PAPER Special Section on Information Theory and Its Applications

Linking Reversed and Dual Codes of Quasi-Cyclic Codes*

Ramy TAKI ELDIN[†a)], *Nonmember and* **Hajime MATSUI**[††b)], *Member*

SUMMARY It is known that quasi-cyclic (QC) codes over the finite field $\mathbb{F}_q$ correspond to certain $\mathbb{F}_q[x]$-modules. A QC code C is specified by a generator polynomial matrix G whose rows generate C as an $\mathbb{F}_q[x]$-module. The reversed code of C, denoted by $\mathcal{R}$, is the code obtained by reversing all codewords of C while the dual code of C is denoted by $C^\perp$. We call C reversible, self-orthogonal, and self-dual if $\mathcal{R} = C$, $C^\perp \supseteq C$, and $C^\perp = C$, respectively. In this study, for a given C, we find an explicit formula for a generator polynomial matrix of $\mathcal{R}$. A necessary and sufficient condition for C to be reversible is derived from this formula. In addition, we reveal the relations among C, $\mathcal{R}$, and $C^\perp$. Specifically, we give conditions on G corresponding to $C^\perp \supseteq \mathcal{R}$, $C^\perp \subseteq \mathcal{R}$, and $C = \mathcal{R} = C^\perp$. As an application, we employ these theoretical results to the construction of QC codes with best parameters. Computer search is used to show that there exist various binary reversible self-orthogonal QC codes that achieve the upper bounds on the minimum distance of linear codes.

key words: *error-correcting codes, minimum distance, reversed codes, reversible codes, self-orthogonal codes, self-dual codes*

1. Introduction

A linear code that is invariant under reversing the coordinates of its codewords is called a reversible code. Constructing reversible codes has received a lot of attention recently because the reversibility feature has been essential for certain applications, e.g., DNA codes [1]–[5] and binary locally repairable codes [6]. In [4], [8], [9], reversibility conditions were considered for various classes of codes over different algebraic structures. The reversibility condition for cyclic codes over the finite field $\mathbb{F}_q$ was investigated in [10]. A cyclic code over $\mathbb{F}_q$ is reversible if and only if its monic generator polynomial $g(x) \in \mathbb{F}_q[x]$ satisfies $g(x) = \beta g^*(x)$ for some $\beta \in \mathbb{F}_q - \{0\}$, where $\mathbb{F}_q[x]$ is the ring of polynomials over $\mathbb{F}_q$ and

$$f^*(x) = x^{\deg(f(x))} f\left(\frac{1}{x}\right)$$

is the reciprocal polynomial of $f(x) \in \mathbb{F}_q[x]$.

Quasi-cyclic (QC) codes are a natural generalization of cyclic codes [11]. QC codes have been researched because they contain good codes with the best known parameters [12], [13]. There exists a one-to-one correspondence between QC codes over $\mathbb{F}_q$ with cycle length m and code length $n = m\ell$ and $\mathbb{F}_q[x]$-submodules of $\left(\mathbb{F}_q[x]\right)^\ell$ that include $(1 - x^m)\left(\mathbb{F}_q[x]\right)^\ell$ for some positive integer ℓ. Therefore, a QC code is identified by its generator polynomial matrix G [14], which generalizes the generator polynomial $g(x)$ for a cyclic code. However, the condition of G for the reversible QC codes has not been known so far except for the case of $\ell = 2$ in [15].

In this paper, we provide necessary and sufficient conditions that determine the various relations between the reversed code and the dual code of a given QC code. For a QC code C, we define a reversed code $\mathcal{R}$ of C as the one consisting of reversed codewords of C while $C^\perp$ denotes the dual code of C. We explicitly derive a generator polynomial matrix F for $\mathcal{R}$ at Theorem 1. Through this result of F, we conclude that C is reversible, i.e., $\mathcal{R} = C$, if and only if $F = MG$ for some invertible polynomial matrix M at Corollary 1. Moreover, we also provide another reversibility condition of G for C that does not use F at Corollary 2. These results enable us to find generator polynomial matrices of reversible QC codes. On the other hand, we investigate various relations among C, $\mathcal{R}$, and $C^\perp$. Because the generator polynomial matrices H of its dual code and F of its reversed code for a given QC code can be calculated explicitly from G, it is easy to derive the conditions that represent the inclusion relations among these three codes. For example, $C \subseteq \mathcal{R}$ if and only if $G = MF$ for some polynomial matrix M. However, in practice, it might be easier to use the condition using only G, rather than using H or F. We find the conditions of G corresponding to the following relations of C, $C^\perp$, and $\mathcal{R}$.

1. $C^\perp \supseteq \mathcal{R}$, see Theorem 2.
2. $C^\perp \subseteq \mathcal{R}$, see Theorem 3.
3. $C^\perp = C$ if $C = \mathcal{R}$, see Theorem 4.
4. $C = \mathcal{R}$ if $C^\perp = C$, see Theorem 4.
5. $C = C^\perp = \mathcal{R}$, see Theorem 4.

A linear code of fixed length n and dimension k is called an optimal code if its minimum distance achieves the upper bound tabulated in [16]. Although it is expected that there are not many reversible codes, we find some desirable codes from our results. We use computer search to verify the above conditions to find some optimal binary reversible QC codes that satisfy self-orthogonality or self-duality. For even ℓ, we find some optimal binary reversible self-dual QC codes. On the other hand, for odd ℓ, because we show

Manuscript received February 19, 2021.
Manuscript revised June 18, 2021.
Manuscript publicized July 30, 2021.

[†]The author is with the Faculty of Engineering, Ain Shams University, Cairo, Egypt.
[††]The author is with Toyota Technological Institute, Nagoya-shi, 468-8511 Japan.

*This paper was partially presented in ISITA2020 [9].

a) E-mail: ramy.farouk@eng.asu.edu.eg
b) E-mail: matsui@toyota-ti.ac.jp

DOI: 10.1587/transfun.2021TAP0010

in Proposition 1 that the minimum distance of any non-trivial binary reversible self-dual QC code is two, we instead consider optimal binary reversible self-orthogonal QC codes in our search. In Table 1, we present several optimal binary reversible self-dual for even ℓ (self-orthogonal for odd ℓ) QC codes with different code parameters.

The rest of the paper is organized as follows. In Sect. 2, the notations of QC codes and their generator polynomial matrices necessary for the sequel are presented. In Sect 3, we show the explicit formula of F and the reversibility conditions. The other conditions describing the different cases between C, $\mathcal{R}$, and $C^{\perp}$ are presented in Sect. 4. Numerical examples and computer search results are shown in Sect. 5. Finally, we conclude the work in Sect. 6.

2. Preliminaries

This section summarizes the basic properties of QC codes (according to [14]), which will be used later. A linear code of length n over $\mathbb{F}_q$ is a linear subspace of the vector space $\left(\mathbb{F}_q\right)^n$. Codewords are the elements of the linear code. A linear code C of length n over $\mathbb{F}_q$ is called a QC code if the cyclic shift of all ℓ sections of each codeword is equal to another codeword, i.e., $\mathbf{c} \in C$ with

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

implies that

$$\left(c_{1,m-1}, c_{1,0}, \cdots, c_{1,m-2}, \cdots, c_{\ell,m-1}, c_{\ell,0}, \cdots, c_{\ell,m-2}\right) \in C,$$

where a positive integer ℓ divides n, $m = n/\ell$ is an integer, and $c_{i,j} \in \mathbb{F}_q$ for all $1 \le i \le \ell$ and $0 \le j \le m-1$.

Similar to cyclic codes, QC codes have a polynomial representation of their codewords. The codeword $\mathbf{c}$ given by (1) corresponds to the polynomial vector

$$\mathbf{c} = (c_1(x)\ c_2(x)\ \cdots\ c_{\ell-1}(x)\ c_\ell(x)), \tag{2}$$

where $c_i(x) = \sum_{j=0}^{m-1} c_{i,j} x^j \in \mathbb{F}_q[x]$ for all $1 \le i \le \ell$. In this polynomial representation, the cyclic shift of all ℓ sections of $\mathbf{c}$ corresponds to the multiplication $x\mathbf{c}$ followed by reduction modulo $1 - x^m$. It is shown that the above QC codes are in one-to-one correspondence with the $\mathbb{F}_q[x]$-submodules of $\left(\mathbb{F}_q[x]\right)^\ell$ that contain a submodule $(1 - x^m)\left(\mathbb{F}_q[x]\right)^\ell$. Throughout the manuscript, we identify a QC code with its corresponding $\mathbb{F}_q[x]$-submodule of $\left(\mathbb{F}_q[x]\right)^\ell$ and do not distinguish them.

A polynomial matrix means a matrix with entries in $\mathbb{F}_q[x]$. We call an ℓ-by-ℓ polynomial matrix G a generator polynomial matrix of C if its rows generate C as an $\mathbb{F}_q[x]$-module, i.e., $C = \left(\mathbb{F}_q[x]\right)^\ell G$.

Lemma 1. *For $i = 1, 2$, let C_i be a QC code and G_i be its generator polynomial matrix. Then, $C_1 \subseteq C_2$ if and only if $G_1 = MG_2$ for some polynomial matrix M.*

Proof. If $C_1 \subseteq C_2$, then, for any $\mathbf{c} \in C_1$, there exists $\mathbf{b} \in \left(\mathbb{F}_q[x]\right)^\ell$ such that $\mathbf{c} = \mathbf{b}G_2$. By taking each row of G_1 as $\mathbf{c} \in C_1$, we see that there exists a polynomial matrix M such that $G_1 = MG_2$. Conversely, if $G_1 = MG_2$, then $\mathbf{b}G_1 = \mathbf{b}MG_2$ for all $\mathbf{b} \in \left(\mathbb{F}_q[x]\right)^\ell$ and $C_1 \subseteq C_2$. □

If G is a generator polynomial matrix of C, then there exists an ℓ-by-ℓ polynomial matrix A with

$$AG = GA = \mathrm{diag}[1 - x^m], \tag{3}$$

where we use $\mathrm{diag}[e_i]$ to denote the ℓ-by-ℓ diagonal matrix with diagonal element e_i at the i-th row for all $1 \le i \le \ell$. Conversely, if a polynomial matrix G satisfies (3) for some polynomial matrix A, then G is a generator polynomial matrix for some QC code. To find A that satisfies (3) from a given G, or more generally, to find M that satisfies $G_1 = MG_2$ in Lemma 1, we apply Euclidean division algorithm [14, Lemma 4] by upper triangular polynomial matrices.

An explicit form of a generator polynomial matrix is given as follows. For an upper triangular polynomial matrix

$$G = \begin{pmatrix} g_{1,1} & g_{1,2} & g_{1,3} & \cdots & g_{1,\ell} \\ 0 & g_{2,2} & g_{2,3} & \cdots & g_{2,\ell} \\ 0 & 0 & g_{3,3} & \cdots & g_{3,\ell} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & g_{\ell,\ell} \end{pmatrix}, \tag{4}$$

G is a generator polynomial matrix of C if and only if the following conditions 1 and 2 are satisfied:

1. Each row of G is a codeword of C.
2. For all $1 \le i \le \ell$, $g_{i,i}$ is equal to $c_i(x) \ne 0$ with the minimum degree among all codewords of the form $(0\ \cdots\ 0\ c_i(x)\ \cdots\ c_\ell(x))$.

Moreover, for a generator polynomial matrix G of the form (4), we say that G is reduced if the following conditions 3 and 4 are satisfied:

3. $g_{j,j}$ is monic for all $1 \le j \le \ell$.
4. $\deg(g_{i,j}) < \deg(g_{j,j})$ for all $1 \le i \ne j \le \ell$.

Any generator polynomial matrix G' of C can be converted to the reduced generator polynomial matrix G by applying elementary row operations as polynomial matrices, or equivalently, there exists an invertible polynomial matrix M such that $MG' = G$, where we say that a polynomial matrix M is invertible if there exists a polynomial matrix M^{-1} such that $MM^{-1} = M^{-1}M = I$ and I is the identity matrix. We note that the reduced generator polynomial matrix of C is unique. Hereinafter, unless otherwise specified, we consider that $G = (g_{i,j})$ denotes the reduced generator polynomial matrix of C and $A = (a_{i,j})$ denotes the polynomial matrix satisfying (3).

If G is a generator polynomial matrix of the form (4), then the dimension k of C is given by

$$k = \sum_{i=1}^{\ell}(m - d_i) = n - \sum_{i=1}^{\ell} d_i = n - \deg(\det(G)),$$

where $d_i = \deg(g_{i,i})$ for all $1 \le i \le \ell$. The last formula $k = n - \deg(\det(G))$ is valid for any generator polynomial matrix of C.

The dual $C^\perp$ of C is a QC code over $\mathbb{F}_q$ with the same parameters ℓ and n as C with dimension $n-k$. From [14, Theorem 1], a generator polynomial matrix H of $C^\perp$ can be obtained as

$$H = \mathrm{diag}[x^{2m-d_i}]A^T\left(\frac{1}{x}\right) + (1-x^m)\mathrm{diag}[a_{i,i}^*], \tag{5}$$

where A^T is the transpose of the polynomial matrix A, $A(1/x)$ is the polynomial matrix replaced each x in A by $1/x$, and $a_{i,i}^* = x^{m-d_i}a_{i,i}(1/x)$ is the reciprocal polynomial of $a_{i,i}$.

For a codeword $\mathbf{c} \in C$ given by (1), the reverse of $\mathbf{c}$ is the vector $\mathbf{r} \in (\mathbb{F}_q)^n$ obtained by reversing the coordinates of $\mathbf{c}$, i.e.,

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

Analogous to (2), the polynomial representation of $\mathbf{r}$ is

$$\mathbf{r} = x^{m-1}\left(c_\ell\left(\frac{1}{x}\right)\ c_{\ell-1}\left(\frac{1}{x}\right)\ \cdots\ c_2\left(\frac{1}{x}\right)\ c_1\left(\frac{1}{x}\right)\right). \tag{6}$$

It is not necessarily true that $\mathbf{r} \in C$. We define the reversed code $\mathcal{R}$ of C as the code consisting of the reverse of all codewords in C, i.e.,

$$\mathcal{R} = \{\text{The reverse } \mathbf{r} \text{ of } \mathbf{c} \mid \mathbf{c} \in C\}.$$

In fact, $\mathcal{R}$ is a QC code over $\mathbb{F}_q$ with the same parameters ℓ, n, k, and the minimum distance as C.

3. Reversed Codes and Reversible Codes

In this section, first, we provide an explicit formula for a generator polynomial matrix of $\mathcal{R}$. Next, we show the necessary and sufficient conditions for QC codes to be reversible codes.

Lemma 2. *The following polynomial matrix U is invertible:*

$$U = (-1+2x^m-2x^{2m})I + \mathrm{diag}[x^{m+d_i}]G\left(\frac{1}{x}\right)\mathrm{diag}[a_{i,i}^*] + \mathrm{diag}[g_{i,i}^*]A\left(\frac{1}{x}\right)\mathrm{diag}[x^{2m-d_i}].$$

Proof. From its definition, $U = (u_{i,j})$ is an upper triangular polynomial matrix. Therefore its determinant is $\det(U) = \prod_{i=1}^{\ell} u_{i,i}$, where

$$\begin{aligned} u_{i,i} &= -1 + 2x^m - 2x^{2m} + x^m g_{i,i}^* a_{i,i}^* + x^m g_{i,i}^* a_{i,i}^* \\ &= -1 + 2x^m - 2x^{2m} + 2x^m(x^m - 1) = -1 \end{aligned}$$

and we use $(a_{i,i}g_{i,i})^* = a_{i,i}^* g_{i,i}^* = x^m - 1$. Thus, U is invertible because its determinant is a unit in $\mathbb{F}_q[x]$. □

Definition 1. *We denote the polynomial matrices F and B by*

$$F = \left(\mathrm{diag}[x^{m+d_i}]G\left(\frac{1}{x}\right) + (1-x^m)\mathrm{diag}[g_{i,i}^*]\right)J \tag{7}$$

and

$$B = J\left(A\left(\frac{1}{x}\right)\mathrm{diag}[x^{2m-d_i}] + (1-x^m)\mathrm{diag}[a_{i,i}^*]\right)U^{-1},$$

where J is the backward identity matrix of size ℓ-by-ℓ, i.e.,

$$J = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ \vdots & \iddots & 1 & 0 \\ 0 & \iddots & \iddots & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix}.$$

Lemma 3. *We have $FB = \mathrm{diag}[1-x^m]$, i.e., F is a generator polynomial matrix for some QC code.*

Proof. One can easily show that $J^{-1} = J$ and

$$\mathrm{diag}[x^{m+d_i}]G\left(\frac{1}{x}\right)A\left(\frac{1}{x}\right)\mathrm{diag}[x^{2m-d_i}] = x^{2m}\mathrm{diag}[x^m - 1].$$

Using these and Lemma 1 to simplify FB, we get

$$\begin{aligned} FBU &= -x^{2m}\mathrm{diag}[1-x^m] \\ &\quad + \mathrm{diag}[x^{m+d_i}]G\left(\frac{1}{x}\right)(1-x^m)\mathrm{diag}[a_{i,i}^*] \\ &\quad + (1-x^m)\mathrm{diag}[g_{i,i}^*]A\left(\frac{1}{x}\right)\mathrm{diag}[x^{2m-d_i}] \\ &\quad + (1-x^m)^2\mathrm{diag}[g_{i,i}^*]\mathrm{diag}[a_{i,i}^*] \\ &= \mathrm{diag}[1-x^m]U. \end{aligned}$$

□

The following theorem shows that F generates the reversed code $\mathcal{R}$ of C.

Theorem 1. *The polynomial matrix F given by (7) is a generator polynomial matrix of the reversed code $\mathcal{R}$ of C.*

Proof. By Lemma 3, F generates a QC code, which we refer to as Q. Because $\deg(g_{i,i}^*) = \deg(g_{i,i})$ and FJ is upper triangular with diagonal entries $g_{i,i}^*$, the dimension of Q is equal to that of C. Hence, $\mathcal{R}$ and Q have the same dimension. Therefore, it suffices to show that $\mathcal{R} \subseteq Q$.

Let $\mathbf{r}$ be an arbitrary codeword in $\mathcal{R}$, and let $\mathbf{c}$ be the corresponding codeword in C. Because of the dimension formula $k = \sum_{i=1}^{\ell}(m-d_i)$, there exists $b_i(x) \in \mathbb{F}_q[x]$ with $\deg(b_i) \le m - d_i - 1$ for all $1 \le i \le \ell$ such that $\mathbf{c} = (b_1\ b_2\ \cdots\ b_\ell)G$. From (6),

$$\mathbf{r} = x^{m-1}\left(b_1\left(\frac{1}{x}\right)\ b_2\left(\frac{1}{x}\right)\ \cdots\ b_\ell\left(\frac{1}{x}\right)\right)G\left(\frac{1}{x}\right)J.$$

Because (7) implies $F \equiv \mathrm{diag}[x^{d_i}]G(1/x)J \pmod{1-x^m}$,

$$\mathbf{r} \equiv (e_1\ e_2\ \cdots\ e_\ell)\,\mathrm{diag}[x^{d_i}]G\left(\frac{1}{x}\right)J \pmod{1-x^m}$$

$$\equiv (e_1\ e_2\ \cdots\ e_\ell)\,F \pmod{1-x^m},$$

where $e_i = x^{m-d_i-1}b_i(1/x) \in \mathbb{F}_q[x]$ for all $1 \le i \le \ell$. The last equation means that there is a polynomial vector $\mathbf{p} \in (\mathbb{F}_q[x])^\ell$ such that

$$\begin{aligned}\mathbf{r} &= (e_1\ e_2\ \cdots\ e_\ell)\,F + (1-x^m)\mathbf{p}\\ &= (e_1\ e_2\ \cdots\ e_\ell)\,F + \mathbf{p}BF = ((e_1\ e_2\ \cdots\ e_\ell) + \mathbf{p}B)\,F.\end{aligned}$$

Consequently, $\mathbf{r} \in Q$ and $\mathcal{R} \subseteq Q$. □

Remark 1. A generator matrix with entries in $\mathbb{F}_q$ as a linear code of the reversed code is equal to the original generator matrix flipped left and right. Hence, a generator polynomial matrix of the reversed code can also be calculated by converting the generator matrix to a polynomial matrix and then by applying elementary row operations as polynomial matrices, cf. [14], where the computational complexity as the number of finite field operations is $O(k^2n)$. On the other hand, the computational complexity of finding F by (7) from G is $O(1)$, but it takes $O(\ell^2 n)$ to make it the reduced form. Because usually ℓ is much smaller than k, e.g., $2k = m\ell$ if $n = 2k$, the computational complexity to obtain F is less in the method using Theorem 1 than in the method via the generator matrix as a linear code.

Two corollaries follow from Theorem 1, providing reversibility conditions for C.

Corollary 1. *A QC code C is reversible if and only if there exists an invertible polynomial matrix M such that $F = MG$.*

Proof. A QC code C is reversible if and only if $C = \mathcal{R}$. The uniqueness of the reduced generator polynomial matrix G of C indicates that the reduced form of F is equal to G. Equivalently, there exists an invertible polynomial matrix M such that $F = MG$. □

Example 1. Let C be a binary QC code of $\ell = 2$, $n = 14$, and

$$G = \begin{pmatrix} 1+x+x^3 & 1+x^2+x^3 \\ 0 & 1+x+x^2+x^4 \end{pmatrix}.$$

The polynomial matrix F is

$$F = \begin{pmatrix} x^7+x^8+x^{10} & 1+x^2+x^3 \\ 1+x^2+x^3+x^4 & 0 \end{pmatrix}.$$

Corollary 1 shows that C is reversible because $F = MG$ for

$$M = \begin{pmatrix} x^7 & 1+x+x^2+x^3+x^4+x^5+x^6 \\ 1+x & 1 \end{pmatrix}.$$

Corollary 2. *A QC code C is reversible if and only if the following two conditions are satisfied:*

1. $\prod_{i=1}^{\ell} g^*_{i,i} = \beta \prod_{i=1}^{\ell} g_{i,i}$ *for some* $\beta \in \mathbb{F}_q - \{0\}$,
2. $\mathrm{diag}[x^{m+d_i}]G(1/x)JA \equiv 0 \pmod{1-x^m}$.

Proof. If C is reversible, then the invertible matrix M mentioned in Corollary 1 fulfills

$$\begin{aligned}(1-x^m)M &= MGA = FA\\ &= \left(\mathrm{diag}[x^{m+d_i}]G\left(\frac{1}{x}\right) + (1-x^m)\mathrm{diag}[g^*_{i,i}]\right)JA.\end{aligned}$$

Condition 2 follows by a reduction modulo $1-x^m$. Calculating the determinants on both sides of the last equation yields

$$\begin{aligned}(1-x^m)^\ell \det(M) &= \left(\prod_{i=1}^{\ell} g^*_{i,i}\right)\det(J)\det(A)\\ &= \left(\prod_{i=1}^{\ell} g^*_{i,i}\right)\det(J)\frac{(1-x^m)^\ell}{\prod_{i=1}^{\ell} g_{i,i}}.\end{aligned}$$

Condition 1 follows from $\beta = \det(M)/\det(J) \in \mathbb{F}_q - \{0\}$.

Conversely, if conditions 1 and 2 are satisfied, then define $M = FA/(1-x^m)$. It follows from

$$M = \frac{1}{1-x^m}\mathrm{diag}[x^{m+d_i}]G\left(\frac{1}{x}\right)JA + \mathrm{diag}[g^*_{i,i}]JA$$

and condition 1 that $\det(M) \in \mathbb{F}_q - \{0\}$. Moreover, condition 2 indicates that M is a polynomial matrix. Thus, M is an invertible polynomial matrix. Multiplying G on both sides, $MG = F$. Then, by Corollary 1, C is reversible. □

Example 2. Consider again Example 1. The polynomial matrix A satisfying (3) is

$$A = \begin{pmatrix} 1+x+x^2+x^4 & 1+x^2+x^3 \\ 0 & 1+x+x^3 \end{pmatrix}.$$

Corollary 2 shows that C is reversible because $\prod_{i=1}^{2} g^*_{i,i} = \prod_{i=1}^{2} g_{i,i} = 1+x^7$ and

$$\begin{aligned}\mathrm{diag}[x^{7+d_i}]G\left(\frac{1}{x}\right)JA &= \begin{pmatrix} x^7+x^{14} & 0 \\ x^7+x^8+x^{14}+x^{15} & x^7+x^{14} \end{pmatrix}\\ &\equiv 0 \pmod{1+x^7}.\end{aligned}$$

Remark 2. Which of Corollaries 1 and 2 is easier to use to check its reversibility depends on the situation. Corollary 1 needs, after finding F, to compute M with $F = MG$ by elementary row operations. On the other hand, Corollary 2 uses only G, but because the product of all diagonal entries is required, ℓ needs to be small for example.

4. Linking Reversed and Dual Codes of C

In this section, we give conditions on G of C that indicate $C^\perp \supseteq \mathcal{R}$ and $C^\perp \subseteq \mathcal{R}$. Next, we deduce the reversibility condition of self-dual codes and the self-duality condition of reversible codes.

Theorem 2. $C^\perp \supseteq \mathcal{R}$ *if and only if* $GJG^T \equiv 0 \pmod{1-x^m}$.

Proof. Assume $C^\perp \supseteq \mathcal{R}$. Then, by Lemma 1, $F = MH$ for some polynomial matrix M. By (5) and (7), this equals

$$\begin{aligned}&\mathrm{diag}[x^{-m-d_i}]GJ + (1-x^{-m})\mathrm{diag}\left[g^*_{i,i}\left(\frac{1}{x}\right)\right]J\\&= M\left(\frac{1}{x}\right)\left(\mathrm{diag}[x^{-2m+d_i}]A^T + (1-x^{-m})\mathrm{diag}\left[a^*_{i,i}\left(\frac{1}{x}\right)\right]\right).\end{aligned} \tag{8}$$

Multiplying (8) on the left by $\mathrm{diag}[x^{m+d_i}]$ and on the right by G^T shows that $GJG^T = (1-x^m)N$ for some matrix N. Then there exists a non-negative integer u such that $S = x^u N$ is a polynomial matrix and we have $GJG^T x^u = (1-x^m)S$. Because x is coprime to $1-x^m$, x^u divides S and N is itself a polynomial matrix. Thus, $GJG^T \equiv 0 \pmod{1-x^m}$.

Conversely, assume $GJG^T = (1-x^m)N$ for some polynomial matrix N. Then $GJG^T = NA^TG^T$, $GJ = NA^T$, and by (5) and (7),

$$F \equiv \mathrm{diag}[x^{m+d_i}]N\left(\frac{1}{x}\right)A^T\left(\frac{1}{x}\right) \equiv LH \pmod{1-x^m},$$

where $L = \mathrm{diag}[x^{d_i}]N(1/x)\mathrm{diag}[x^{d_i-m}]$. That is $F = LH + (1-x^m)P$ for some matrix P. Equivalently, $F = (L+PE)H$ for some polynomial matrix E with $EH = \mathrm{diag}[1-x^m]$. Then there exists a non-negative integer v such that $T = x^v(L+PE)$ is a polynomial matrix and we have $Fx^v = TH$. Because H is a lower triangular matrix, we have $TH = \left(\sum_{p=j}^{\ell} t_{i,p}h_{p,j}\right)$ if $T = (t_{i,j})$ and $H = (h_{i,j})$. Because x^v divides $t_{i,\ell}h_{\ell,\ell}$ and $h_{\ell,\ell}$ is coprime to x, x^v divides $t_{i,\ell}$ for all $1 \le i \le \ell$. If x^v divides $\sum_{p=j}^{\ell} t_{i,p}h_{p,j}$ and $t_{i,p}$ for all $1 \le i \le \ell$ and $j < p \le \ell$, it follows from $\sum_{p=j}^{\ell} t_{i,p}h_{p,j} = t_{i,j}h_{j,j} + \sum_{p=j+1}^{\ell} t_{i,p}h_{p,j}$ that x^v divides $t_{i,j}h_{j,j}$. By induction on j, x^v divides T and $L+PE$ is itself a polynomial matrix. Hence, by Lemma 1, $C^\perp \supseteq \mathcal{R}$. □

Example 3. Let C be a QC code of $(q,\ell,n) = (2,2,14)$ and

$$G = \begin{pmatrix} 1+x^2+x^3 & 1+x^4+x^6 \\ 0 & 1+x^7 \end{pmatrix},\ A = \begin{pmatrix} 1+x^2+x^3+x^4 & 1+x^2+x^3 \\ 0 & 1 \end{pmatrix}.$$

Theorem 2 shows that $C^\perp \supseteq \mathcal{R}$ because

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

Lemma 1 again shows that $C^\perp \supseteq \mathcal{R}$ because $MH = F$ for

$$\begin{aligned}&\begin{pmatrix} x^3+x^4+x^6 & 1+x+x^3 \\ 1+x+x^3 & 0 \end{pmatrix}\begin{pmatrix} 1+x+x^2+x^4 & 0 \\ x^4+x^5+x^7 & 1 \end{pmatrix}\\&= \begin{pmatrix} x^3+x^4+x^6 & 1+x+x^3 \\ 1+x^7 & 0 \end{pmatrix}.\end{aligned}$$

Remark 3. Because $C^\perp \supseteq \mathcal{R}$ if and only if $F = MH$ for some polynomial matrix M, the computational complexity of finding M with $F = MH$ by elementary row operations is equal to $O(\ell^2 n)$. On the other hand, the computational complexity of checking $GJG^T \equiv 0 \pmod{1-x^m}$ is equal to $O(m^2\ell^3) = O(n^2\ell)$ because of the product of polynomial matrices. Hence, the computational complexity of checking $C^\perp \supseteq \mathcal{R}$ is smaller if $F = MH$ is used, but the method of Theorem 2 has the advantage that only G is used.

The equivalent condition for self-orthogonality of reversible QC codes follows from Theorem 2.

Corollary 3. *If C is reversible, then C is self-orthogonal if and only if $GJG^T \equiv 0 \pmod{1-x^m}$.*

Proof. If C is reversible, then $\mathcal{R} = C$. From Theorem 2, $C^\perp \supseteq C$ if and only if $GJG^T \equiv 0 \pmod{1-x^m}$. □

The inverse $C^\perp \subseteq \mathcal{R}$ of the inclusion relation in Theorem 2 is investigated similarly to Theorem 2.

Theorem 3. *$C^\perp \subseteq \mathcal{R}$ if and only if $A^TJA \equiv 0 \pmod{1-x^m}$.*

Proof. It can be shown in the same way as Theorem 2. Here, we prove it by another method using Theorem 2. By taking dual codes on both sides, $C^\perp \supseteq \mathcal{R}$ if and only if $C \subseteq \mathcal{R}^\perp$. Hence, by replacing C in Theorem 2 by $C^\perp$, $C^\perp \subseteq \mathcal{R}$ if and only if $HJH^T \equiv 0 \pmod{1-x^m}$. We show that $HJH^T \equiv 0 \pmod{1-x^m}$ if and only if $A^TJA \equiv 0 \pmod{1-x^m}$. Assume $HJH^T = (1-x^m)N$ for some polynomial matrix N. Then, by (5) and substituting $1/x$ for x,

$$\mathrm{diag}[x^{-2m+d_i}]A^TJA\mathrm{diag}[x^{-2m+d_i}] = (1-x^{-m})N'$$

for some matrix N'. Thus, $A^TJA = (1-x^m)N''$ for some matrix N''. Similarly to the proof of Theorem 2, N'' is shown to be a polynomial matrix. Conversely, the proof from $A^TJA \equiv 0 \pmod{1-x^m}$ to $HJH^T \equiv 0 \pmod{1-x^m}$ is shown in the same way. □

Example 4. Let C be the dual code of C in Example 3. Then G is the upper triangulation of H in Example 3, i.e.,

$$G = \begin{pmatrix} 1 & 1+x+x^2 \\ 0 & 1+x+x^2+x^4 \end{pmatrix} = \begin{pmatrix} 1+x+x^3+x^4+x^5 & 1+x+x^2 \\ x^4+x^5+x^7 & 1+x+x^2+x^4 \end{pmatrix}H.$$

Theorem 3 shows that $C^\perp \subseteq \mathcal{R}$ because

$$A = \begin{pmatrix} 1+x^7 & 1+x^4+x^5 \\ 0 & 1+x+x^3 \end{pmatrix},\ A^TJA = (1+x+x^3)(1+x^7)J.$$

Lemma 1 again shows that $C^\perp \subseteq \mathcal{R}$ because $H = MF$ for

$$\begin{aligned}&\begin{pmatrix} 1+x^7 & 0 \\ x^3+x^5+x^6 & 1+x^2+x^3 \end{pmatrix}\\&= \begin{pmatrix} 0 & 1+x^2+x^3 \\ 1+x^2+x^3 & 1+x^3+x^4+x^5 \end{pmatrix}\begin{pmatrix} 1+x^5+x^6 & 1 \\ 1+x^2+x^3+x^4 & 0 \end{pmatrix}.\end{aligned}$$

Corollary 4. *If C is reversible, then $C^\perp \subseteq C$ if and only if $A^TJA \equiv 0 \pmod{1-x^m}$.*

Because a self-dual code is self-orthogonal with $k = n/2$, Corollaries 3 and 4 imply that $GJG^T \equiv A^TJA \equiv 0 \pmod{1-x^m}$ for any reversible self-dual QC code. However, these identities become simpler through the use of $k = n/2$. This is shown in Theorem 4, but the following result is required.

Lemma 4. *We have $k = n/2$ and $GJG^T \equiv 0 \pmod{1-x^m}$*

if and only if $A = JG^T J$.

Proof. If $A = JG^T J$, then $GJG^T = GAJ = \mathrm{diag}[1-x^m]J \equiv 0 \pmod{1-x^m}$. In addition, $a_{i,i} = g_{\ell-i+1,\ell-i+1}$ for all $1 \le i \le \ell$. Then $k = n/2$ because

$$k = \sum_{i=1}^{\ell}(m - d_i) = \sum_{i=1}^{\ell} \deg(a_{i,i}) = \sum_{i=1}^{\ell} d_{\ell-i+1} = n - k.$$

Conversely, assume $k = n/2$ and $GJG^T = (1-x^m)M$ for some polynomial matrix M. Let $(I_{i,j}) = MJ$. Then $GJG^T J = (1-x^m)(I_{i,j})$. We show that $(I_{i,j})$ is the identity matrix.

- For $1 \le j < i \le \ell$, $I_{i,j} = 0$ because G and $JG^T J$ are upper triangular matrices.
- For $1 \le i = j \le \ell$, $g_{i,i}g_{\ell-i+1,\ell-i+1} = (1-x^m)I_{i,i}$. By equating the degrees, $d_i + d_{\ell-i+1} = m + \deg(I_{i,i})$. If $\deg(I_{i,i}) > 0$ for some $1 \le i \le \ell$, we get the contradiction

$$\begin{aligned} n/2 + n/2 &= \sum_{i=1}^{\ell} d_i + \sum_{i=1}^{\ell} d_{\ell-i+1} = \sum_{i=1}^{\ell}(d_i + d_{\ell-i+1}) \\ &= \sum_{i=1}^{\ell}(m + \deg(I_{i,i})) > \sum_{i=1}^{\ell} m = n. \end{aligned}$$

  Hence $\deg(I_{i,i}) = 0$ for all $1 \le i \le \ell$, i.e., $I_{i,i} = 1$ because $g_{i,i}$ and $g_{\ell-i+1,\ell-i+1}$ are monic polynomials.
- For $1 \le i < j \le \ell$, because of $JG^T J = (g_{\ell-j+1,\ell-i+1})$, we have $\sum_{h=i}^{j} g_{i,h}g_{\ell-j+1,\ell-h+1} = (1-x^m)I_{i,j}$. This implies $I_{i,j} = 0$ because the left side has a degree less than m as shown below

$$\begin{aligned} &\deg\left(\sum_{h=i}^{j} g_{i,h}g_{\ell-j+1,\ell-h+1}\right) \\ &\le \max_{i\le h\le j}\{\deg(g_{i,h}) + \deg(g_{\ell-j+1,\ell-h+1})\} \\ &< \max_{i\le h\le j}\{\deg(g_{h,h}) + \deg(g_{\ell-h+1,\ell-h+1})\} = m. \end{aligned}$$

We have shown that $GJG^T J = \mathrm{diag}[1-x^m]$, which implies $A = JG^T J$. □

The following result simplifies the conditions in Corollaries 3 and 4 for self-dual codes. It also shows that the self-duality condition of reversible QC codes is the same as the reversibility condition of self-dual QC codes. In fact, this generalizes a result in [15] where only QC codes of $\ell = 2$ were considered. Moreover, we provide a condition for QC codes to be reversible and self-dual.

Theorem 4. *1. If $A = JG^T J$, then C is self-dual if and only if C is reversible.*
2. If C is self-dual, then C is reversible if and only if $A = JG^T J$.
3. If C is reversible, then C is self-dual if and only if $A = JG^T J$.

Proof. If $A = JG^T J$ and C is self-dual, then $GJG^T = A^T JA = (1-x^m)J \equiv 0 \pmod{1-x^m}$. Theorem 2 implies $C = C^\perp \supseteq \mathcal{R}$, while Theorem 3 implies $C = C^\perp \subseteq \mathcal{R}$. Hence, $C = \mathcal{R}$, i.e., reversible.

If $A = JG^T J$ and C is reversible, then Lemma 4 shows that $GJG^T \equiv 0 \pmod{1-x^m}$ and $k = n/2$. By Corollary 3, C is self-orthogonal with $k = n/2$, i.e., self-dual.

If C is reversible and self-dual, then $k = n/2$ and $GJG^T \equiv 0 \pmod{1-x^m}$ by Corollary 3. Consequently, $A = JG^T J$ by Lemma 4. □

Example 5. Consider again Example 1. Theorem 4 shows that C is self-dual because $A = JG^T J$. Alternatively, because the polynomial matrix H satisfying (5) is

$$H = \begin{pmatrix} 1 + x^2 + x^3 + x^4 & 0 \\ x^7 + x^8 + x^{10} & 1 + x^2 + x^3 \end{pmatrix},$$

the self-duality of C can be checked by $H = MG$ with

$$M = \begin{pmatrix} 1 + x & 1 \\ x^7 & 1 + x^2 + x^3 + x^4 + x^5 + x^6 \end{pmatrix}.$$

Remark 4. Because, in most cases, G and A are obtained at the same time, cf. [14], the formula $A = JG^T J$ can effectively check the reversibility and the self-duality from one to the other at $O(1)$.

5. Optimal Binary Reversible Self-Dual QC Codes

In this section, we apply the theoretical results described in Sects. 3 and 4 to search for optimal binary QC codes that satisfy reversibility with self-orthogonality or self-duality. Although we mainly search optimal binary reversible self-dual QC codes, we consider to search optimal binary reversible self-orthogonal QC codes of odd ℓ because of Proposition 1.

Proposition 1. *If C is a binary reversible self-dual QC code of odd ℓ with $C \neq \{0\}$, then $d_{\min} = 2$.*

Proof. Because C is self-dual and ℓ is odd, m is even. Let $g = g_{(\ell+1)/2,(\ell+1)/2}$. We prove that $d_{\min} \le 2$ by showing that the $((\ell+1)/2)$-th row of G is $(0, \cdots, 0, 1 + x^{m/2}, 0, \cdots, 0)$. From Theorem 4, $A = JG^T J$, hence, from (3), $g^2 = 1 + x^m = (1 + x^{m/2})^2$, i.e., $g = 1 + x^{m/2}$. For any $(\ell+3)/2 \le j \le \ell$, the product of the $(\ell - j + 1)$-th row of A with the j-th column of G gives $\sum_{h=j}^{\ell-j+1} g_{\ell-h+1,j}g_{h,j} = 0$. Because of $q = 2$, all terms in the last equation are canceled out except $g^2_{(\ell+1)/2,j}$. Hence $g_{(\ell+1)/2,j} = 0$ for all $(\ell+3)/2 \le j \le \ell$. Hence, $d_{\min} \le 2$. Because of $C \neq \{0\}$, $d_{\min} = 2$. □

Example 6. Let C be a binary QC code of $\ell = 3$, $n = 6$, and

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

We show that C is self-dual, reversible, and optimal. The

Table 1 Optimal binary reversible self-orthogonal QC codes.

ℓ	n	k	$d_{\min}$	$G = (g_{i,j})$
2	64	32	12	$g_{1,1} = \langle 0\rangle$, $g_{1,2} = \langle 2,5,6,7,8,9,10,11,12,15,16,18,19,20,22,24,25,28,29,30,31\rangle$, $g_{2,2} = \langle 0,32\rangle$
3	36	6	16	$g_{1,1} = \langle 0,1,2,4,5,6\rangle$, $g_{1,2} = \langle 1,5,7,11\rangle$, $g_{1,3} = \langle 0,6,7,8,10,11\rangle$, $g_{2,2} = g_{3,3} = \langle 0,12\rangle$
4	68	34	12	$g_{1,1} = g_{1,2} = \langle 0\rangle$, $g_{1,3} = \langle 0,3,4,7,10,11,14\rangle$, $g_{1,4} = \langle 1,2,6,7,10,12,14\rangle$, $g_{2,2} = \langle 0,1\rangle$, $g_{2,3} = \langle 1,4,5,9,10,15\rangle$, $g_{2,4} = \langle 0,3,4,7,8,9,12,14\rangle$, $g_{3,3} = g_{3,4} = \langle 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\rangle$, $g_{4,4} = \langle 0,17\rangle$
5	25	8	8	$g_{1,1} = g_{2,2} = \langle 0,1\rangle$, $g_{1,4} = g_{2,5} = \langle 1,4\rangle$, $g_{1,5} = g_{2,4} = \langle 1,2,3,4\rangle$, $g_{3,3} = g_{4,4} = g_{5,5} = \langle 0,5\rangle$
6	36	18	8	$g_{1,1} = g_{1,3} = g_{2,2} = g_{2,5} = \langle 0\rangle$, $g_{1,4} = \langle 2,4\rangle$, $g_{1,5} = g_{4,4} = g_{4,6} = \langle 0,1,2,3,4,5\rangle$, $g_{1,6} = \langle 0,1,3,5\rangle$, $g_{2,4} = \langle 3\rangle$, $g_{2,6} = \langle 0,1,2,4,5\rangle$, $g_{3,3} = \langle 0,1\rangle$, $g_{3,4} = \langle 0,3,4\rangle$, $g_{3,5} = \langle 3,4\rangle$, $g_{3,6} = \langle 0,2,5\rangle$, $g_{5,5} = g_{6,6} = \langle 0,6\rangle$
7	42	14	12	$g_{1,1} = \langle 0\rangle$, $g_{1,3} = \langle 0,1,2,3\rangle$, $g_{1,4} = \langle 0,3\rangle$, $g_{1,5} = \langle 5\rangle$, $g_{1,6} = \langle 2,3,4,5\rangle$, $g_{2,2} = \langle 0,1\rangle$, $g_{2,3} = \langle 2\rangle$, $g_{2,4} = \langle 1,4\rangle$, $g_{2,5} = \langle 0,1,4,5\rangle$, $g_{2,6} = g_{3,6} = g_{4,4} = g_{4,6} = \langle 0,1,2,3,4,5\rangle$, $g_{2,7} = \langle 1\rangle$, $g_{3,3} = \langle 0,2,4\rangle$, $g_{3,7} = \langle 1,3,5\rangle$, $g_{5,5} = g_{6,6} = g_{7,7} = \langle 0,6\rangle$
8	40	20	8	$g_{1,1} = g_{2,2} = g_{3,3} = g_{4,4} = \langle 0\rangle$, $g_{1,5} = g_{4,8} = \langle 0,2,4\rangle$, $g_{1,6} = g_{2,5} = g_{3,8} = g_{4,7} = \langle 0,1,4\rangle$, $g_{1,7} = g_{2,8} = \langle 0,2\rangle$, $g_{1,8} = \langle 1,2,4\rangle$, $g_{2,6} = g_{3,7} = \langle 3\rangle$, $g_{2,7} = \langle 2\rangle$, $g_{3,5} = g_{4,6} = \langle 1\rangle$, $g_{3,6} = \langle 1,4\rangle$, $g_{4,5} = \langle 1,2,3,4\rangle$, $g_{5,5} = g_{6,6} = g_{7,7} = g_{8,8} = \langle 0,5\rangle$
9	54	24	12	$g_{1,1} = g_{1,2} = g_{3,3} = g_{3,4} = \langle 0\rangle$, $g_{1,6} = \langle 1\rangle$, $g_{1,7} = \langle 1,3,5\rangle$, $g_{1,8} = \langle 0,2\rangle$, $g_{1,9} = g_{2,5} = g_{3,5} = g_{4,5} = \langle 1,2,4,5\rangle$, $g_{2,2} = g_{4,4} = \langle 0,1\rangle$, $g_{2,6} = g_{4,8} = \langle 0,1,4\rangle$, $g_{2,7} = \langle 0,1,2,3,4\rangle$, $g_{2,8} = \langle 1,4\rangle$, $g_{2,9} = \langle 0,2,3,4\rangle$, $g_{3,6} = \langle 3,4\rangle$, $g_{3,7} = \langle 0,1,3,5\rangle$, $g_{3,8} = \langle 2\rangle$, $g_{3,9} = \langle 2,3,5\rangle$, $g_{4,6} = \langle 0,1,2,3\rangle$, $g_{4,7} = \langle 0,1,2,5\rangle$, $g_{4,9} = \langle 0,2,4\rangle$, $g_{5,5} = g_{7,7} = g_{9,9} = \langle 0,6\rangle$, $g_{6,6} = g_{6,7} = g_{8,8} = g_{8,9} = \langle 0,1,2,3,4,5\rangle$
10	40	20	8	$g_{1,1} = g_{2,2} = g_{3,3} = g_{4,4} = g_{5,5} = g_{3,6} = g_{5,8} = \langle 0\rangle$, $g_{1,6} = g_{3,8} = g_{5,10} = \langle 0,1\rangle$, $g_{1,7} = g_{1,9} = g_{2,10} = g_{4,10} = g_{5,6} = \langle 2,3\rangle$, $g_{1,8} = g_{2,7} = g_{3,10} = g_{4,9} = \langle 1,2\rangle$, $g_{1,10} = g_{4,6} = g_{5,7} = \langle 3\rangle$, $g_{2,6} = g_{5,9} = \langle 0,1,2\rangle$, $g_{2,8} = g_{3,9} = \langle 1\rangle$, $g_{2,9} = g_{4,7} = \langle 2\rangle$, $g_{3,7} = g_{4,8} = \langle 0,2,3\rangle$, $g_{6,6} = g_{7,7} = g_{8,8} = g_{9,9} = g_{10,10} = \langle 0,4\rangle$

polynomial matrix A satisfying (3) is

$$A = \begin{pmatrix} 1+x^2 & 0 & x \\ 0 & 1+x & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Corollary 2 shows that C is reversible because $g^*_{i,i} = g_{i,i}$ for all $1 \le i \le 3$ and

$$\operatorname{diag}[x^{2+d_i}]G\left(\frac{1}{x}\right)JA = \begin{pmatrix} x+x^3 & 0 & 0 \\ 0 & x^2+x^4 & 0 \\ x^2+x^6 & 0 & x^3+x^5 \end{pmatrix} \equiv 0 \pmod{1+x^2}.$$

Theorem 4 shows that C is self-dual because $A = JG^TJ$. In [16], the upper bound on the minimum distance of a binary linear code of length 6 and dimension 3 is 3. Although $d_{\min} = 2$, we consider C optimal because binary self-dual codes must have even $d_{\min}$.

Example 7. Let C be a binary QC code of $\ell = 5$, $n = 30$, and

$$G = \begin{pmatrix} 1 & 0 & 0 & 1+x+x^2 & 1+x+x^3+x^5 \\ 0 & 1 & 0 & 1+x^2+x^4+x^5 & 1+x+x^2 \\ 0 & 0 & 1+x^3 & 0 & 0 \\ 0 & 0 & 0 & 1+x^6 & 0 \\ 0 & 0 & 0 & 0 & 1+x^6 \end{pmatrix}.$$

The polynomial matrix A satisfying (3) is

$$A = \begin{pmatrix} 1+x^6 & 0 & 0 & 1+x+x^2 & 1+x+x^3+x^5 \\ 0 & 1+x^6 & 0 & 1+x^2+x^4+x^5 & 1+x+x^2 \\ 0 & 0 & 1+x^3 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

By Theorem 4, C is self-dual and reversible because $g^*_{i,i} = g_{i,i}$ for all $1 \le i \le 5$, $\operatorname{diag}[x^{6+d_i}]G(1/x)JA \equiv 0 \pmod{1+x^6}$, and $A = JG^TJ$. As can be seen from the third row of G, C has $d_{\min} = 2$. Although C is binary reversible self-dual, it is far from being optimal; In [16], the upper bound on the minimum distance of a binary linear code of length 30 and dimension 15 is 8.

It is known [13], [16] that the class of QC codes contains many binary codes with the best known parameters. The outline of computer search this time is to first randomly produce G and then check for the existence of the optimal reversible self-dual or self-orthogonal QC code. For even ℓ, we check the conditions in Corollary 2 and Theorem 4 to confirm that the obtained optimal binary QC codes are reversible and self-dual. For odd ℓ, we check the conditions in Corollaries 2 and 3 to confirm that the obtained optimal binary QC codes are reversible and self-orthogonal. The minimum distance is calculated by the full search or the method in [17]. All these codes are listed in Table 1, where the nonzero entries $g_{i,j}$ of the reduced generator polynomial matrices $G = (g_{i,j})$ are tabulated and we write, e.g., $g_{i,j} = \langle 0,6,7,8,10,11\rangle$ to mean $g_{i,j} = 1+x^6+x^7+x^8+x^{10}+x^{11} \in \mathbb{F}_2[x]$.

6. Conclusion

In this paper, first we have shown an explicit formula for a generator polynomial matrix F of the reversed QC code $\mathcal{R}$ of a QC code C with the reduced generator polynomial matrix G. It can be obtained immediately from this explicit formula that C is reversible, i.e., $\mathcal{R} = C$, if and only if $F = MG$ for some invertible polynomial matrix M. Moreover, in Corollary 2, we have characterized G of reversible C in terms of the entries of G without F. In Theorems 2 and 3, we have shown a necessary and sufficient condition of $C^{\perp} \supseteq \mathcal{R}$ and that of $C^{\perp} \subseteq \mathcal{R}$. In Theorem 4, we have given a condition on G of reversible and self-dual C. Because the method using generator matrices of linear codes does not take advantage of the characteristics of QC codes, the above formulas of generator polynomial matrices enable us efficiently to construct and search QC codes with reversibility, self-orthogonality, and self-duality.

As an application, we have used computer search to find binary reversible self-orthogonal or self-dual QC codes that achieve the best parameters of linear codes in [16]. We have focused on searching optimal binary reversible codes that are self-dual if ℓ is even and self-orthogonal if ℓ is odd because of Proposition 1. We have summarized our computer search results in Table 1, where we have shown the existence of binary reversible self-orthogonal or self-dual QC codes that attain upper bounds of $d_{\min}$ for various ℓ, n, and k.

Acknowledgments

This work was supported in part by JSPS KAKENHI Grant Number JP19K22850.

References

[1] N. Aboluion, D.H. Smith, and S. Perkins, "Linear and nonlinear constructions of DNA codes with Hamming distance d, constant GC-content and a reverse-complement constraint," Discrete Math., vol.312, no.5, pp.1062–1075, March 2012.
[2] H. Hong, L. Wang, H. Ahmad, J. Li, Y. Yang, and C. Wu, "Construction of DNA codes by using algebraic number theory," Finite Fields Th. App., vol.37, pp.328–343, Jan. 2016.
[3] R. Taki ElDin and H. Matsui, "Run-length constraint of cyclic reverse-complement and constant GC-content DNA codes," IEICE Trans. Fundamental, vol.E103-A, no.1, pp.325–333, Jan. 2020.
[4] N. Bennenni, K. Guenda, and S. Mesnager, "DNA cyclic codes over rings," Advances in Mathematics of Communications (AMC), vol.11, no.1, pp.83–98, Feb. 2017.
[5] P. Gaborit and O.D. King, "Linear constructions for DNA codes," Theor. Comput. Sci., vol.334, no.1–3, pp.99–113, April 2005.
[6] Y. Kim, C. Kim, and J. No, "Overview of binary locally repairable codes for distributed storage systems," Electronics, vol.8, no.6, 596, May 2019.
[7] H.J. Kim, W.-H. Choi, and Y. Lee, "Designing DNA codes from reversible self-dual codes over $GF(4)$," Discrete Math., vol.344, no.1, 112159, Jan. 2021.
[8] R. Taki ElDin and H. Matsui, "Quasi-cyclic codes via unfolded cyclic codes and their reversibility," IEEE Access, vol.7, pp.184500–184508, Dec. 2019.
[9] R. Taki ElDin and H. Matsui, "Generator polynomial matrices of reversed and reversible quasi-cyclic codes," International Symposium on Information Theory and its Applications (ISITA2020), pp.165–169, Oct. 2020.
[10] J.L. Massey, "Reversible codes," Information and Control, vol.7, no.3, pp.369–380, Sept. 1964.
[11] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
[12] S. Ling and P. Sole, "Good self-dual quasi-cyclic codes exist," IEEE Trans. Inf. Theory, vol.49, no.4, pp.1052–1053, April 2003.
[13] C. Martínez-Pérez and W. Willems, "Self-dual doubly even 2-quasi-cyclic transitive codes are asymptotically good," IEEE Trans. Inf. Theory, vol.53, no.11, pp.4302–4308, Nov. 2007.
[14] H. Matsui, "On generator and parity-check polynomial matrices of generalized quasi-cyclic codes," Finite. Fields. Th. App., vol.34, pp.280–304, July 2015.
[15] R. Taki ElDin and H. Matsui, "On reversibility and self-duality for some classes of quasi-cyclic codes," IEEE Access, vol.8, pp.143285–143293, Aug. 2020.
[16] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes," online available at http://www.codetables.de/ accessed on Feb. 19, 2021.
[17] M. Grassl, "Searching for linear codes with large minimum distance," Algorithms and Computation in Mathematics, vol.19, pp.287–313, Springer, 2006.

Ramy Taki ElDin received his Ph.D. in 2015 from the Faculty of Engineering, Ain Shams University, Egypt. His Ph.D. was on algebraic techniques of encoding/decoding cyclic codes over finite fields. Since 2015, he has been an Assistant Professor in the Faculty of Engineering, Ain Shams University, Egypt. In 2019, he received a one year Postdoctoral Fellowship at the Toyota Technological Institute, Japan. His research interests include number theory and coding theory.

Hajime Matsui received a Ph.D. in 1999 from the Graduate School of Mathematics, Nagoya University, Japan. From 1999 to 2002, he was a Postdoctoral Fellow at the Toyota Technological Institute, Japan. From 2002 to 2006, he was a Research Associate at the same institute, where he 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.