f_2^*, \tag{12}$$

$$a_3(x)\mu f_1 + a_4(x)\mu f_2 = 0. \tag{13}$$

From (10) and (12), $g_{1,1} | \mu^* f_1^*$ and $g_{1,1} | \mu^* f_2^*$. Thus, $g_{1,1} | \mu^*$ because f_1 and f_2 are coprime. Thus $g_{1,1} | \mu^*$. From (11), $\mu | g_{1,1}^*$, hence $\mu^* | g_{1,1}$. Consequently, condition (1a) follows. Substituting (12) in (13) with the use of condition (1a), we get

$$x^{m-d_{22}-1} f_2^* f_1 + \alpha a_4(x) f_2 = 0.$$

Since f_2 is coprime to $x^{m-d_{22}-1} f_1$, $f_2 | f_2^*$, i.e., f_2 is self-reciprocal polynomial. Substituting (10) in (11) with the

use of condition (1a), we get $\alpha a_2(x) f_2 = \alpha^2\, x^{m-d_{11}-1} - x^{m-d_{12}-1} f_1\, f_1^*$. Equivalently,

$$\begin{aligned}\alpha x^{d_{11}+1} a_2(x) f_2 &= \left(\alpha^2\, x^m - x^{m-d_{12}+d_{11}} f_1\, f_1^*\right)\\ &= \left(\alpha^2\left(x^m-1\right) - \left(x^{m-\deg(f_1)} f_1\, f_1^* - \alpha^2\right)\right).\end{aligned}$$

Condition (1c) follows because $f_2 | (x^m - 1)$.

Conversely, if conditions (1a), (1b), and (1c) are met, then, there exist $a_1(x), a_2(x), a_3(x), a_4(x) \in \mathbb{F}_q[x]$ satisfying (10) to (13). For any codeword $\mathbf{c} \in \mathcal{Q}$, there exist $b_1(x), b_2(x) \in \mathbb{F}_q[x]$ such that

$$\mathbf{c} = (b_1\, g_{1,1},\, b_1\, g_{1,2} + b_2\, g_{2,2}).$$

Let $\mathbf{r}$ be the codeword of $\mathcal{Q}$ given by

$$\begin{aligned}\mathbf{r} = \Big(&\left(a_1(x) b_1(x^{m-1}) + a_3(x) b_2(x^{m-1})\right) g_{1,1},\\ &\left(a_1(x) b_1(x^{m-1}) + a_3(x) b_2(x^{m-1})\right) g_{1,2}\\ &+ \left(a_2(x) b_1(x^{m-1}) + a_4(x) b_2(x^{m-1})\right) g_{2,2}\Big).\end{aligned}$$

Using (10) to (13) and reduction modulo $x^m - 1$, we get

$$\begin{aligned}\mathbf{r} \equiv \Big(&x^{m-1} b_1\left(\frac{1}{x}\right) g_{1,2}\left(\frac{1}{x}\right) + x^{m-1} b_2\left(\frac{1}{x}\right) g_{2,2}\left(\frac{1}{x}\right),\\ &x^{m-1} b_1\left(\frac{1}{x}\right) g_{1,1}\left(\frac{1}{x}\right)\Big) \in \mathcal{Q}.\end{aligned}$$

From (6), $\mathbf{r}$ is the reverse of $\mathbf{c}$. Hence, $\mathcal{Q}$ is reversible.

Now we prove the self-orthogonality conditions. The code $\mathcal{Q}$ is self-orthogonal if and only if $G = MH$ for some polynomial matrix M. Equivalently, there exist $m_1, m_2, m_3, m_4 \in \mathbb{F}_q[x]$ such that

$$\begin{aligned} m_1\left(x^m - 1\right) - m_2 x^{m+d_{11}-d_{12}} f_1^* \mu^* h^* &= g_{1,1} g_{1,1}^*, && (14)\\ m_2 h^* &= \mu f_1, && (15)\\ m_3\left(x^m - 1\right) - m_4 x^{m+d_{11}-d_{12}} f_1^* \mu^* h^* &= 0, && (16)\\ m_4 h^* &= \mu f_2. && (17)\end{aligned}$$

If $\mathcal{Q}$ is self-orthogonal, then $h^* | \mu$ due to the coprimality of f_1 and f_2, (15), and (17). Hence, condition (2a) follows. Equation (14) reduces to

$$\begin{aligned} g_{1,1} g_{1,1}^* &= m_1\left(x^m - 1\right) - \beta f_1\, x^{m+d_{11}-d_{12}} f_1^* \mu^* h^*\\ &= m_1\left(x^m - 1\right) - x^{m+d_{11}-d_{12}} f_1\, f_1^* \mu^* \mu\\ &= m_1\left(x^m - 1\right) - x^{m+d_{11}-d_{12}} f_1\, f_1^* \beta^* h \mu\\ &= \left(m_1 f_2 - \beta^* x^{m+d_{11}-d_{12}} f_1\, f_1^*\right) \mu h\\ &= \gamma\, \mu h,\end{aligned}$$

where $\gamma = \left(m_1 f_2 - \beta^* x^{m+d_{11}-d_{12}} f_1\, f_1^*\right)$. That is, $m_1 f_2 = \beta^* x^{m+d_{11}-d_{12}} f_1\, f_1^* + \gamma$ and condition (2c) follows.

Conversely, assume conditions (2a), (2b), and (2c) are satisfied. Then $G = MH$ for the polynomial matrix

$$M = \begin{bmatrix} \left(\beta^* x^{m+d_{11}-d_{12}} f_1 f_1^* + \gamma\right)/f_2 & \beta f_1\\ \beta^* x^{m+d_{11}-d_{12}} f_1^* & \beta f_2 \end{bmatrix}. \quad (18)$$

Hence, $\mathcal{Q}$ is self-orthogonal. ■

Corollary 2: The QC code $\mathcal{Q}$ is self-dual if and only if the following conditions are met:

1) $\mu = \beta h^*$ *for some* $\beta \in \mathbb{F}_q - \{0\}$.
2) $g_{1,1} g_{1,1}^* = \gamma\, \mu h$ *for some* $\gamma \in \mathbb{F}_q - \{0\}$.
3) f_2 *divides* $\left(x^{m-\deg(f_1)} f_1\, f_1^* + \gamma \beta^{-1}\right)$.

Proof: The code $\mathcal{Q}$ is self-dual if and only if the polynomial matrix M given by (18) is invertible. The determinant of M is $\det(M) = \beta\gamma$. Then, M is invertible if and only if $\beta, \gamma \in \mathbb{F}_q - \{0\}$. In addition, since $\deg(\mu) = \deg(h) = \deg(g_{1,1})$, $m + d_{11} - d_{12} = m - \deg(f_1)$. ■

For even and odd q, the following examples emphasize the existence of reversible codes that are not self-dual and vice versa.

Example 2: In $\mathbb{F}_2[x]$, we have $x^6 + 1 = (x+1)^2 (x^2 + x + 1)^2$. Let $\mathcal{Q}$ be the binary QC code of length 12, index $\ell = 2$, and reduced generator polynomial matrix

$$G = \begin{bmatrix} (x+1)^2 & x(x+1)^2\\ 0 & (x+1)^2 (x^2 + x + 1) \end{bmatrix}.$$

From Theorem 1, $\mathcal{Q}$ is reversible because

1) $\mu^* = \gcd(g_{1,2}, g_{2,2})^* = (x+1)^2 = g_{1,1}$, i.e., $\alpha = 1$.
2) $f_2 = g_{2,2}/\mu = x^2 + x + 1$ is self-reciprocal.
3) $f_1 = g_{1,2}/\mu = x$. Hence, $\left(x^{m-\deg(f_1)} f_1\, f_1^* - \alpha^2\right) = x^5(x)(1) + 1 = x^6 + 1$ is divisible by f_2.

From (4), although the dimension of $\mathcal{Q}$ is $k = 6 = n/2$, $\mathcal{Q}$ is not self-dual because condition (1) of Corollary 2 is not satisfied. In particular, $h^* = x^2 + x + 1 \neq \mu$.

Example 3: In $\mathbb{F}_2[x]$, we have

$$x^{14} + 1 = (x+1)^2 (x^3 + x + 1)^2 (x^3 + x^2 + 1)^2.$$

Let $\mathcal{Q}$ be the binary QC code of length 28, index 2, and reduced generator polynomial matrix

$$G = \begin{bmatrix} (x^3+x+1)(x^3+x^2+1) & x(x^3+x+1)^2\\ 0 & (x+1)^2 (x^3+x+1)^2 \end{bmatrix}.$$

From Corollary 2, the code $\mathcal{Q}$ is self-dual because

1) $\mu = \gcd(g_{1,2}, g_{2,2}) = (x^3 + x + 1)^2 = h^*$, i.e., $\beta = 1$.
2) $g_{1,1} g_{1,1}^* = (x^3+x+1)^2 (x^3+x^2+1)^2 = \mu h$, i.e., $\gamma = 1$.
3) $f_1 = g_{1,2}/\mu = x$. Hence, $f_2 = (x+1)^2$ divides $\left(x^{m-\deg(f_1)} f_1\, f_1^* + \gamma \beta^{-1}\right) = x^{14} + 1$.

From Theorem 1, $\mathcal{Q}$ is not reversible because $g_{1,1} \neq \mu^*$.

Example 4: In $\mathbb{F}_5[x]$, we have

$$x^6 - 1 = (x+1)(x+4)(x^2 + x + 1)(x^2 + 4x + 1).$$

Let $\mathcal{Q}_1$ be the QC code over $\mathbb{F}_5$ of length 12, index 2, and reduced generator polynomial matrix

$$G_1 = \begin{bmatrix} x+4 & 4(x+1)(x+4)(x^2+x+2)\\ 0 & (x+4)(x^2+x+1)(x^2+4x+1) \end{bmatrix}.$$

From Theorem 1, $\mathcal{Q}_1$ is reversible because

1) $\mu = (x+4)$ and $g_{1,1} = 4\mu^*$, i.e., $\alpha = 4$.
2) $f_2 = (x^2 + x + 1)(x^2 + 4x + 1)$ is self-reciprocal.
3) $f_1 = 4(x+1)(x^2 + x + 2)$, hence f_2 divides

$$\begin{aligned}&\left(x^{m-\deg(f_1)} f_1\, f_1^* - \alpha^2\right)\\ &\quad = 2(x+2)(x+3)(x^2+x+1)(x^2+4x+1)(x^3+x^2+2).\end{aligned}$$

Although the dimension of $\mathcal{Q}_1$ is $k = 6 = n/2$, it is not self-dual because condition (1) of Corollary 2 is not satisfied.

Let $\mathcal{Q}_2$ be the QC code over $\mathbb{F}_5$ of length 12, index 2, and reduced generator polynomial matrix

$$G_2 = \begin{bmatrix} 1 & 2(x+3)(x^4+2x^2+2x+1) \\ 0 & x^6-1 \end{bmatrix}.$$

From Corollary 2, $\mathcal{Q}_2$ is self-dual because

1) $\mu = 1 = h^*$, i.e., $\beta = 1$.
2) $g_{1,1}g_{1,1}^* = 1 = \mu h$, i.e., $\gamma = 1$.
3) $f_1 = 2(x+3)(x^4+2x^2+2x+1)$, and f_2 divides

$$\left(x^{m-\deg(f_1)} f_1 f_1^* + \gamma\beta^{-1}\right) = 2(x^6-1)(x^2+2x+3)(x^3+2x+4).$$

Although $g_{1,1} = \alpha\mu^*$ for $\alpha = 1$ and f_2 is self-reciprocal, but $\mathcal{Q}_2$ is not reversible because condition (1c) of Theorem 1 is not satisfied.

V. OPTIMAL QC CODES OF INDEX 2 WITH SEVERAL PROPERTIES

In this section, we examine QC codes of index 2 that combine more than one property. We start with a self-orthogonality condition for reversible QC codes of index 2.

Theorem 2: Let $\mathcal{Q}$ be a reversible QC code over $\mathbb{F}_q$ of length $2m$, index 2, and generator polynomial matrix as given by (8). Then, $\mathcal{Q}$ is self-orthogonal if and only if

$$\begin{cases} g_{1,1}g_{2,2} \equiv 0 \pmod{x^m+1}, & \text{for even } q. \\ g_{1,1}g_{1,1}^* \equiv 0 \pmod{x^m-1}, & \text{for odd } q. \end{cases}$$

Proof: Let $\mathcal{Q}$ be a reversible code. If $\mathcal{Q}$ is self-orthogonal, then all conditions in Theorem 1 are met. For even q,

$$g_{1,1}g_{2,2} = \alpha\beta^* h g_{2,2} = \alpha\beta^*(x^m+1) \equiv 0 \pmod{x^m+1}.$$

However, for odd q, we have $\gamma = \alpha^2\beta^*$ because $\gamma\mu h = g_{1,1}g_{1,1}^* = \alpha\mu^*\alpha\mu = \alpha^2\beta^*\mu h$. But conditions (1c) and (2c) of Theorem 1 ensure that

$$\begin{aligned} \left(x^{m-\deg(f_1)} f_1 f_1^* - \alpha^2\right) &= \eta_1 f_2 \text{ and} \\ \beta^*\left(x^{m-\deg(f_1)} f_1 f_1^* + \alpha^2\right) &= \beta^*\left(x^{m+d_{11}-d_{12}} f_1 f_1^* + \alpha^2\right) \\ &= \left(\beta^* x^{m+d_{11}-d_{12}} f_1 f_1^* + \gamma\right) \\ &= \eta_2 f_2, \end{aligned}$$

for some $\eta_1, \eta_2 \in \mathbb{F}_q[x]$. Consequently,

$$\begin{aligned} g_{1,1}g_{1,1}^* &= \alpha^2\beta^*\mu h = \frac{1}{2}2\alpha^2\beta^*\mu h = \frac{1}{2}(\eta_2 - \beta^*\eta_1) f_2 \mu h \\ &= \frac{1}{2}(\eta_2 - \beta^*\eta_1)(x^m-1) \equiv 0 \pmod{x^m-1}. \end{aligned}$$

Conversely, if q is even and $g_{1,1}g_{2,2} = \eta(x^m+1)$ for some $\eta \in \mathbb{F}_q[x]$, then $g_{1,1} = \eta h$, and

1) $\mu = g_{1,1}^*/\alpha = \eta^* h^*/\alpha = \beta h^*$, where $\beta = \eta^*/\alpha$.
2) $g_{1,1}g_{1,1}^* = \eta h \alpha\mu = \gamma\mu h$, where $\gamma = \alpha\eta$.
3) From condition 1(c) of Theorem 1, f_2 divides

$$\left(\beta^* x^{m+d_{11}-d_{12}} f_1 f_1^* + \gamma\right) = \frac{\eta}{\alpha}\left(x^{m-\deg(f_1)} f_1 f_1^* + \alpha^2\right).$$

Hence $\mathcal{Q}$ is self-orthogonal by Theorem 1. Now, if q is odd and $g_{1,1}g_{1,1}^* = \eta(x^m-1)$ for some $\eta \in \mathbb{F}_q[x]$, then $\mathcal{Q}$ is self-orthogonal by Theorem 1 because

1) Since $\alpha^2\mu\mu^* = g_{1,1}g_{1,1}^* = \eta(x^m-1) = -\eta\mu^* f_2^* h^*$, $\mu = \beta h^*$ for $\beta = -\eta f_2^*/\alpha^2$.
2) $g_{1,1}g_{1,1}^* = \eta f_2 \mu h = \gamma\mu h$, where $\gamma = \eta f_2$.
3) f_2 divides $\left(\beta^* x^{m+d_{11}-d_{12}} f_1 f_1^* + \gamma\right)$ because it divides β^* and γ.

■

The following examples show that self-orthogonal reversible QC codes of index 2 exist for odd and even q.

Example 5: In $\mathbb{F}_3[x]$, we have $x^6-1 = (x-1)^3(x+1)^3$. Let $\mathcal{Q}$ be the ternary QC code of length 12 and index 2 generated by

$$G = \begin{bmatrix} (x-1)^2(x+1)^2 & -(x-1)^2(x+1)^2 \\ 0 & x^6-1 \end{bmatrix}.$$

The dimension of $\mathcal{Q}$ is $k = 2$ and its minimum distance is $d_{\min} = 6$. From Theorem 1, $\mathcal{Q}$ is reversible because

1) $g_{1,1} = \mu^* = \mu = (x-1)^2(x+1)^2$, i.e., $\alpha = 1$.
2) $f_2 = (x-1)(x+1)$ is self-reciprocal.
3) Since $f_1 = -1$, $\left(x^{m-\deg(f_1)} f_1 f_1^* - \alpha^2\right) = x^6 - 1$ is divisible by f_2.

Moreover, Theorem 2 shows that $\mathcal{Q}$ is self-orthogonal because $g_{1,1}g_{1,1}^* \equiv 0 \pmod{x^6-1}$. Hence, $\mathcal{Q}$ is self-orthogonal reversible code.

Example 6: In $\mathbb{F}_2[x]$, we have $x^{15}+1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$. Let $\mathcal{Q}$ be the binary QC code of length 30 and index 2 generated by

$$G = \begin{bmatrix} g_{1,1} & g_{1,2} \\ 0 & g_{2,2} \end{bmatrix},$$

where

$$\begin{aligned} g_{1,1} &= (x+1)(x^4+x+1), \\ g_{1,2} &= x(x+1)^2(x^3+x+1)(x^4+x^3+1), \\ g_{2,2} &= (x+1)(x^2+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1). \end{aligned}$$

The dimension of $\mathcal{Q}$ is $k = 14$ and its minimum distance is $d_{\min} = 8$. According to [15], $\mathcal{Q}$ achieves the upper bound on the minimum distance of binary linear codes of length 30 and dimension 14. Thus, we call $\mathcal{Q}$ an optimal code. From Theorem 1, $\mathcal{Q}$ is reversible because

1) $g_{1,1} = \mu^*$ because $\mu = (x+1)(x^4+x^3+1)$.
2) $f_2 = (x^2+x+1)(x^4+x^3+x^2+x+1)$ is self-reciprocal.
3) Since $f_1 = x(x+1)(x^3+x+1)$, f_2 divides

$$\begin{aligned} &\left(x^{m-\deg(f_1)} f_1 f_1^* - 1\right) \\ &= x^{11}(x+1)^2(x^3+x+1)(x^3+x^2+1)+1 \\ &= (x^2+x+1)(x^4+x^3+x^2+x+1) \\ &\quad (x^{13}+x^{12}+x^{11}+x^9+x^7+x^6+x^3+x^2+1). \end{aligned}$$

Moreover, $\mathcal{Q}$ is self-orthogonal by Theorem 2 since $g_{1,1}g_{2,2} \equiv 0 \pmod{x^m+1}$. Hence, $\mathcal{Q}$ combines optimality, self-orthogonality, and reversibility.

Although there are self-orthogonal reversible QC codes of index 2 for odd and even q (cf. Examples 5 and 6), the following results confirm that self-dual reversible codes exist only for even q. In addition, we demonstrate that the reversibility condition of self-dual codes is the same as the self-duality condition of reversible codes.

Corollary 3: Let $\mathcal{Q}$ be a reversible QC code over $\mathbb{F}_q$ of length $n = 2m$, index 2, and generator polynomial matrix G as given by (8)*. Then, $\mathcal{Q}$ is self-dual if and only if q is even and $g_{1,1}g_{2,2} = x^m + 1$.*

Proof: From (4), the dimension of $\mathcal{Q}$ is $k = 2m - d_{11} - d_{22}$. If $\mathcal{Q}$ is self-dual, then $k = m$ and $d_{11} + d_{22} = m$. From Theorem 2, if q is even, then $g_{1,1}g_{2,2} = \eta(x^m + 1)$. Hence $\deg(\eta) = d_{11} + d_{22} - m = 0$, i.e., $\eta \in \mathbb{F}_q$. The reduced form of G implies that $\eta = 1$, hence $g_{1,1}g_{2,2} = x^m + 1$. On the other hand, if q is odd, Theorem 2 implies that

$$0 \geq m - 2d_{11} = d_{22} - d_{11} = d_{22} - \deg(\mu) = \deg(f_2).$$

This is impossible unless $f_1 = 0$, i.e., G is diagonal, which contradicts Corollary 1 because a diagonal G generates a self-dual code only if q is even.

Conversley, if q is even and $g_{1,1}g_{2,2} = x^m + 1$, Theorem 2 shows that $\mathcal{Q}$ is self-orthogonal. Then $\mathcal{Q}$ is self-dual because $k = 2m - d_{11} - d_{22} = m = n/2$. ∎

Corollary 4: Let $\mathcal{Q}$ be a self-dual QC code over $\mathbb{F}_q$ of length $2m$, index 2, and generator polynomial matrix G as given by (8)*. Then, $\mathcal{Q}$ is reversible if and only if q is even and $g_{1,1}g_{2,2} = x^m + 1$.*

Proof: From Corollary 3, if $\mathcal{Q}$ is reversible, then the self-duality of $\mathcal{Q}$ implies that q is even and $g_{1,1}g_{2,2} = x^m + 1$. Conversely, if q is even and $g_{1,1}g_{2,2} = x^m + 1$, then $g_{1,1} = h$. By Theorem 1 and Corollary 2, $\mathcal{Q}$ is reversible because

1) $g_{1,1} = h = \mu^*/\beta = \alpha\mu^*$ for $\alpha = 1/\beta$.
2) f_2 is self-reciprocal since

$$f_2 = \frac{x^m+1}{\mu h} = \frac{x^m+1}{\beta h^* h} = \frac{x^m+1}{h^*\mu^*} = f_2^*.$$

3) Since $g_{1,1} = \alpha\mu^*$, $\gamma = \alpha$ and f_2 divides

$$\left(x^{m-\deg(f_1)} f_1 f_1^* + \gamma\beta^{-1}\right) = \left(x^{m-\deg(f_1)} f_1 f_1^* - \alpha^2\right).$$

∎

Proposition 2: Let $\mathcal{Q}$ be a self-orthogonal QC code over $\mathbb{F}_q$ of length $2m$, index 2, and generator polynomial matrix G as given by (8)*. If q is even, $g_{1,1} = \alpha\mu^*$, and $g_{1,1}g_{2,2}/(x^m+1)$ is coprime to f_2, then $\mathcal{Q}$ is reversible.*

Proof: From Theorem 1, we have $\mu = \beta h^*$, $g_{1,1}g_{1,1}^* = \gamma\mu h$, and $f_2 \mid \left(\beta^* x^{m+d_{11}-d_{12}} f_1 f_1^* + \gamma\right)$ for some $\beta, \gamma \in \mathbb{F}_q[x]$. Now, $\beta f_2 = \beta(x^m-1)/\mu h = (x^m-1)/h^* h = \beta^*(x^m-1)/h^*\mu^* = -\beta^* f_2^*$. Since $\left(g_{1,1}g_{2,2}\right)/(x^m+1) = \alpha\mu^*/h = \alpha\beta^*$ is coprime to f_2, we have $f_2 | f_2^*$, i.e., self-reciprocal. In addition, f_2 divides $\left(\beta^* x^{m+d_{11}-d_{12}} f_1 f_1^* + \gamma\right) = \beta^*\left(x^{m-\deg(f_1)} f_1 f_1^* + \alpha^2\right)$. Thus, the coprimality of f_2 and β^* implies condition (1c) of Theorem 1. Therefore, $\mathcal{Q}$ is reversible. ∎

Example 7: In $\mathbb{F}_4[x]$, we have $x^{16}+1 = (x+1)^{16}$. Let $\mathcal{Q}$ be the QC code over $\mathbb{F}_4$ of length 32, index 2, and

$$G = \begin{bmatrix} x+1 & g_{1,2} \\ 0 & (x+1)^{15} \end{bmatrix},$$

where $g_{1,2} = x^6(x+1)(x+\omega)(x^3+\omega^2)(x^3+x+1)$ and ω is a zero to $x^2+x+1 \in \mathbb{F}_2[x]$. By Theorem 1, $\mathcal{Q}$ is reversible because

1) $g_{1,1} = \mu^* = (x+1)$, i.e., $\alpha = 1$.
2) $f_2 = (x+1)^{14}$ is self-reciprocal.
3) $f_1 = x^6(x+\omega)(x^3+\omega^2)(x^3+x+1)$ and f_2 divides

$$\begin{aligned}\left(x^{m-\deg(f_1)} f_1 f_1^* - 1\right) &= (x+1)^{14}(x^2+\omega x+\omega) \\ &\quad (x^2+\omega^2 x+\omega^2)(x^5+x^4+x^3+x^2+1).\end{aligned}$$

Corollary 3 shows that the reversible code $\mathcal{Q}$ is self-dual because q is even and $g_{1,1}g_{2,2} = x^{16}+1$. The dimension of $\mathcal{Q}$ is $k = 16$ and its minimum distance is $d_{\min} = 10$.

According to [15], the best known minimum distance for a linear code over $\mathbb{F}_4$ of length 32 and dimension 16 is 11. Although the QC code of Example 7 is self-dual and reversible, it is not optimal. However, in the following examples, we illustrate that there are optimal self-dual reversible QC codes of index 2.

Example 8: In $\mathbb{F}_2[x]$, we have

$$x^7+1 = (x+1)(x^3+x+1)(x^3+x^2+1).$$

Let $\mathcal{Q}$ be the binary QC code of length 14, index 2, and

$$G = \begin{bmatrix} x^3+x^2+1 & x^3+x+1 \\ 0 & (x+1)(x^3+x+1) \end{bmatrix}.$$

With Theorem 1, one can prove that $\mathcal{Q}$ is reversible. From Corollary 3, $\mathcal{Q}$ is self-dual because q is even and $g_{1,1}g_{2,2} = x^7+1$. According to [15], $\mathcal{Q}$ is optimal because $d_{\min} = 4$, which is the upper bound on the minimum distance of a binary linear code of length 14 and dimension 7.

Example 9: In $\mathbb{F}_4[x]$, we have

$$\begin{aligned}x^{11}+1 = (x+1)&(x^5+\omega x^4+x^3+x^2+\omega^2 x+1) \\ &(x^5+\omega^2 x^4+x^3+x^2+\omega x+1),\end{aligned}$$

where ω is a zero to $x^2+x+1 \in \mathbb{F}_2[x]$. Let $\mathcal{Q}$ be the QC code over $\mathbb{F}_4$ of length 22, index 2, and

$$G = \begin{bmatrix} 1 & g_{1,2} \\ 0 & x^{11}+1 \end{bmatrix},$$

where

$$g_{1,2} = \omega^2 x^{10} + \omega x^9 + \omega^2 x^6 + \omega x^5 + \omega x^4 + \omega^2 x^3 + x^2 + \omega x + \omega^2.$$

From Theorem 1, $\mathcal{Q}$ is reversible. From Corollary 3, $\mathcal{Q}$ is self-dual. In addition, $\mathcal{Q}$ is optimal because $d_{\min} = 8$, which is the best known minimum distance for a linear code over $\mathbb{F}_4$ of length 22 and dimension 11.

TABLE 1. 1-Generator binary optimal self-dual reversible QC codes of index 2.

$g_{1,2}$	$[2m, k, d_{\min}]$
$\langle 7, 6, 4, 2, 0\rangle$	$[16, 8, 4]$
$\langle 10, 6, 3, 1, 0\rangle$	$[22, 11, 6]$
$\langle 11, 10, 9, 8, 7, 5, 4, 3, 0\rangle$	$[26, 13, 6]$
$\langle 18, 17, 15, 13, 8, 7, 4, 1, 0\rangle$	$[38, 19, 8]$
$\langle 17, 15, 10, 9, 6, 3, 2, 1, 0\rangle$	$[38, 19, 8]$
$\langle 19, 15, 14, 13, 12, 8, 4, 2, 0\rangle$	$[40, 20, 8]$
$\langle 19, 17, 15, 14, 13, 12, 11, 8, 6\rangle$	$[40, 20, 8]$
$\langle 22, 19, 13, 12, 10, 9, 7, 5, 3\rangle$	$[46, 23, 10]$
$\langle 22, 21, 17, 16, 14, 12, 10, 8, 5\rangle$	$[46, 23, 10]$
$\langle 24, 23, 22, 21, 20, 17, 16, 15, 12, 10, 9, 6, 5, 3, 2, 1, 0\rangle$	$[50, 25, 10]$
$\langle 24, 22, 21, 20, 18, 17, 16, 15, 14, 12, 9, 7, 6, 4, 3, 2, 1\rangle$	$[50, 25, 10]$
$\langle 24, 18, 16, 13, 12, 11, 9, 8, 6, 5, 4, 2, 1\rangle$	$[52, 26, 10]$
$\langle 25, 24, 18, 14, 12, 8, 7, 6, 5, 4, 3, 2, 0\rangle$	$[52, 26, 10]$
$\langle 26, 25, 23, 21, 20, 18, 16, 14, 13, 11, 10, 9, 6, 4, 2, 1, 0\rangle$	$[54, 27, 10]$
$\langle 26, 25, 24, 23, 22, 21, 17, 16, 15, 11, 10, 7, 6, 5, 4, 2, 0\rangle$	$[54, 27, 10]$
$\langle 24, 22, 21, 20, 18, 17, 16, 15, 14, 13, 12, 9, 2\rangle$	$[60, 30, 12]$
$\langle 29, 27, 25, 22, 21, 15, 13, 11, 10, 8, 6, 4, 1\rangle$	$[60, 30, 12]$
$\langle 31, 29, 28, 26, 25, 22, 21, 18, 16, 15, 14, 12, 11, 9, 8, 6, 4, 3, 2, 1, 0\rangle$	$[64, 32, 12]$
$\langle 30, 29, 22, 20, 18, 14, 12, 11, 9, 5, 4, 3, 0\rangle$	$[64, 32, 12]$
$\langle 32, 30, 27, 26, 24, 18, 15, 14, 12, 11, 10, 9, 8, 6, 3, 2, 0\rangle$	$[66, 33, 12]$
$\langle 32, 27, 24, 23, 22, 19, 14, 13, 10, 9, 7, 5, 1\rangle$	$[66, 33, 12]$
$\langle 32, 27, 26, 22, 21, 19, 18, 16, 12, 11, 9, 5, 3\rangle$	$[68, 34, 12]$
$\langle 27, 26, 25, 24, 21, 20, 19, 18, 17, 14, 11, 9, 7, 6, 5, 2, 1\rangle$	$[68, 34, 12]$
$\langle 38, 37, 35, 33, 31, 29, 28, 23, 19, 18, 17, 16, 15, 5, 4, 2, 0\rangle$	$[78, 39, 14]$
$\langle 36, 35, 34, 33, 24, 21, 20, 16, 15, 13, 12, 9, 8, 6, 5, 3, 1\rangle$	$[78, 39, 14]$
$\langle 40, 38, 36, 35, 31, 28, 27, 26, 23, 21, 17, 16, 15, 14, 13, 12, 8\rangle$	$[82, 41, 14]$
$\langle 40, 39, 38, 34, 33, 30, 26, 24, 20, 17, 15, 14, 13, 12, 11, 9, 7, 6, 4, 3, 2\rangle$	$[82, 41, 14]$
$\langle 47, 44, 41, 39, 38, 30, 29, 27, 26, 23, 22, 21, 20, 17, 14, 13, 12, 11, 10, 7, 6, 5, 3, 2, 0\rangle$	$[96, 48, 16]$

The code generated in Example 9 is an example of a 1-generator QC code [13], [18]. A 1-generator QC code of index 2 has a generator polynomial matrix (8) with $g_{2,2} = x^m - 1$. That is, the code is generated by $(g_{1,1}, g_{1,2})$ as an $\mathbb{F}_q[x]/\langle x^m - 1\rangle$-module. In the special case of 1-generator QC code with $g_{1,1} = 1$, Corollaries 3 and 4 reduce to the result [13, Corollary 4], i.e., self-duality is equivalent to reversibility.

We conclude this section by presenting some optimal self-dual reversible codes of different code lengths in the class of binary 1-generator QC codes of index 2. We search for generator polynomial matrices of the form

$$G = \begin{bmatrix} 1 & g_{1,2} \\ 0 & x^m + 1 \end{bmatrix}$$

that meet the reversibility conditions of Theorem 1, and hence are self-dual by Corollary 3. In Table 1, we provide polynomials $g_{1,2}$ from computer search results. Since binary self-dual codes have even minimum distances, any code in Table 1 is optimal in the sense that its minimum distance is the largest even integer less than or equal to the upper bound in [15]. We write $g_{1,2} = \langle 18, 17, 15, 13, 8, 7, 4, 1, 0\rangle$ to mean $g_{1,2} = x^{18} + x^{17} + x^{15} + x^{13} + x^8 + x^7 + x^4 + x + 1 \in \mathbb{F}_2[x]$. For each of the codes in Table 1, one can verify the reversibility conditions of Theorem 1 by using $\mu = 1, f_1 = g_{1,2}, f_2 = x^m + 1$, and $h = 1$.

VI. CONCLUSION

In this work, we focused on two classes of QC codes: the class of QC codes generated by diagonal generator polynomial matrices and the class of QC codes of index 2. We provided equivalent conditions for reversibility, self-orthogonality, and self-duality of QC codes in these classes. Consequently, we were able to combine some of these properties in QC codes of these classes. We showed that self-orthogonal reversible QC codes of index 2 exist for odd and even q. However, self-dual reversible QC codes of index 2 exist only for even q. We supported the theoretical results with computer search to include the property of being optimal. Finally, we considered the class of binary 1-generator QC codes of index 2. In Table 1, we offered some of these codes that combine the properties of being optimal, self-dual, and reversible. Many interesting numerical examples are presented.

REFERENCES

[1] T. Kasami, "A Gilbert–Varshamov bound for quasi-cycle codes of rate 1/2," *IEEE Trans. Inf. Theory*, vol. IT-20, no. 5, p. 679, Sep. 1974.
[2] S. Ling and P. Solé, "Good self-dual quasi-cyclic codes exist," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 1052–1053, Apr. 2003.
[3] S. Ling and P. Solé, "Good self-dual quasi-cyclic codes over F_q, q odd," in *Coding, Cryptography and Combinatorics* (Progress in Computer Science and Applied Logic), vol. 23, K. Feng, H. Niederreiter, and C. Xing, Eds. Basel, Switzerland: Birkhäuser, 2004, pp. 223–226.
[4] H. Matsui, "On generator and parity-check polynomial matrices of generalized quasi-cyclic codes," *Finite Fields Appl.*, vol. 34, pp. 280–304, Jul. 2015.
[5] R. T. Eldin and H. Matsui, "Quasi-cyclic codes via unfolded cyclic codes and their reversibility," *IEEE Access*, vol. 7, pp. 184500–184508, Dec. 2019.
[6] M. Barbier, C. Chabot, and G. Quintin, "On quasi-cyclic codes as a generalization of cyclic codes," *Finite Fields Appl.*, vol. 18, no. 5, pp. 904–919, Sep. 2012.
[7] A. Zeh and S. Ling, "Construction of quasi-cyclic product codes," in *Proc. 10th Int. ITG Conf. Syst., Commun. Coding*, Feb. 2015, pp. 1–6.

[8] R. T. Eldin and H. Matsui, "Run-length constraint of cyclic reverse-complement and constant GC-content DNA codes," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. E103.A, no. 1, pp. 325–333, Jan. 2020.
[9] F. Gursoy, E. S. Oztas, and I. Siap, "Reversible DNA codes using skew polynomial rings," *Applicable Algebra Eng., Commun. Comput.*, vol. 28, no. 4, pp. 311–320, May 2017.
[10] E. Oztas, B. Yildiz, and I. Siap, "A novel approach for constructing reversible codes and applications to DNA codes over the ring $\mathbb{F}_2[u]/(u^{2k}-1)$," *Finite Fields Appl.*, vol. 46, pp. 217–234, Jul. 2017.
[11] R. T. Eldin and H. Matsui, "On constant GC-content cyclic DNA codes with long codewords," in *Proc. Int. Symp. Inf. Theory Appl. (ISITA)*, Singapore, Oct. 2018, pp. 21–25.
[12] J. L. Massey, "Reversible codes," *Inf. Control*, vol. 7, no. 3, pp. 369–380, Sep. 1964.
[13] M. Zeraatpisheh, M. Esmaeili, and T. A. Gulliver, "Quasi-cyclic codes: Algebraic properties and applications," *Comput. Appl. Math.*, vol. 39, no. 2, pp. 1–21, Feb. 2020.
[14] N. J. A. Sloane, "Is there a (72, 36) $d = 16$ self-dual code?" *IEEE Trans. Inf. Theory*, vol. IT-19, no. 2, p. 251, Apr. 1973.
[15] M. Grassl. (2020). *Bounds on the Minimum Distance of Linear Codes and Quantum Codes*. [Online]. Available: http://www.codetables.de/
[16] N. Aydin, N. Connolly, and J. Murphree, "New binary linear codes from quasi-cyclic codes and an augmentation algorithm," *Applicable Algebra Eng., Commun. Comput.*, vol. 28, no. 4, pp. 339–350, Aug. 2017.
[17] Y. Jia, S. Ling, and C. Xing, "On self-dual cyclic codes over finite fields," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2243–2251, Apr. 2011.
[18] J. Pei and X. Zhang, "1-generator quasi-cyclic codes," *J. Syst. Sci. Complex.*, vol. 20, no. 4, pp. 554–561, Dec. 2007.

RAMY TAKI ELDIN received the Ph.D. degree from the Faculty of Engineering, Ain Shams University, Egypt, in 2015, with a focus on algebraic techniques of encoding/decoding cyclic codes over finite fields. Since 2015, he has been an Assistant Professor with the Faculty of Engineering, Ain Shams University, Egypt. He currently received the Postdoctoral Fellowship at the Toyota Technological Institute, Japan. His research interests include number theory and coding theory.

HAJIME MATSUI received the Ph.D. degree from the Graduate School of Mathematics, Nagoya University, Japan, in 1999. From 1999 to 2002, he was a Postdoctoral Fellow with the Toyota Technological Institute, Japan, where he was a Research Associate, from 2002 to 2006, and has been working as an Associate Professor, since 2006. His research interests include number theory, error-correcting codes, and computer science. He received the Best Paper Award from IEICE, in 2016.